Cisco Bring Your Own Device (BYOD) Release 2.2

Last Updated: May 21, 2013

Cisco Validated Design

Building Architectures to Solve Business Problems

Important—The most current release of this document is available at: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html.

About the Authors

Zeb Hallock

Zeb Hallock, Technical Marketing Engineer, Systems Development Unit, Cisco Systems

Zeb Hallock is in the Enterprise Systems Engineering group of Cisco, focusing on digital media systems. He is also pursuing creation and development of future-based collaboration systems, holding two patents in the field. He has been with Cisco for 10 years working on enterprise system testing, system design and testing of H.323 based video conferencing, and network infrastructure. He has also been a specialist working on Cisco Unified IP Contact Center Cisco Unified MeetingPlace. Before Cisco he worked as a consultant designing and implementing local and wide area networks.

John Johnston

John Johnston, Technical Marketing Engineer, Systems Development Unit, Cisco Systems

John Johnston is a Technical Marketing Engineer in the Systems Development Unit (SDU) at Cisco. He has been with Cisco for 10 years, with previous experience as a network consulting engineer in Cisco's advanced services group. Prior to joining Cisco, he was a consulting engineer with MCI's Professional Managed Services group. Johnston has been designing or troubleshooting enterprise networks for the past 15 years. In his spare time, he enjoys working with microprocessor-based electronic projects including wireless environmental sensors. Johnston holds CCIE certification 5232. He holds a bachelor of science degree in electrical engineering from the University of North Carolina's Charlotte campus.

Fernando Macias

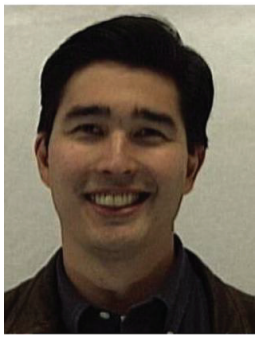
Fernando Macias, Solutions Architect, Systems Development Unit, Cisco Systems

Fernando Macias is a Solutions Architect in the Systems Development Unit (SDU), focusing on solutions for the enterprise market segment. Fernando has been with Cisco for over 13 years and has developed networking solutions that include Video, Security, and Content Delivery products. Fernando was also a member of Cisco's Advanced Services, where he provided network design support to large enterprise companies and a Systems Engineer for Cisco's commercial region. Prior to joining SDU, Fernando focused on Cloud Computing and Security, with the goal of leading Public Sector customers in their path to Cloud Computing.

In addition to Masters Degrees in Technology Management and Software Engineering, Fernando holds his Cisco CCIE certification in Routing and Switching.

Roland Saville, Technical Leader, Systems Development Unit, Cisco Systems

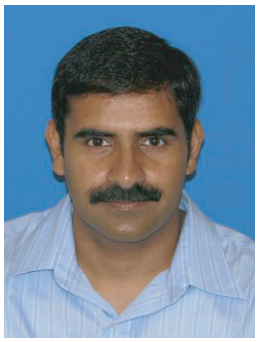
Roland Saville is a technical leader for the Systems Development Unit (SDU) at Cisco, focused on developing best-practice design guides for enterprise network deployments. He has more than 15



Roland Saville

years of experience at Cisco as a systems engineer, consulting systems engineer, technical marketing engineer, and technical leader. During that time, he has focused on a wide range of technology areas including the integration of voice and video onto network infrastructures, network security, wireless LAN networking, RFID, and energy management. He has also spent time focusing on the retail market segment. Prior to Cisco, he spent eight years as a communications analyst for Chevron Corporation. Saville holds a bachelor of science degree in electrical engineering from the University of Idaho and a master of business administration degree from Santa Clara University. He co-authored the book "Cisco TelePresence Fundamentals" and has eight U.S. patents.

Srinivas Tenneti, Technical Marketing Engineer, Systems Development Unit, Cisco Systems



Srinivas Tenneti

Srinivas Tenneti is a Technical Marketing Engineer in the Systems Development Unit (SDU) at Cisco, responsible for the design and architecture of security components for the BYOD project. He has more than 11 years of experience at Cisco where has worked in development, System Testing, and in Enterprise design and architecture. In the last 5 years Srinivas has worked on the design and architecture of GET-VPN, DMVPN, Branch Architecture, Internet Edge, and PKI as a service for VPN protocols. Srinivas has co-authored the book *PKI Uncovered: Certificate-Based Security Solutions for Next Generation Networks*.

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

Cisco Bring Your Own Device (BYOD) CVD Release 2.2

Cisco Bring Your Own Device (BYOD) CVD Release 2.2

Important—The most current release of this document is available at: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html.

Solution Overview

Bring Your Own Device (BYOD) has become one of the most influential trends that has or will touch each and every IT organization. The term has come to define a megatrend occurring in IT that requires sweeping changes to the way devices are used in the workplace.

What is BYOD? Does it mean employees pay for their own devices they use for work? Possibly, but the BYOD trend means much more. It is about end users being able to use the compute and communication devices they choose to increase productivity and mobility. These can be devices purchased by the employer, purchased by the employee, or both. BYOD means any device, with any ownership, used anywhere.

This document discusses how this trend will affect businesses, explores the challenges it creates for IT, and outlines the Cisco® technologies that are part of the solution. Cisco offers a comprehensive architecture to address these challenges, allowing end users the freedom to bring their choice of device to work while still affording IT the controls to ensure security and prevent data loss.

Cisco's BYOD Smart Solution 1.0

This document also forms the foundation for Cisco's BYOD Smart Solution 1.0 release. The BYOD Smart Solution is a comprehensive approach to BYOD that includes validated design guidance, professional services and support, an integrated roadmap, and a modular approach that follows the use cases outlined in this validated design. For more information, see: http://www.cisco.com/go/byod/.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

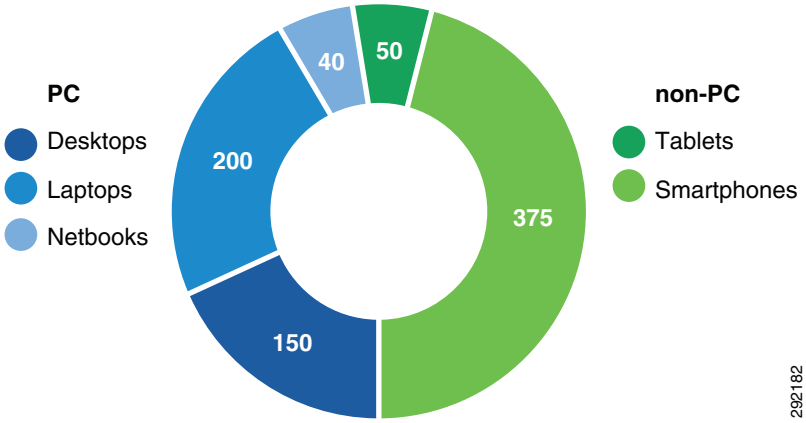
Business Drivers

To understand the challenges BYOD poses, it is helpful to understand the business trends that are driving BYOD adoption.

Consumer Devices

Previously, employers provided desktop and laptop computers that were typically the most advanced tools to which an employee had access. With the explosion in consumer devices, including laptops, netbooks, tablets, smartphones, e-readers, and others, employees typically have some of the most advanced productivity tools being used in their personal lives. Employees quickly asked their IT organizations: Why can't I use these tremendous productivity tools at work? Many IT organizations initially rejected the idea, citing security reasons and the inability to scale to approve and support more than a small handful of devices.

Figure 1 PC and Non-PC Sales, 2011 (Millions)—Source: Deloitte, 2011



In the last year, the persistence of end users demanding to leverage their tablet computers and smartphones to extend their productivity, even if they had to purchase the devices themselves, has led many IT departments to adopt less restrictive policies, allowing employees basic connectivity or, increasingly, full access to the IT network and corporate applications. This trend is likely irreversible and every IT organization will need to quickly adapt to the consumer device phenomenon. It should also be noted that in some industries and vertical segments, IT departments will only allow corporate issued devices on their networks, such as classified government networks, financial trading floors, etc. Nevertheless, every business needs a BYOD strategy, even if the intention is to deny all devices except IT approved and managed devices.

Multiple Needs and Multiple Devices

Many people had a desktop PC or laptop and added a mobile phone for voice calls. Mobile phones have largely been replaced with smartphones that can run applications and include Internet access and a camera. Many smartphones and tablets are as powerful and capable as laptops and PCs, enabling a new class of uses and applications.

In the future a single device may be used for computing, communications, and applications.

However today most believe there will continue to be different devices best suited to particular uses. For example, a laptop is not as portable as a smartphone, so people are likely to carry their smartphone for mobile communications. Tablets are powerful devices as well, but it is likely laptops and PCs will still

be used for document creation and publishing. This means people will more likely carry and use multiple devices and less likely that a single, all-purpose device will emerge. Figure 2 shows how various devices are suited to different tasks.

Figure 2 Variety of Devices

The impact of this trend is that many more devices will be connected to the network by the same employee or person, often simultaneously, and likely lead to a large increase in overall connected devices.

Work and Personal Overlap

Increasingly, work is an activity that people do, not a place to which they go. Extended connectivity through mobile and remote access to the corporate network gives employees tremendous flexibility and increased productivity. It also leads to a blurring of the line between work time and personal time, with employees trading set work schedules for the flexibility of working when and where they want to, often interweaving work and personal tasks.

A side effect of this flexibility is that users probably do not want to carry and switch between personal and work devices. Most employees want to be able to use a single smartphone, tablet, or laptop for both work and personal tasks and not also carry around corporate devices.

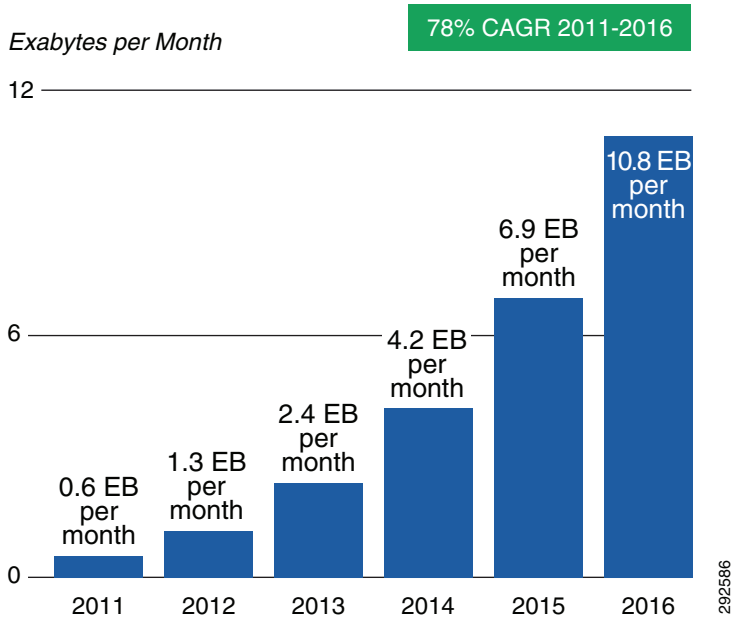
Many employees are willing to use their personal tablet or smartphone, for example, to access work applications. Many employers are considering or have implemented subsidy programs, whereby an employee is provided with money for devices, but it is up to the employee to purchase the devices they want.

The effect of this time and device overlap is that corporate and personal data will be increasingly co-mingled on devices, leading to security and privacy challenges.

Anywhere, Anytime Mobility

It is estimated that mobile devices and the traffic they create on networks will increase by 18X between 2011 and 2016, driven by more powerful smartphones and tablets, with users demanding Internet access and access to applications wherever and whenever they want. Mobile data traffic will grow at a compound annual growth rate (CAGR) of 78% from 2011 to 2016. Enabling this is an explosive build-out of WiFi networks by employers, 3G and 4G networks by mobile providers, as well as public WiFi by retailers, municipalities, etc.

Figure 3 *Worldwide Mobile Data Forecast 2011-2016 (Source: Cisco Visual Networking Index, 2011-2016)*



The more employees can easily access work using WiFi and mobile networks, the more widespread these networks will become, thereby further enabling access. The Cisco Visual Networking Index estimates that by the end of 2016 there will be 1.4 mobile devices per capita. The end result is pervasive connectivity anywhere and anytime, which means corporate networks will have more devices connected more frequently, leading to an even broader need for the 24/7 availability of applications.

Challenges for IT Organizations

Adopting BYOD comes with a set of challenges for the IT organization. Many of the benefits of BYOD, such as having the choice of any device and anywhere, anytime access, are somewhat antithetical to traditional IT requirements for security and support.

Providing Device Choice and Support

Traditionally, IT pre-determined a list of approved workplace devices, typically a standardized desktop, laptop, and perhaps even a small, standardized set of mobile phones and smartphones. Employees could choose among these devices, but generally were not permitted to stray from the approved devices list.

With BYOD, IT must approach the problem differently. Devices are evolving so rapidly that it is impractical to pre-approve each and every device brand and form-factor. It is also somewhat impractical to expect IT organizations to have the same level of support for each and every device that employees may bring to the workplace.

Hence most IT organizations have to establish, at a macro level, what types of devices they will permit to access the network, perhaps excluding a category or brand due to unacceptable security readiness or other factors. Support must also be considered, such as adopting more IT-assisted and self-support models.

Maintaining Secure Access to the Corporate Network

Device choice does not mean sacrificing security. IT must establish the minimum security baseline that any device must meet to be used on the corporate network, including WiFi security, VPN access, and perhaps add-on software to protect against malware.

In addition, due to the wide range of devices, it is critical to be able to identify each device connecting to the network and authenticate both the device and the person using it.

On-Boarding of New Devices

Most BYOD implementations will have a wide-range of devices including desktop PCs, laptops, netbooks, smartphones, tablets, and e-readers. It is likely some devices will be corporate owned and managed, while other devices may be employee purchased and self-supported.

On-boarding of new devices—bringing a new device onto the network for the first time—should be simple and, ideally, self-service with minimal IT intervention, especially for employee bought devices. IT also needs the ability to push updates to on-boarded devices as required.

Ideally on-boarding should be clientless, meaning no pre-installed software is required. This has an added benefit: if a self-service on-boarding model is successfully implemented, it can be easily extended to provide access to guests as well.

Enforcing Company Usage Policies

Businesses have a wide range of policies they need to implement, depending upon their industry and its regulations and the company's own explicit policies. Adoption of BYOD must provide a way to enforce policies, which can be more challenging on consumer devices like tablets and smartphones.

Another complication results from the mixing of personal and work tasks on the same device. Smartphones are likely used for business and personal calls and tablets likely have both personal and business applications installed. Access to the Internet, peer-to-peer file sharing, and application use may be subject to different policies when a user is on their personal time and network and when they are accessing the corporate network during work hours.

Visibility of Devices on the Network

Traditionally an employee had a single desktop PC or laptop on the network and probably an IP desk phone. If the employee called IT for support, it was likely straightforward to locate that user's device on the network and troubleshoot the issue.

With BYOD adoption, each employee is likely to have three, four, or more devices connected to the network simultaneously. Many of the devices will have multiple modes, able to transition from wired Ethernet to WiFi to 3G/4G mobile networks, moving in and out of these different connectivity modes during a session. It is critical for IT to have tools that provide visibility of all the devices on the corporate network and beyond.

Protecting Data and Loss Prevention

One of the largest challenges with any BYOD implementation is ensuring protection of corporate data. If a corporate asset, such as a laptop, is used to access business applications and data, typically that asset is tightly controlled by IT and likely subject to more restrictive usage policies.

Some industries need to comply with confidentiality regulations like HIPAA, security compliance regulations like PCI, or more general security practice regulations like Sarbanes-Oxley and others. Companies need to show compliance is possible with BYOD adoption, which can be more challenging than with a corporate-owned and managed device.

An employee-owned tablet or smartphone is likely being routinely used for personal access and business applications. Cloud-based file sharing and storage services are convenient for personal data, but can be potential sources of leakage for confidential corporate data.

IT must have a strategy for protecting business data on all devices whether corporate managed or employee self-supported and managed. This may include a secure business partition on the device which acts as a container of corporate data that can be tightly controlled and may also include the need for a Virtual Desktop Infrastructure (VDI) application to allow access to sensitive or confidential data without storing the data on the device.

Revoking Access

At some point in the lifecycle of a device or employee, it may become necessary to terminate access to the device. This could be due to a lost or stolen device, an employee termination, or even an employee changing roles within the company.

IT needs the ability to quickly revoke access granted to any device and possibly remotely wipe some or all of the data (and applications) on the device.

Ensuring Wireless LAN Performance and Reliability

As wireless access becomes pervasive, performance and reliability expectations are the same as what is expected from the wired network, including reliable connectivity, throughput, application response times, and increasingly voice, video, and other real-time collaboration applications.

This fundamental shift demands that IT change the service level of the corporate wireless LAN (WLAN) network from one of convenience to a mission critical business network, analogous to the wired network. Design and operation of the WLAN must include high availability, performance monitoring and mitigation, as well as seamless roaming.

Managing the Increase in Connected Devices

The increasing number of devices connected to the network, most likely with each employee having many devices simultaneously connected, can lead to IP address starvation as most legacy IP address plans were created under the assumption of fewer devices. This may hasten the need for IPv6 deployments both at the Internet edge as well as inside the enterprise network.

Challenges for End Users

The demand for BYOD is largely driven by users who want to choose the devices they use in the workplace. From a user perspective, there are challenges to address.

Keeping it Simple

BYOD solutions and technologies are quickly evolving, however one of the largest challenges is how to make it simple for people to get connected to and use corporate resources. The number of device possibilities, the range of connection types and locations, and the lack of widely adopted approaches can translate to difficulties for users.

Each device brand and form factor may require slightly different steps to be on-boarded and connected. Security precautions and steps may also vary depending upon how and where the user is trying to connect. For example, the corporate WiFi may require only user credentials, whereas connecting through a public WiFi hotspot may require credentials, a virtual private network (VPN), and other security steps.

Ultimately any BYOD solution needs to be as simple as possible for users, provide a common experience no matter where and when they are connecting, and be as similar as possible across devices.

Mixing Personal Devices With Work

BYOD brings a mix of personal and work tasks on the same device. Contact lists, E-mail, data files, applications, and Internet access can pose challenges. Ideally, users want to separate their personal data and activities from work. Personal photos, text messages, phone calls, and Internet browsing performed on their own time needs to be subject to personal privacy, while documents, files, applications using corporate data, and Internet browsing performed on company time needs to be in compliance with corporate policies.

Some employers make connecting with an employee-owned device contingent on signing an agreement so the company can monitor compliance, acceptable use policies, and otherwise act to protect corporate data. In some cases this may include remote wiping of all data on the device—potentially including personal data—which obviously can be a source of contention between IT and users if not properly managed.

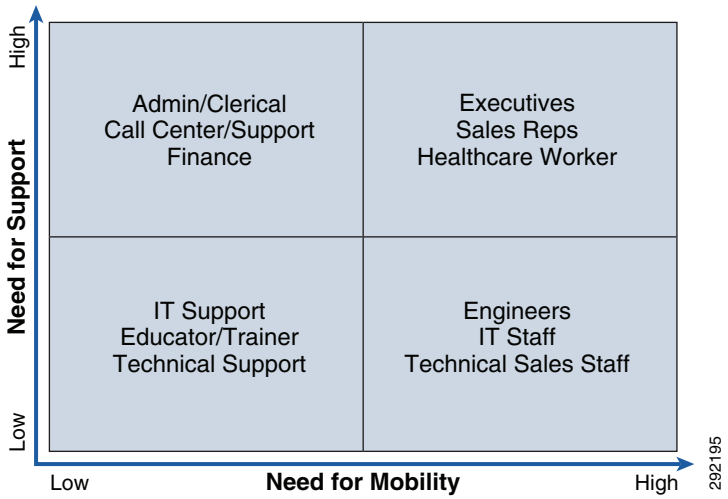
Considerations for BYOD Adoption

For any widespread adoption of BYOD, there are a number of factors that need to be considered.

Understand User Segments and Needs

It is important to understand that there are different segments of users within any BYOD implementation. One recommendation is to conduct a user segmentation analysis within the company to help understand needs and likely level of required support. An example is shown in Figure 4.

Figure 4 User Segments and Needs



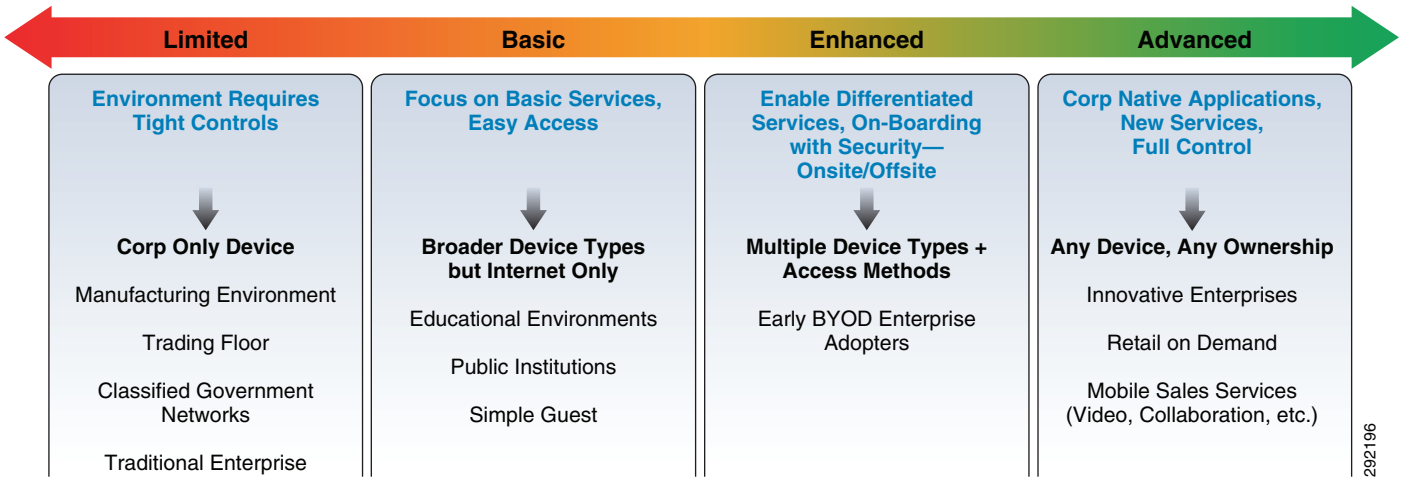
Every company is different. Figure 4 evaluates employee roles against the need for mobility and mobile applications and against the likely level of required support. BYOD deployments are easy with users who only need low levels of IT support, possibly using self-support communities to share best practices. Deployments may be more difficult with users who have high mobility needs but also require high support levels, such as executives.

Conducting such an analysis will help you understand entitlement policies and support models and may prevent frustration and cost overruns in the IT budget.

Deciding on a BYOD Adoption Strategy

Different businesses will approach BYOD with different expectations across a spectrum of adoption scenarios. Every business needs a BYOD strategy, even if the intention is to deny all devices except IT approved and managed devices. Figure 5 shows a number of possible adoption scenarios into which most businesses fit.

Figure 5 BYOD Adoption Scenarios



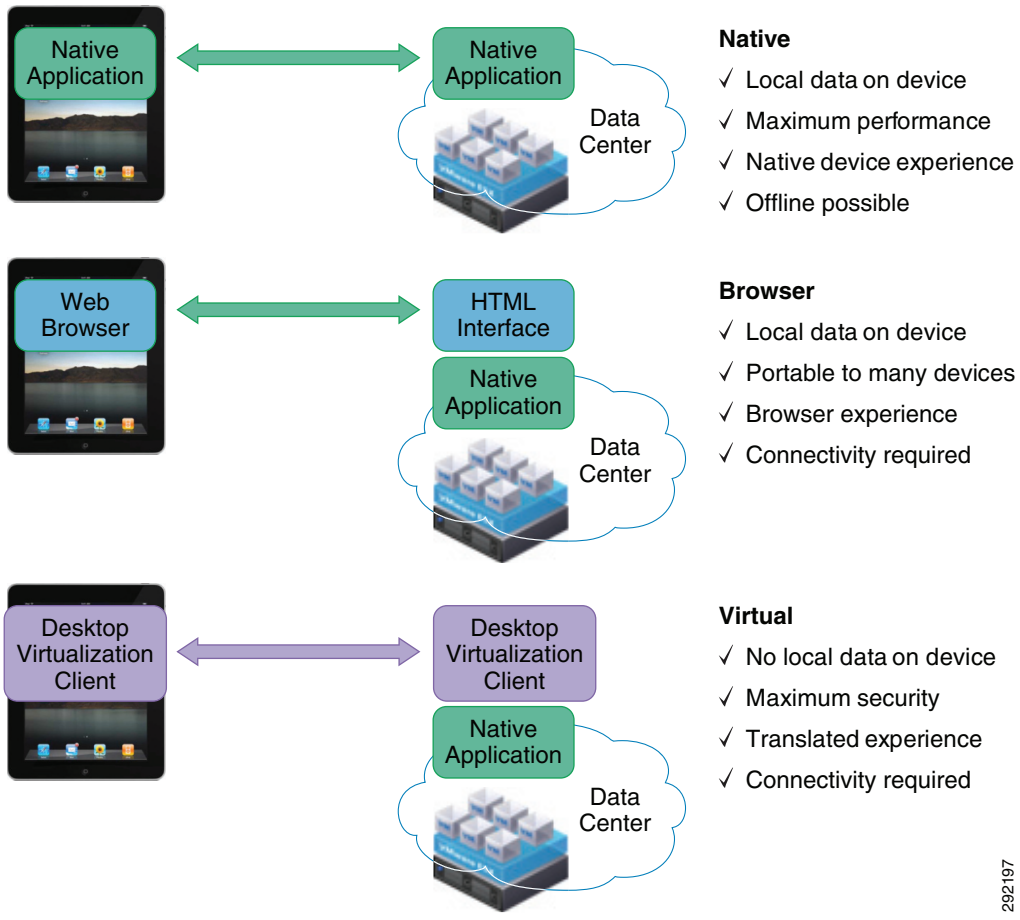
Businesses within industries with high degrees of regulation, such as finance or secure government agencies, may need to take a restrictive approach with BYOD adoption to protect sensitive data. Devices may need to be tightly controlled and managed as in the traditional IT approach, which may still be valid in these instances.

For many companies, adoption will range from allowing a broader set of devices with restrictive access to applications to embracing BYOD in full, encouraging broad adoption of many or all device types and deploying security measures to enable access to a broad set of enterprise applications and data. In the broadest sense, some companies will adopt a "mobile first" strategy, whereby their own internal applications development will be prioritized on tablets and smartphones, seeking competitive advantage by leveraging the broadest set of productivity tools and devices.

Considering Application Strategies

Securing and preventing the loss of corporate data is a top concern when implementing BYOD. It is important to understand three possible application architectures and the trade-offs involved: native, browser, and virtual. These are shown in Figure 6.

Figure 6 Native, Browser, and Virtual Modes



In native mode, applications running on the device communicate directly with the application server in the host data center (or cloud). Data may be exchanged and stored directly on the BYOD device. Typically the application performance and user experience are closest to the specific device; in other

words, a business application functions much like any other application on the device. All the productivity benefits and device behavior are preserved and applications can be tailored to provide enhanced experiences.

A browser approach is increasingly being adopted for application access due to the ease of portability across devices and operating systems. Essentially any device with a standard HTML browser capability can be used to access the application. The disadvantages are that much like native mode, data may be exchanged and stored directly on the BYOD device, leading to security challenges and concerns about data loss. In addition, there may be some sacrifice of user experience.

To contrast, in virtual mode applications exist on the application server in the data center (or cloud) and are represented through a VDI client on the device. Data is not stored locally on the BYOD device. Only display information is exchanged and rendered on the BYOD device. While this method provides maximum data security, user experience may be a compromise due to the translation from an application server to the form-factor and OS native to the BYOD device. Early adopters of this approach have provided somewhat negative feedback.

It is important to make decisions about which mode, native or virtual, will be relied on for the application architecture. Many companies may use a hybrid approach, using native mode for many standard business applications and virtual mode for a subset of applications with stricter confidentiality or sensitive data requirements.

Extending Collaboration to BYOD Devices

Ultimately, employees want to connect to the network not only for access to data applications, but also to collaborate with one another. Just as in traditional workspaces, users with BYOD devices want access to their company's voice, video, and conferencing services.

Standalone approaches, such as relying on the smartphone's cellular communications, can be somewhat effective. To be truly effective, it is essential to have an integrated approach that makes employees easily reachable within their company's communications directory and systems. Another consideration is how then do we extend these services to devices without cellular voice capabilities, such as an Apple iPad?

A complete BYOD solution must consider how to extend the full suite of collaboration applications to BYOD devices, including integrated voice, video, IM, conferencing, application sharing, and presence. Any solution needs to consider not only the employees using BYOD devices, but also others trying to collaborate with them.

Have an Encompassing End User Agreement

Although not part of the network architecture, one area that must be well thought out prior to any BYOD implementation is the end user agreement (EUA). Because of the mixing of personal and corporate data, and the potential of having employee-owned devices being used for work, it is critical to outline policies up front and be sure to communicate these to employees in advance.

IT organizations need to familiarize themselves with laws, including the Computer Fraud and Abuse Act, the Wiretap Act, and Communications Assistance for Law Enforcement Act (CALEA).

What will company policies be? Will communications be subject to monitoring? Will policies apply to both corporate and personal? Areas to be addressed include (but are not limited to):

- Text messaging
- Voice calling via cellular and via VoIP services such as Skype or Google Voice
- Internet browsing
- Instant messaging

- E-mail
- GPS and geo-location information
- Applications purchased/installed
- Stored photographs, videos, and e-books
- Device “wiping”

As a simple example, many businesses regularly filter and monitor Internet access to ensure compliance with policies against accessing inappropriate Web sites at work. Most BYOD devices have direct internet access through public WiFi and/or 3G/4G mobile Internet access. It would be common to have a policy against browsing X-rated Web sites on a device connected through the corporate network. Will the same policy apply if the employee decides to browse sites on their employee-owned device, on personal time, through public Internet access?

As another example, it would be common to have policies against transmitting inappropriate E-mails containing very personal photos through E-mail or text messaging while using a corporate-owned device or corporate network. Will the same policies apply to personal E-mails or personal text messaging on an employee-owned device? Which communications will be monitored? Which will not?

There have been several legal challenges recently for cases involving an employer who remotely “wiped” an employee-owned device, including both the corporate and personal data it contained. Imagine the surprise as an employee when by using your new tablet to access the corporate network, you unknowingly agreed to let IT delete your favorite family photos. Other challenges exist around potentially illegal wiretap situations where employees are challenging that their text message conversations were being illegally monitored by their company who failed to notify them.

The key to avoiding legal liabilities is to notify, notify, and notify again. Make it clear to employees in a written policy that they must accept how the company will treat corporate and personal data and communications on the BYOD device. By agreeing to the EUA, make it clear what rights the employee is forfeiting to gain access to the network with an employee-owned device.

Have a Lost or Stolen Device Policy

Similar to the previous discussion about having a complete EUA in place, businesses should have a plan in place for how lost or stolen devices will be handled. What will be the process for notification by employees? What are the necessary steps to remove access to the corporate network? What steps can and will be taken to remotely remove local data stored on the device?

Different solutions offered in the market provide varying degrees of capabilities to reach out to a device remotely and destroy data or applications to insure they remain confidential. Consider the types of data that are likely to be stored on BYOD devices and integrate mitigation plans into the overall BYOD strategy before deployment.

Design Overview

This section describes different uses cases for deploying BYOD and the design considerations for each use case. The remaining sections in this design guide provide more details on how to implement each use case.

There are numerous ways to enable a BYOD solution based on the unique business requirements of each organization. While some organizations may take a more open approach and rely on basic authentication, other organizations will prefer more secure ways to identify, authenticate, and authorize devices. A robust network infrastructure with the capabilities to manage and enforce these policies is critical to a successful BYOD deployment.

This design guide shows different ways to enforce these policies, relying on digital certificates, Microsoft Active Directory (AD) credentials, and unique device identifiers, such as MAC addresses.

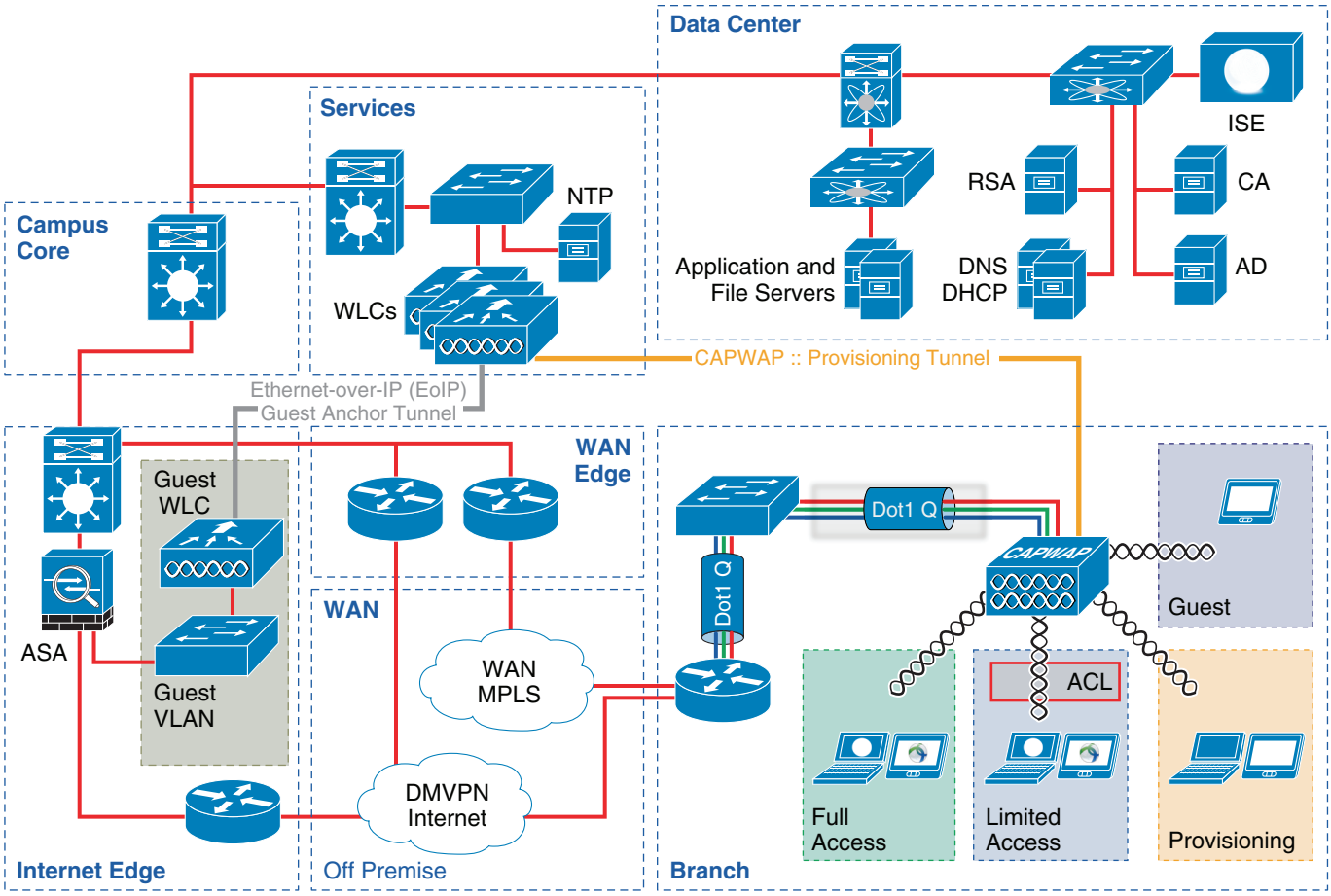
Providing a positive user experience is important for any BYOD deployment. Employees should be provided with a simple way to on-board their devices and enable the necessary security features on those devices with minimum manual intervention.

The method by which organizations determine corporate-issued versus employee-owned devices, presented within this design guide, is through the use of digital certificates and unique device identifiers. Because of the reliance on digital certificates, a discussion regarding the secure on-boarding of devices is included in this section.

The Cisco BYOD solution architecture builds on the Cisco Borderless Network Architecture and assumes best practices are followed in network infrastructure designs for campus, branch offices, Internet edge, and home office implementations. The Cisco BYOD architecture showcases the critical components to allow secure access for any device, ease of accessing the network, and centralized enforcement of company usage policies. This robust architecture supports a multitude of devices such as employee-owned, corporate-owned, or guest users trying to access the network locally or from remote locations.

Figure 7 shows a high-level illustration of the Cisco BYOD solution architecture. These infrastructure components are explained in detail in the following sections.

Figure 7 HIgh-Level BYOD Solution Architecture



Cisco Solution Components

Cisco provides a comprehensive BYOD solution architecture, combining elements across the network for a unified approach to secure device access, visibility, and policy control. To solve the many challenges described earlier, a BYOD implementation is not a single product, but should be integrated into an intelligent network.

Cisco Access Points

Cisco Access Points provide WiFi connectivity for the corporate network and handle authentication requests to the network via 802.1X. In addition, the Cisco Access Points at the branch location can either tunnel all the traffic to the campus or switch traffic locally based on the configuration.

Cisco Wireless Controller

Cisco Wireless LAN Controller (WLC) is used to automate wireless configuration and management functions and to provide the visibility and control of the WLAN. The WLC extends the same access policy and security from the wired network core to the wireless edge while providing a centralized access point configuration. The WLC interacts with the Cisco Identity Services Engine (ISE) to enforce authentication and authorization policies across device endpoints. Multiple WLCs may be managed and monitored by Cisco Prime Infrastructure.

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a core component of the Cisco BYOD solution architecture. It delivers the necessary services required by enterprise networks, such as Authentication, Authorization, and Accounting (AAA), profiling, posture, and guest management on a common platform. The ISE provides a unified policy platform that ties organizational security policies to business components.

The ISE also empowers the user to be in charge of on-boarding their device through a self-registration portal in line with BYOD policies defined by IT. Users have more flexibility to bring their devices to their network with features such as sponsor-driven guest access, device classification, BYOD on-boarding, and device registration.

The document *Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x* provides a detailed description of which end user devices are supported (http://www.cisco.com/en/US/docs/security/ise/1.1.1/compatibility/ise_sdt.html#wp80321).

Cisco Adaptive Security Appliance

Cisco Adaptive Security Appliance (ASA) provides traditional edge security functions, including firewall and Intrusion Prevention System (IPS), as well as providing the critical secure VPN (AnyConnect) termination point for mobile devices connecting over the Internet, including home offices, public WiFi hotspots, and 3G/4G mobile networks. The ASA delivers solutions to suit connectivity and mobility requirements for corporate-owned devices as well as employee-owned laptops, tablets, or mobile devices.

Cisco AnyConnect Client

Cisco AnyConnect™ client provides 802.1X supplicant capability on trusted networks and VPN connectivity for devices that access the corporate network from un-trusted networks, including public Internet, public WiFi hotspots, and 3G/4G mobile networks. Deploying and managing a single supplicant client has operational advantages as well as provides a common look, feel, and procedure for users.

In addition, the AnyConnect client can be leveraged to provide device posture assessment of the BYOD device, as well as a degree of policy enforcement and enforcing usage policies.

Cisco Integrated Services Routers

Cisco Integrated Services Routers (ISR), including the ISR 2900 and ISR 3900 families, provide WAN connectivity for branch and home offices and connectivity for the wired and WLAN infrastructure in the branch office. In addition, ISRs may provide direct connectivity to the Internet and cloud services, application and WAN optimization services, and may also serve as termination points for VPN connections by mobile devices.

Cisco Aggregation Services Routers

Cisco Aggregation Services Routers (ASR), available in various configurations, provide aggregate WAN connectivity at the campus WAN edge. In addition, ASRs may provide direct connectivity to the Internet and cloud services and may also serve as firewall. The ASR runs Cisco IOS XE software and offers Flexible Packet Matching (FPM) and Application Visibility and Control (AVC).

Cisco Catalyst Switches

Cisco Catalyst® switches, including the Catalyst 3000, Catalyst 4000, and Catalyst 6000 families, provide wired access to the network and handle authentication requests to the network via 802.1X. In addition, when deployed as access switches, they provide power-over-Ethernet (PoE) for devices such as VDI workstations, IP phones, and access points.

Cisco Prime Infrastructure

Cisco Prime Infrastructure (PI) is an exciting new offering from Cisco aimed at managing wireless and wired infrastructure while consolidating information from multiple components into one place. While allowing management of the infrastructure, Prime Infrastructure gives a single point to discover who is on the network, what devices they are using, where they are, and when they accesed the network.

Cisco Prime Infrastructure 1.2 is the evolution of Cisco Prime Network Control System 1.1 (NCS). It provides additional infrastructure and wired device management and configuration capabilities while improving on existing capabilities in NCS 1.1.

Cisco Prime Infrastructure interacts with many other components to be a central management and monitoring portal. Prime Infrastructure has integration directly with two other appliance-based Cisco products, the Cisco Mobility Services Engine (MSE) and Identity Services Engine (ISE) for information consolidation. Prime Infrastructure controls, configures, and monitors all Cisco Wireless LAN Controllers (WLCs), and by extension, all Cisco access points (APs) on the network. Prime Infrastructure also configures and monitors Cisco Catalyst switches and Cisco routers.

Secure Access to the Corporate Network

On-boarding for new devices (certificate enrollment and profile provisioning) should be easy for end users with minimal intervention by IT, especially for employee owned devices. Device choice does not mean giving up security. IT needs to establish the minimum security baseline that any device must meet to access the corporate network. This baseline should include WiFi security, VPN access, and add-on software to protect against malware. Proper device authentication is critical to ensure secure on-boarding of new devices and to ensure secure access to other devices on the network. Hence, proper device authentication protects the entire network infrastructure.

Who is accessing the network, *what* device they are using and *where* they are located need to be considered before implementing a BYOD solution. The user can initiate the provisioning process from a campus or a branch location. This design allows the user to provision and access resources from either location. In the past, a username/password was all that was needed as most access to the network was from an employee sitting behind a desk within the organization. A simple server to collect and authenticate this information was all that was needed. As networks implemented wireless into their organizations, a unique SSID (Wireless Network name) with a username and password was needed.

Digital certificates and two-factor authentication provide a more secure method to access the network. The end user typically must download client software to request a certificate and/or provide a secure token for access. One of the challenges with deploying digital certificates to client end points accessing the network remotely is that the user and endpoint may need to access the company's certification authority (CA) server directly (after being authenticated to the corporate network) to manually install the client certificate. This method requires the end user to manually install the client certificate while ensuring the certificate is installed in the proper certificate store on the local end point.

Deploying digital certificates on non-PC based devices requires a different process as many of these devices do not natively support all the features and functionality needed to create/download and install digital client certificates. As users become more and more mobile, authenticating users and devices accessing the network is an important aspect of BYOD.

Certificate Enrollment and Mobile Device Provisioning

Deploying digital certificates to endpoint devices requires a network infrastructure that provides the security and flexibility to enforce different security policies, regardless of where the connection originates. This solution focuses on providing digital certificate enrollment and provisioning while enforcing different permission levels. This design guide covers Android™ and Apple® iOS™ mobile devices, in addition to Windows 7 and Mac OS X.

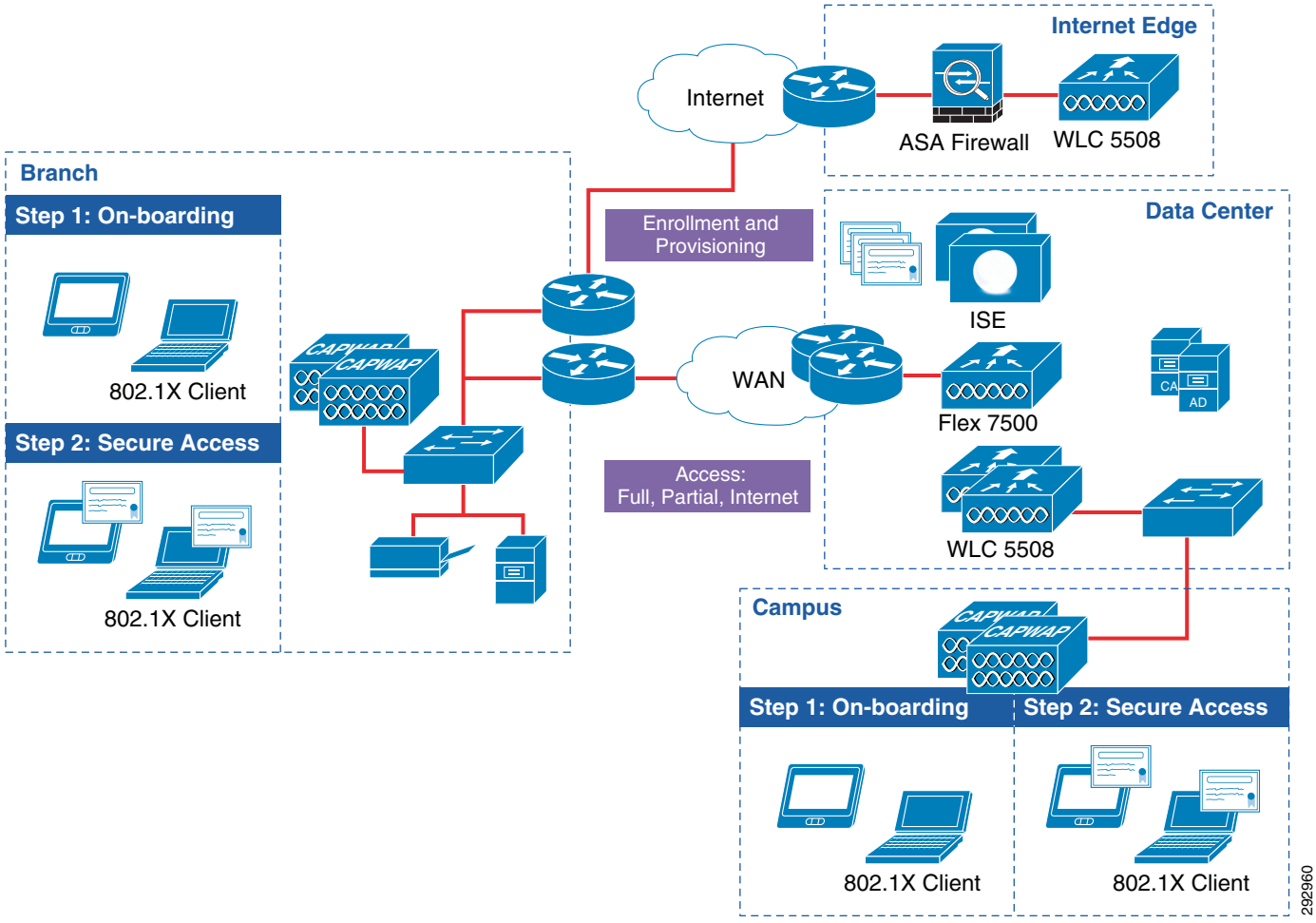
Figure 8 highlights the general steps that are followed for this solution when a mobile device connects to the network:

1. A new device connects to a provisioning SSID, referred to as the BYOD_Provisioning SSID. This SSID (open or secured with PEAP) is configured to redirect the user to a guest registration portal.
2. The certificate enrollment and profile provisioning begins after the user is properly authenticated.
3. The provisioning service requests information from the mobile device and provisions the configuration profile, which includes a WiFi profile with the parameters to connect to a secure SSID, called the BYOD_Employee SSID.
4. For subsequent connections, the device uses the BYOD_Employee SSID and is granted access to network resources based on different ISE authorization rules.

The design guide also covers a single SSID environment, where the same SSID is used for both provisioning and secure access.

Devices that do not go through the provisioning process simply connect to a guest SSID, which may be configured to provide Internet-only or limited access for guests or employees.

Figure 8 Enrollment and Provisioning for Mobile Devices



BYOD Use Cases in this Design Guide

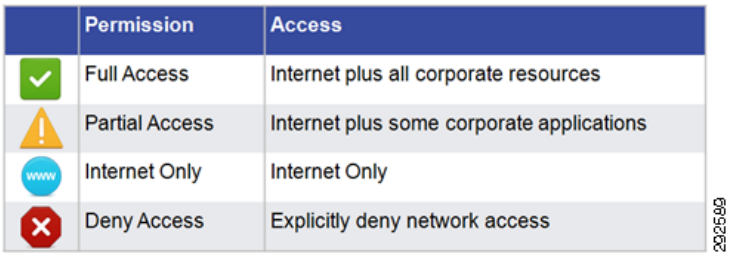
An organization's business policies will dictate the network access requirements which their BYOD solution must enforce. The following three use cases are examples of access requirements an organization may enforce:

- Enhanced Access—This comprehensive use case provides network access for corporate, personal, and contractor/partner devices. It allows a business to build a policy that enables granular role-based application access and extends the security framework on and off-premises.
- Limited Access—Enables access exclusively to corporate issued devices.
- Basic Access—This use case is an extension of traditional wireless guest access. It represents an alternative where the business policy is to not on-board/register employee wireless personal devices, but still provides Internet-only or partial access to the network.

ISE evaluates digital certificates, Active Directory group membership, device type, etc. to determine which network access permission level to apply. ISE provides a flexible toolset to identify devices and enforce unique access based on user credentials and other conditions.

Figure 9 shows the different permission levels configured in this design guide. These access levels may be enforced using access lists in the wireless controller or Catalyst switches or by relying on dynamic virtual LAN (VLAN) assignment. The design guide shows different ways to enforce the desired permissions.

Figure 9 Permission Levels



Design Use Case 1—Enhanced Access

This use case provides the infrastructure to on-board new devices onto the network by enrolling digital certificates and provisioning configuration files. The use case focuses on how to provide different access levels to personal devices based on authentication and authorization rules. Cisco ISE is used to enroll and provision personal devices only and it is assumed that the corporate devices will be on-boarded using a different method.

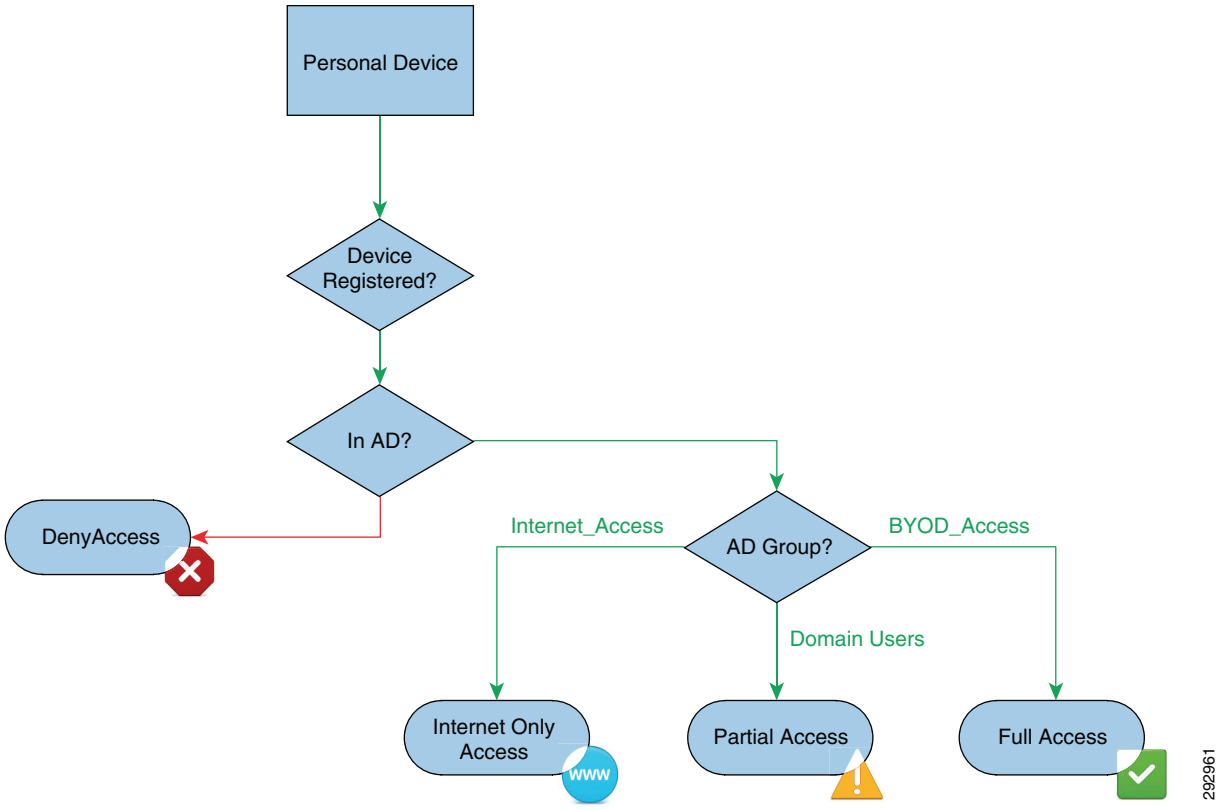
Employees that have registered their devices at the self-registration portal and have received a digital certificate are granted unique access based on their Active Directory group membership:

- Full Access—If the employee belongs to the BYOD_Access Active Directory group.
- Partial Access—If the employee belongs to the Domain Users Active Directory group.
- Internet Access—If the employee belongs to the Internet_Access Active Directory group.

The use case also explains how to prevent personal owned devices, for example Android devices, from accessing the network. Some organizations may not be ready to allow employees to connect their personal devices into the network and may decide to block their access until business or legal requirements are met. Cisco ISE provides the capability of identifying (profiling) the device type and preventing those devices from connecting to the network. This use case includes device profiling in ISE to deny access to Android devices.

Figure 10 highlights the connectivity flow for personal devices.

Figure 10 Personal Devices BYOD Access



This use case provides an effective way for organizations to embrace a BYOD environment for their employees and provide differentiated access to network resources. It also provides an option to deny specific types of personal devices from accessing the network.

Table 1 defines the network access permission assigned for each device type for the Enhanced Use Case and references the sections in this document that provide design details.

Table 1 Enhanced Access Use Case Permissions

	Campus	Remote Access	Branch	Section in This Document
Corporate Device	Full Access	Full Access	Full Access	Limited BYOD Access
Personal Device	Full/Partial/Internet Access	Full/Partial Access	Full/Partial/Internet Access	Enhanced BYOD Access
Contractor/Partner	Partial/Internet Only	Partial Only	Partial Access	Enhanced BYOD Access
Guest	Wireless Internet Only	Wireless Internet Only	Internet Only	BYOD Guest Wireless Access

Design Use Case 2—Limited Access

This use case applies to organizations that decide to enforce a more restrictive policy that allows only devices owned or managed by the corporation to access the network and denies access to employee personal devices.

Corporate owned devices are provisioned by the network administrator. Based on their certificate and Active Directory group membership, the devices are granted full access to the network. This use case introduces the use of a Whitelist, a list of corporate devices maintained by the Cisco ISE that is evaluated during the authorization phase.

Figure 11 shows the two different cases and the conditions that have to be met for each case.

Figure 11 Corporate Device BYOD Access

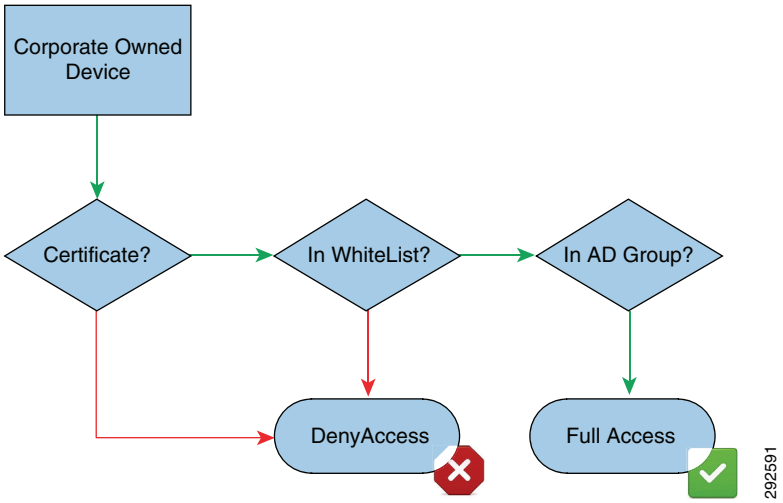


Table 2 defines the network access permission assigned for each device type for the Limited Access Use Case. It also references the sections in this document that provide the design details.

Table 2 Limited Access Use Case Permissions

	Campus	Remote Access	Branch	Section in This Document
Corporate Device	Full Access	Full Access	Full Access	Limited BYOD Access
Personal Device	Deny Access	Deny Access	Deny Access	Enhanced BYOD Access
Contractor/Partner	Deny Access		Deny Access	Enhanced BYOD Access
Guest	Wireless Internet Only		Wireless Internet Only	BYOD Guest Wireless Access

Design Use Case 3—Basic Access

Some organizations may implement a business policy which does not on-board wireless employee personal devices, yet provides some access to corporate services and the Internet for such devices. Some of the possible reasons include:

- The organization does not have the desire or the ability to deploy digital certificates on employee's personal devices.
- The employees may be unwilling to allow the organization to "manage" their personal device.
- The organization does not wish to manage and maintain separate lists of registered devices and devices which have full network access.

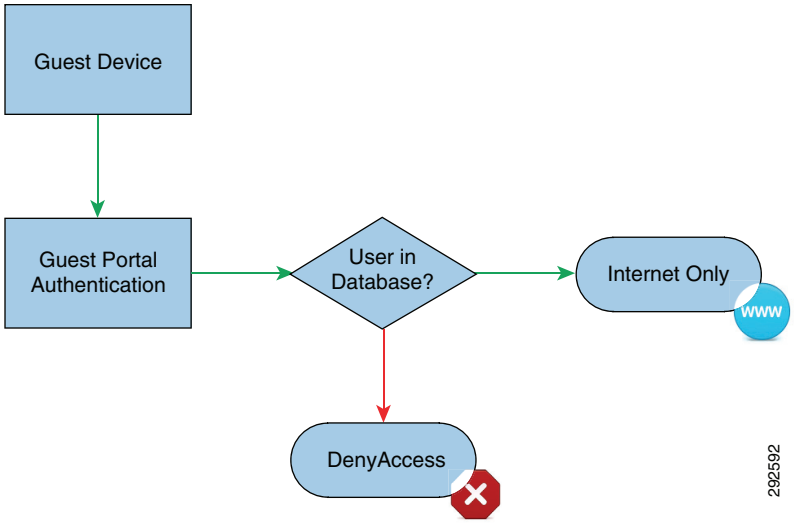
The design for this use case is based around extending traditional guest wireless access and providing similar guest-like wireless access for employee personal devices. The design guide focuses on two methods for extending guest wireless access to allow employee personal devices access to the guest network:

- Allowing employees to provision guest credentials for themselves.
- Extending guest Web authentication (Web Auth) to also utilize the Microsoft Active Directory (AD) database when authenticating guests or employees using personal devices.

In addition, the design guide discusses another option in which a second guest-like wireless SSID is provisioned for employee personal devices.

The Basic Access use case builds on traditional wireless guest access. Figure 12 shows the typical method for authenticating a device connecting to the guest wireless network.

Figure 12 Guest Wireless Access



This design guide discusses two approaches for modifying an existing guest wireless access implementation to enable Basic Access for employee personal devices.

Figure 13 Basic Access

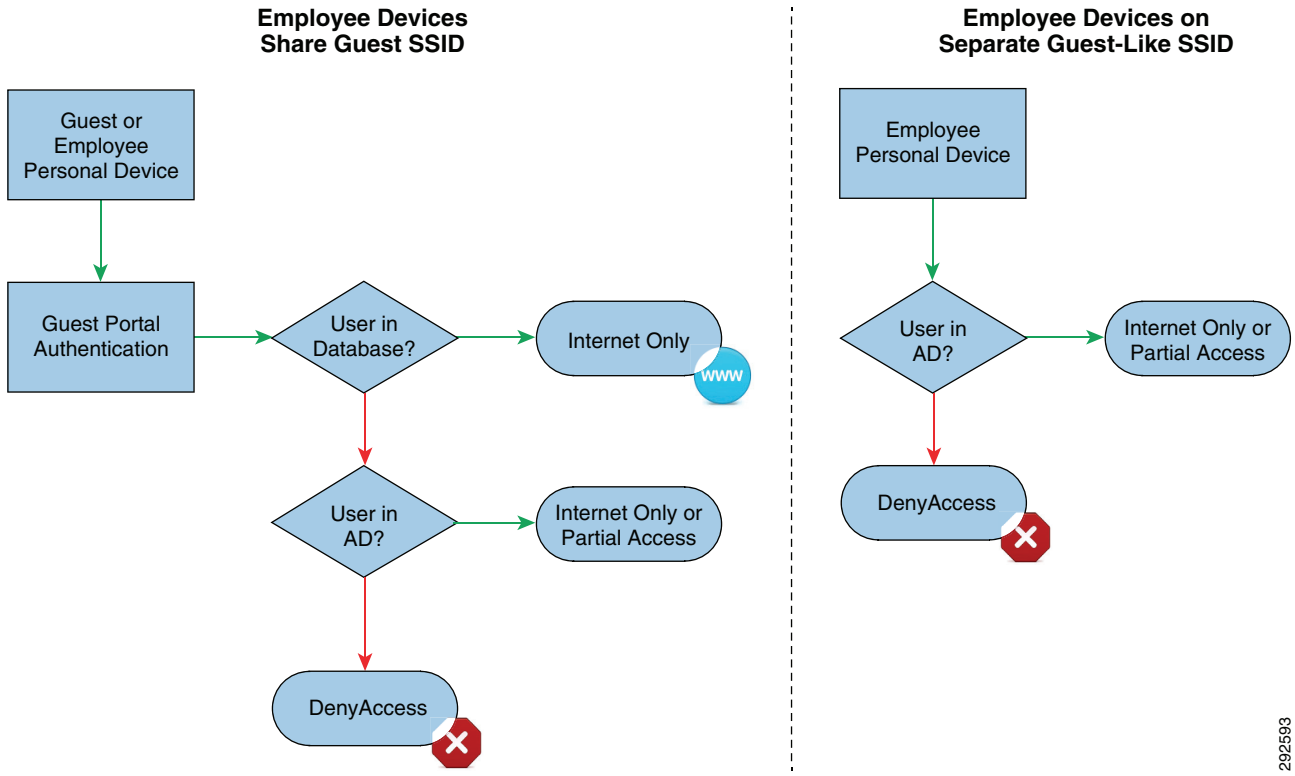


Table 3 defines the network access permission assigned for each device type for the Basic Access Use Case. It also references the sections in this document that provide the design details.

Table 3 Basic Access Use Case Permissions

	Campu	Remote	Branch	Section in This Document
Corporate Device	Full Access	Full Access	Full Access	Limited BYOD Access
Personal Device	Wireless Partial/Internet Only		Wireless Partial/Internet Only	Enhanced BYOD Access
Contractor/Partner	Wireless Partial/Internet Only		Wireless Partial/Internet Only	Enhanced BYOD Access
Guest	Wireless Internet Only		Wireless Internet Only	BYOD Guest Wireless Access

Branch Wide Area Network Design

Many network administrators will re-examine the wide area network prior to deploying a BYOD solution at the branch. Guest networks in particular have the ability to increase loads to a rate that can consume WAN bandwidth and compromise corporate traffic. While wired rates have increased from 10 Mbps to 1 Gbps and cellular networks have increase bandwidth from 30 Kbps for GPRS to around 20 Mbps for LTE, traditional branch WAN bandwidths have not experienced the same increase in performance. Employees and guests expect bandwidth, delay, and jitter on the corporate network to be at least as good

as they experience at home or on the cellular network. Furthermore, because WiFi access is typically free for corporate users and because most hand held devices will prefer WiFi over cellular, corporate users will likely continue using the guest or corporate SSID for Internet access, even when the LTE network offers faster speeds. This is forcing network administrators to explorer new WAN transport mechanisms such as Metro Ethernet and VPN over Cable to meet user expectations. Another approach is to offload guest Internet traffic at the branch in an effort to preserve WAN bandwidth for corporate traffic. Corporate Security Pollicy will need to be considered, however, relative to direct Internet access from the branch. As a result, the WAN is experiencing increased loads. While there are no new WAN requirements for branch BYOD services, some areas such as transport technology, access speeds, and encryption should be reviewed.

Branch WAN Infrastructure

The branch WAN infrastructure within this design includes ASR1006s as the headend routers. Two different WAN connections were terminated on these devices; the first router was configured as a service provider MPLS circuit and the second router was configured with an Internet connection. These headend routers were both placed in a “WAN edge” block that existed off of the campus core. The ASR that terminated the Internet connection also made use of IOS Zone-Based Firewall (ZBFW) and only tunneled traffic towards the branch was permitted.

Within the branch, two different designs were validated. The first design consisted of two Cisco 2921 ISR-G2 routers. One of the two routers terminated the SP MPLS circuit, while the second router terminated the Internet connection which could be utilized as a branch backup exclusively or as an alternate path for corporate traffic. The second design consisted of a single Cisco 2921 ISR-G2 router which terminated both circuits.

In both deployment modes, the Cisco IOS Zone-Based Firewall (ZBFW) was implemented to protect the branch’s connection to the Internet. Although entirely feasible, local Internet access from the branch was not permitted. For this purpose as well as for corporate data, DMVPN was implemented and only tunnel access granted for secure connectivity back to the campus headend routers for access to the data center or Internet where access was available through the typical corporate firewall/gateway. DMVPN was additionally used to secure traffic across the service provider’s MPLS circuit.

It is beyond the scope of this document to provide configuration information and design guidance around DMVPN, ZBFW configuration, QOS, and other aspects of the WAN infrastructure.

For detailed reference information around Next Generation Enterprise WAN (NGEW) design, refer to the documentation on Design Zone:
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html.

For additional QOS Design Guidance, refer to the *Medianet Design Guide* at:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_medianet.html.

Branch WAN Bandwidth Requirements

In the design presented within this document, branch access points are managed by a wireless LAN controller in the campus data center. A CAPWAP tunnel is established between the wireless controller and the access points within the branch locations. This CAPWAP tunnel is used for control traffic and possibly data traffic during the on-boarding process in some designs. This traffic is transported over the WAN. Since the design presented in this document utilizes a centralized AAA server (such as Cisco ISE), there may be an increase in authentication and authorization traffic as more employee managed devices are on-boarded. These new endpoints may also generate additional new traffic.

Further, guest Internet access is carried back to an anchor controller in the campus DMZ with this design. Finally, even though corporate managed and employee managed devices may use a FlexConnect design to locally terminate traffic onto local VLANs within the branch, a large percentage of traffic will continue to flow over the WAN to the corporate data center. All of this may result in increased loads on the WAN circuit as a result of the BYOD deployment.

It may be difficult to forecast the additional amount of traffic loading because the level of participation may not be well known prior to deploying BYOD. Wireless guest traffic in particular can be difficult to budget and may vary substantially depending on local events. A reasonable design goal is to provision a minimum of 1.5 Mbps at each branch that offers BYOD. The head-end WAN aggregation circuits should be provisioned to follow traditional oversubscription ratios (OSR) for data. This will allow adequate bandwidth for smaller deployments. Larger branch locations will likely need additional bandwidth, especially if the guest users are likely to expect the use of high bandwidth applications such as streaming video traffic. The WAN architecture should offer enough flexibility to adjust service levels to meet demand. Sub-rate MPLS access circuits or a dedicated WAN router that can allow additional bandwidth to be brought online can accomplish this. Address space adequate for each branch should also be considered because FlexConnect can allow wireless DHCP clients to pull from local scopes. Additional information concerning bandwidth management techniques such as rate-limiting is discussed in BYOD Guest Wireless Access.

Encryption Requirement

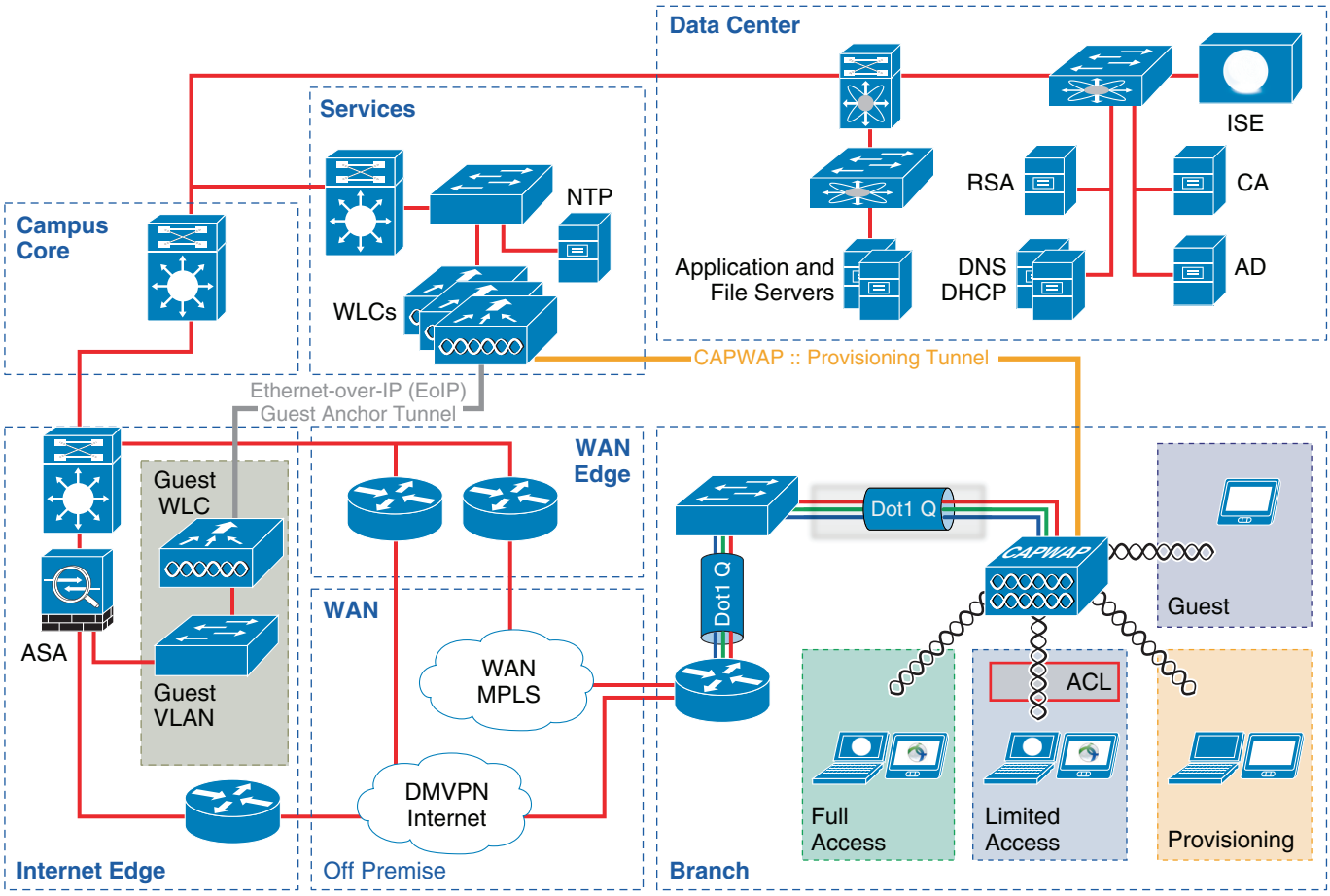
Another component of the BYOD enabled branch is a FlexConnect wireless design with local branch termination. This allows branch wireless devices to directly access resources located on the branch LAN without the need to traverse a CAPWAP tunnel to the wireless controller. This reduces the amount of traffic that needs to be carried by the WAN by eliminating the hair-pinning of traffic from the branch location, back to the wireless controller within the campus, and then back to the branch server. The effect reduces load in both directions—upstream within a CAPWAP tunnel and downstream outside of the CAPWAP tunnel. The benefits are realized when a wireless branch device is connecting to a server located in the same branch. If the traffic is destined for the data center, it still transits the WAN but outside of the CAPWAP tunnel, benefiting from the same level of security and performance as wired traffic. Depending on the application, it may not be encrypted so additional WAN security might be needed. If the branch is using a broadband connection as either the primary or backup path, then obviously encryption technologies such as DMVPN should be deployed. However, even if an MPLS VPN service is being used, the enterprise may still want to consider encrypting any traffic that passes off premise.

Transport

Not all wireless branch traffic will be terminated locally on the branch access point. In the designs in this version of the design guide, guest traffic is still tunneled within a CAPWAP tunnel to a central controller at a campus location. Depending upon the on-boarding design implemented (single SSID versus dual SSID), traffic from devices which are in the process of being on-boarded may also remain in the CAPWAP tunnel to the central controller. This traffic may compete for bandwidth with the corporate traffic also using the WAN link, but not inside a tunnel. These concerns are addressed with a mix of traditional QoS services and wireless rate-limiting. In some situations, the transport will determine what is appropriate. If Layer 2 MPLS tunnels are in place, destination routing can be used to place CAPWAP traffic on a dedicated path to the wireless controllers. This may be useful as an approach to isolated guest traffic from the branch towards the campus since FlexConnect with local termination will pass most corporate traffic outside of a CAPWAP tunnel directly to its destination. Return traffic from the campus towards the branch is more difficult to manage without more complex route policies, but may be possible with careful planning.

Figure 14 illustrates at a high level a typical WAN architecture.

Figure 14 WAN Architecture



Branch Network Design

The anywhere, any device requirement of BYOD implies that employees can use either corporate or personal devices at either campus or branch locations. When they do, the pertinent component of the BYOD architecture is the ability to enforce policies on these devices at either the branch or at the campus location. Policy enforcement is effective if and only if there is a well-designed branch network infrastructure in place. This branch netwok infrastructure can be categorized into WAN and LAN components. This section discusses the high level key design elements of LAN design.

In the BYOD designs in this document, the main use cases provide full access for corporate owned or managed devices and partial access or Internet only access for employee managed devices. To implement the use cases, the method adopted in this design guide for branch locations is to place the device into an appropriate VLAN after a device is authenticated and authorized. For example, a corporate managed device which needs full access to the network is placed in a VLAN that is meant for corporate owned devices only. On the other hand, the personal devices are placed in a different VLAN.

Wireless Controller Design

There are currently two implementation modes in the Cisco Unified Wireless Network (CUWN) architecture:

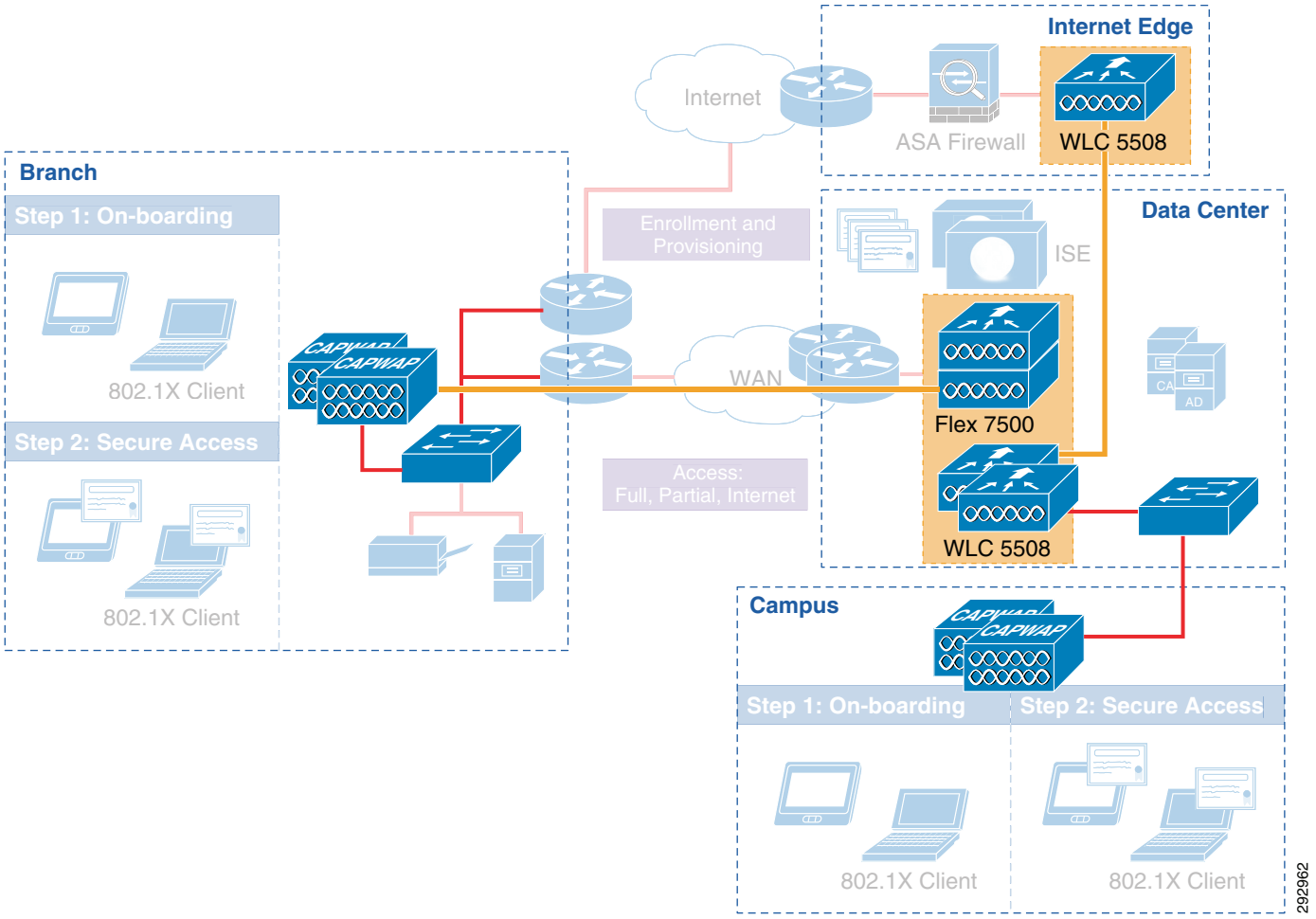
- Local mode (also referred to as centralized controller design)
- FlexConnect mode

Centralized wireless controller designs require all the wireless traffic to be tunneled back to the wireless controller before it is terminated on an Ethernet segment and switched or routed to different locations. This mode provides greater control and is often easier to implement security policies, since all wireless traffic is brought back to a central point.

The second mode, FlexConnect, is an innovative Cisco technology which provides more flexibility in deploying a wireless LAN. For example, the wireless LAN may be configured to authenticate users using a centralized AAA server, but once the user is authenticated the traffic is switched locally. The local switching functionality provided by FlexConnect eliminates the need for data traffic to go all the way back to the wireless controller when access to local resources at the branch is a requirement. This reduces the Round Trip Time (RTT) delay for access to applications on local branch servers, increasing application performance. It can also reduce unnecessary hair-pinning of traffic when accessing resources local to the branch. In the BYOD designs in this document, both of these wireless modes are implemented. Centralized wireless controller designs are presented for devices located within the campus and and FlexConnect designs are presented for devices at branch locations.

Figure 15 shows at a high level how both centralized and FlexConnect modes are implemented in this design.

Figure 15 Wireless Controller Designs



Wireless LAN Controller High Availability

High availability of the wireless network is becoming increasingly important as more devices with critical functions move to the wireless medium. Real-time audio, video, and text communication relies on the corporate wireless network and the expectation of no down time is becoming the norm. The negative impacts of wireless network outages are now just as impactful as outages of the wired network.

With Cisco's Wireless LAN Controller (WLC) 7.3 software release, the ability to have an active and hot-standby wireless controller has been introduced, allowing the Access Points (APs) to perform a rapid stateful switchover (SSO). This new capability allows all the AP sessions to statefully switch over to the hot-standby WLC with an identical configuration to the primary WLC. All unique configuration parameters and groupings specific to individual APs and AP groups are retained. An example of retained configuration is Flex-Connect grouping, which applies different restrictions and settings to sub-sets of APs based on branch location. Clients will be disassociated when a failover occurs. However, clients should automatically re-associate after the stateful switchover of the access point occurs.

The active and standby WLCs use a dedicated redundant interface to send keep-alives every 100 milliseconds, as well as sending configuration, operational data synchronization, and role negotiation information between them. The redundancy interface is a dedicated port that is directly connected

between WLCs by an Ethernet cable. For the WiSM2, a dedicated redundancy VLAN is used in place of the redundancy port. Failovers are triggered by loss of keep-alives as well as network faults. The active and standby WLCs share the same management IP address, with only the active being up until a failure occurs.

For more information, refer to the WLC High Availability Deployment Guide: http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bd3504.shtml.

Application Considerations

When implementing a BYOD solution, the applications that run on employee-owned devices need to be considered before selecting which of the particular BYOD use cases discussed above to deploy. The application requirements for these devices determine the level of network connectivity needed. The network connectivity requirements in turn influence the choice of the BYOD use case to apply.

Quality of Service

In addition to network connectivity, quality of service (QoS) is an important consideration for applications, especially those delivering real-time media. Device specific hardware, such as dedicated IP phones which sent only voice traffic, allowed for the configuration of dedicated voice wireless networks. However, with the widespread use of smartphones and tablets which support collaboration software (such as Cisco's Jabber client), devices are capable of sending voice, video, and data traffic simultaneously. Hence, QoS is necessary to provide the necessary per-hop behavior as such traffic traverses the network infrastructure.

QoS can be categorized into the following broad functions:

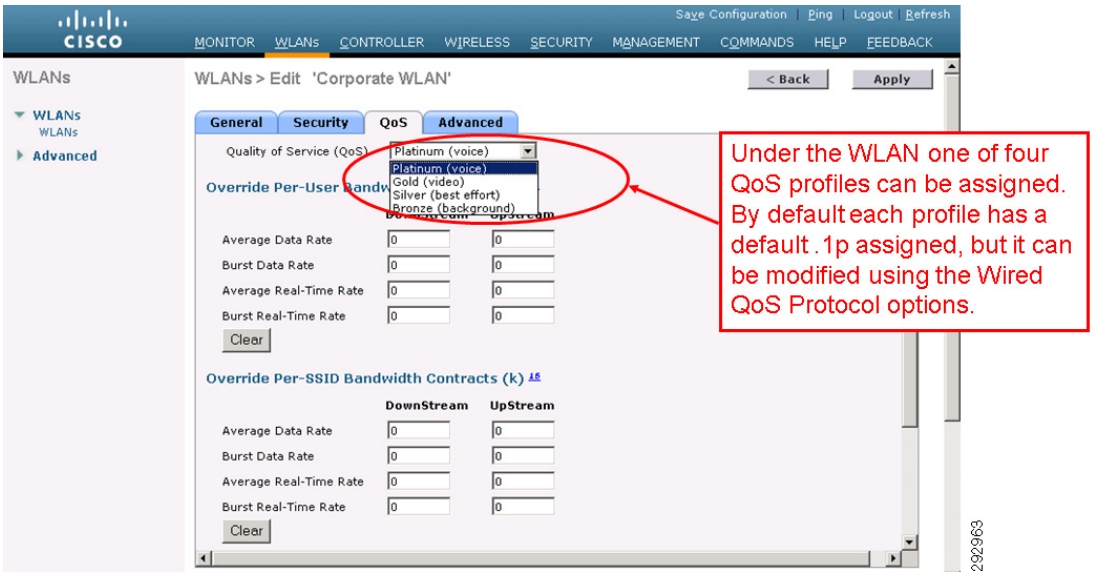
- Classification and Marking
- Bandwidth Allocation/Rate Limiting (Shaping and/or Policing)
- Trust Boundary Establishment
- Queueing

For a discussion regarding implementing wired QoS, refer to *Medianet Campus QoS Design 4.0* at: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html.

The following sections discuss various aspects of wireless QoS.

As of WLC software version 7.3, wireless QoS is configured by applying one of four QoS Profiles—Platinum, Gold, Silver, or Bronze—to the the WLAN to which a particular client device is associated. An example of the configuration is shown in Figure 16.

Figure 16 Application of a QoS Profile to a WLAN



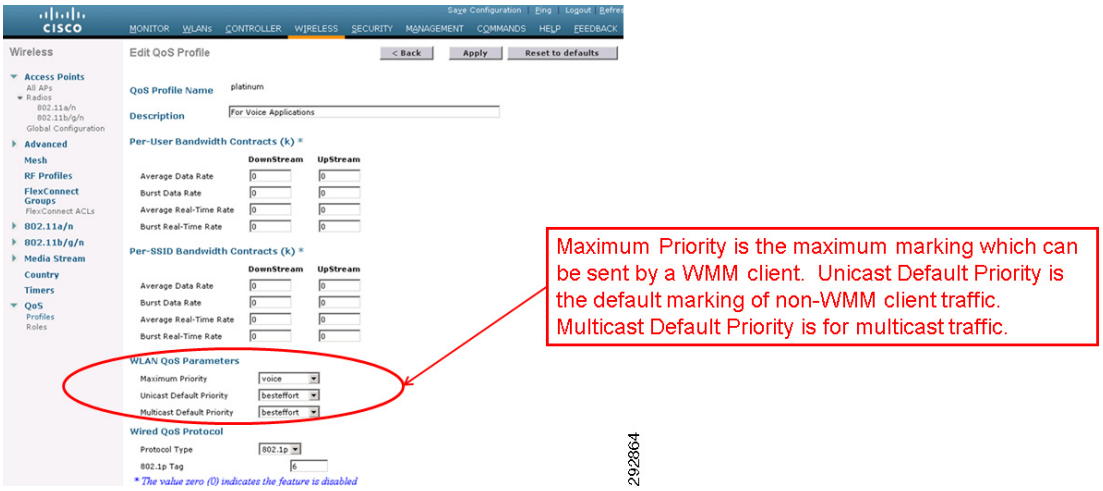
Note that the QoS settings for the profile can be overridden on a per-WLAN basis from within the QoS tab of the WLAN configuration.

The DSCP marking of client traffic, as it traverses the network within a CAPWAP tunnel, is controlled by three fields within the WLAN QoS Parameters field within the QoS Profile:

- Maximum Priority—This is the maximum 802.11 User Priority (UP) that a packet sent by a Wi-Fi Multimedia (WMM)-enabled client can send. The User Priority maps to a DSCP value within the outer header of the CAPWAP tunnel as the packet traverses the network infrastructure. If the WMM-enabled client sends an 802.11 packet with a User Priority higher than allowed, the wireless controller marks the packet down to the maximum allowed User Priority. This in turn maps to a DSCP of the external CAPWAP header as the packet is sent over the network infrastructure.
- Unicast Default Priority—This is the default 802.11 User Priority (UP) to which a unicast packet sent by a non-WMM-enabled client is assigned. This User Priority maps to a DSCP value within the outer header of the CAPWAP tunnel as the packet traverses the network infrastructure.
- Multicast Default Priority—This is the default 802.11 User Priority (UP) for for multicast traffic. This User Priority maps to a DSCP value within the outer header of the CAPWAP tunnel as the packet traverses the network infrastructure.

An example of the configuration of the WLAN QoS Parameters is shown in Figure 17.

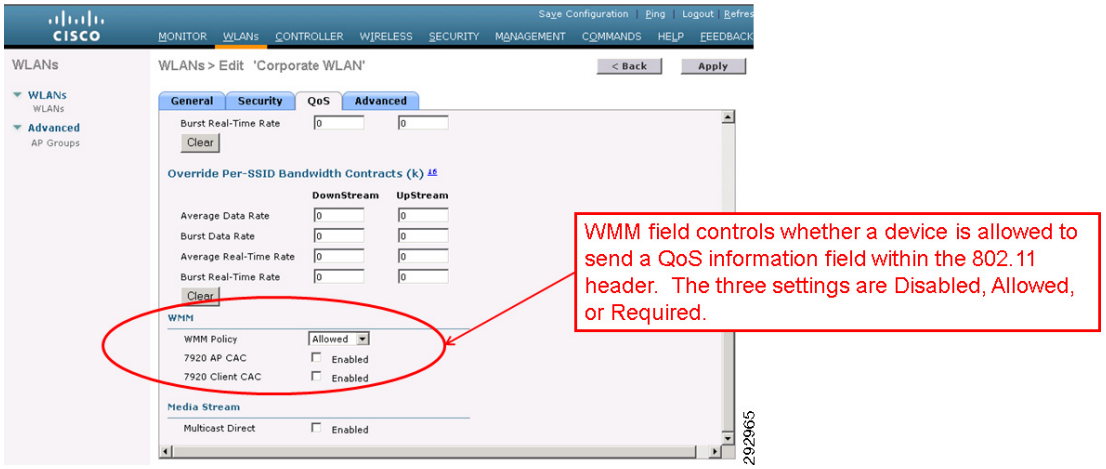
Figure 17 Controlling the Marking of Wireless Packets



It should be noted that this setting applies primarily to Local Mode (centralized wireless controller) designs and FlexConnect designs with central termination of traffic, since the WLAN QoS Parameters field results in the mapping of the 802.11 User Priority to the DSCP value within the outer header of the CAPWAP tunnel. The original DSCP marking of the packet sent by the wireless client is always preserved and applied as the packet is placed onto the Ethernet segment, whether that is at the wireless controller for centralized wireless controller designs or at the access point for Flexconnect designs with local termination.

The wireless trust boundary is established via the configuration of the WMM Policy within the QoS tab of the WLAN configuration. An example is shown in Figure 18.

Figure 18 Configuration of WMM Policy



The three possible settings for WMM Policy are:

- Disabled—The access point will not allow the use of QoS headers within 802.11 packets from WMM-enabled wireless clients on the WLAN.
- Allowed—The access point will allow the use of QoS headers within 802.11 packets from wireless clients on the WLAN. However, the access point will still allow non-WMM wireless clients (which do not include QoS headers) to associate to the access point for that particular WLAN.

- Required—The access point requires the use of QoS headers within 802.11 packets from wireless clients on the WALN. Hence, any non-WMM-enabled clients (which do not include QoS headers) will not be allowed to associate to the access point for that particular WLAN.

Note Where possible, it is advisable to configure WMM policy to Required. Some mobile devices may incorrectly mark traffic from collaboration applications when the WMM policy is set to Allowed versus Required. Note however that this requires all devices on the WLAN to support WMM before being allowed onto the WLAN. Before changing the WMM policy to Required, the network administrator should verify that all devices which utilize the WLAN are WMM-enabled. Otherwise, non-WMM-enabled devices will not be able to access the WLAN.

The configuration of the WMM Policy, along with the WLAN QoS Parameters, together create the wireless QoS trust boundary and determine the marking of wireless traffic within the CAPWAP tunnel as it traverses the network infrastructure.

Rate Limiting

One additional option to prevent the wireless medium from becoming saturated, causing excessive latency and loss of traffic, is rate limiting. Rate limiting may be implemented per device or per SSID to prevent individual devices from using too much bandwidth and negatively impacting other devices and applications. Rate limiting is particularly useful for guest access implementations and is discussed in detail in BYOD Guest Wireless Access.

Cisco Jabber

Cisco's Jabber clients are unified communications (UC) applications that are available for Android and Apple mobile devices as well as Microsoft Windows and Apple Mac computers. These client applications provide instant messaging (IM), presence, voice, video, and visual voicemail features. These features require that the employee-owned device is allowed to establish call signaling flows between the device itself and the corporate Cisco Unified Communications Manager (Unified CM) server, typically deployed within the campus data center. Note that the Basic Access use case discussed above terminates employee-owned devices on a DMZ segment off of the Internet Edge firewall. Cisco Jabber requires only Internet access to access WebEx cloud-based services like IM, meetings, and point-to-point voice and video calls. However, to deliver these same services with on-premise corporate assets such as Unified CM and other back-end UC applications, connectivity through the firewall is required for Jabber features to function. In addition to signaling, media flows also need to be allowed between the Jabber client and other IP voice and video endpoints, such as corporate IP phones deployed throughout the corporate network. This requires the network administrator to allow a range of addresses and ports inbound from the DMZ segment through the Internet Edge firewall. Given these connectivity considerations for real time communications and collaboration, the network administrator may instead decide to implement the Enhanced Access use case discussed above. With this BYOD model, the employee-owned devices are on-boarded (registered with the Cisco ISE server and provisioned with digital certificates) and terminated on the inside of the corporate network. This requires no modifications to the Internet Edge firewall, and potentially fewer security concerns.

For more information on Cisco Jabber, see Cisco Jabber Clients and the Cisco BYOD Infrastructure.

Mobile Device and Application Management

There are a wide range of third-party tools for mobile device management (MDM) and mobile application management (MAM) that allow IT to set device policy in the same way that ISE sets network policy. An MDM can set device use policies such as encrypted storage or pin lock requirements. They can also provision built-in applications. In addition, they can gather metrics on the device not typically found on laptops and desktops. Finally, MDMs can track the location of devices, wipe the devices over the air, and disable the use of features such as the camera and audio recorder. All of this is possible without installing client software on the end device. 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 black listed application is active or the device has been rooted or jailbroken.

Mobile Application Managers (MAM) can distribute software from public application stores or in house applications from private application servers. In some situations, the MAM can provision the application in the same way that an MDM can provision built-in applications. Almost all full-featured MDMs include a MAM function. These tools take a device-centric approach to management and will be covered in future versions of this document. By contrast, ISE is a network-centric approach to device management. Each method has merit and they are not mutually exclusive. Customers may choose to deploy both an MDM and ISE solution in parallel. In this situation, the tools are autonomous and independent of one another. To be effective, a consistent policy should be in effect at both the network and device level. For example, if a MAM is distributing Jabber to mobile devices, the network policy should allow these devices to use Jabber over the network. On the other hand, if cloud storage is blacklisted on corporate issued mobile devices, then the WLAN ACL should not allow packets to reach the cloud storage servers. Providing crisp and distinct classifications such as Full Access, Limited Access, and Basic access will simplify developing a consistent use policy for both network and device.

License Requirements for BYOD Solution

Cisco ISE comes with several license options, such as Evaluation, Base, Advanced, and Wireless. For this design to be implemented, ISE requires the Advanced license option. To obtain more information on licensing, see:
http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Configuring the Infrastructure

This section discusses the different Infrastructure components that are critical to the deployment of the BYOD design. Infrastructure components that are discussed in this section are:

- Wireless Controllers
- Access Layer Switches
- Identity Service Engine
- Certification Authority (CA) server

This section discusses how to configure these components such that the rest of the sections can rely on these components for deploying different use cases.

Wireless Infrastructure

The wireless controller (WLC) is used to automate wireless configuration and management functions and to provide visibility and control of the wireless networks. The WLC is able to interact with the Identity Service Engine. Together, they enforce authentication and authorization policies across endpoints.

While designing the WLAN networks, take the following into consideration:

- The role of the WLAN
- The authentication mechanism for the WLAN
- The number of WLANs present in a network

This design guide logically separates the WLAN into distinct logical functions, provisioning and network access. These two functions can be provided by two different WLANs or combined into one WLAN. This design guide covers both single and dual SSID deployment models for both the branch location and the campus. Note that wireless guest access is implemented on a different WLAN as well.

Some considerations when selecting a single versus dual SSID configuration:

- Some organizations prefer having a dedicated SSID for on-boarding devices.
- Others see dual SSID as an extra management burden.
- A second SSID adds channel overhead.
- Enabling too many SSIDs may degrade wireless performance.

The organization's unique requirements and preferences will dictate which model to deploy. The ISE and WLC configurations may easily be changed to support either option.

Branch Wireless LAN Design—FlexConnect

Clients connecting from the branch locations are managed by a cluster of Flex 7500 Wireless Controllers or Virtual Wireless LAN Controllers (vWLCs). The vWLC is software which can run on industry standard virtualization infrastructure and is more suitable for small- and medium-sized businesses. The configuration parameters described in this section apply to both the vWLC and Flex 7500 controllers.

For information on how to set up vWLCs using VMware and supported features, see: http://www.cisco.com/en/US/partner/products/ps12723/products_tech_note09186a0080bd2d04.shtml.

FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

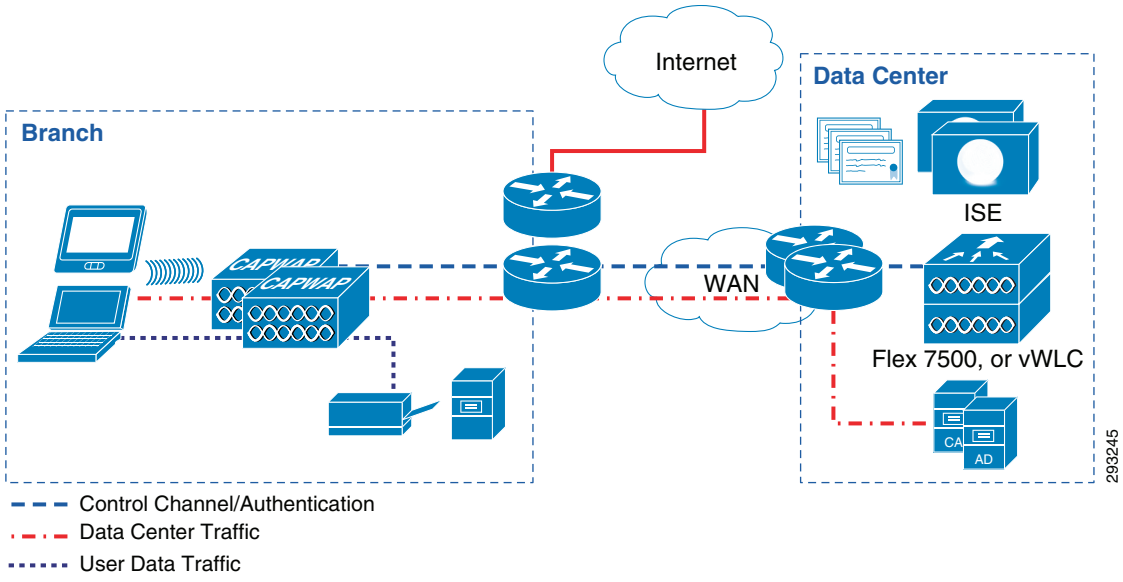
When they are connected to the controller, they can also send traffic back to the controller. In the connected mode, the FlexConnect access point can also perform local authentication.

Distributing client data traffic using the FlexConnect architecture offers some advantages:

- A controller is not required at each branch location
- Mobility resiliency within branch during WAN link failures
- Central management and troubleshooting

The FlexConnect architecture shown in Figure 19 shows several different traffic flows originating at the branch.

Figure 19 FlexConnect Architecture



When an endpoint associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration.

With respect to data packet flows, the WLAN can be in any one of the following modes:

- Central switching—Central switched WLANs tunnel both the wireless user traffic and all control traffic to the centralized WLC, where the user traffic is mapped to a dynamic interface or VLAN.
- Local switching—In this mode the FlexConnect access point switches data packets locally by dropping all client data locally at the wired interface. Wireless user traffic is mapped to discrete VLANs via 802.1Q trunking.

The Flex 7500 Wireless Branch Controller Deployment Guide offers more details: http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml#override

As mentioned in Design Overview, the key strategy for providing differentiated access to users is done by assigning users to different VLANs dynamically. To implement this requirement, a feature called AAA overrides for FlexConnect is used. This feature allows VLANs to be dynamically assigned to an SSID. To implement this feature, one of the requirements is to pre-configure the access point with all of the possible VLANs that can be returned by the AAA server. The VLAN assignment that is returned by ISE, as part of authorization, is applied. In this design three VLANs have been chosen for wireless connectivity on the BYOD_Employee SSID.

Table 4 illustrates those VLANs and the purpose of each.

Table 4 VLANs and Purpose

VLAN Number	VLAN Name	Description
10	Wireless_Full	Users assigned to this VLAN get full access to campus and branch servers.
11	Wireless_Partial	Users assigned to this VLAN get only partial access to campus and branch servers.

Table 4 VLANs and Purpose

VLAN Number	VLAN Name	Description
12	Wireless_Internet	Users assigned to this VLAN get only Internet access.
18	AP_Mgmt_Flex	This is the native VLAN that the user will initially be placed into, until the authorization policy determines the appropriate VLAN.

Since more than one VLAN is configured for local switching, FlexConnect APs at the branch must be connected to an 802.1Q trunk link. Both the AP and the upstream switchport need to be configured for 802.1Q trunking. The following is an example configuration of the access layer switch which connects to the FlexConnect AP:

```
interface GigabitEthernet1/0/3
 description to Branch #1 AP
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 10-18
 switchport mode trunk
 spanning-tree portfast trunk
```

Branch Wireless IP Address Design

Each VLAN defined above is designed such that when a user associates to a SSID which is mapped to a VLAN, then the user gets a unique subnet. To implement this behavior, the branch router is configured with Layer 3 subinterfaces. These subinterfaces are configured with the ip-helper address pointing to a DHCP server. The DHCP server can be located at the campus location or within the branch. For the purposes of this guide, the DHCP server was located at the branch. The following example configuration implements this:

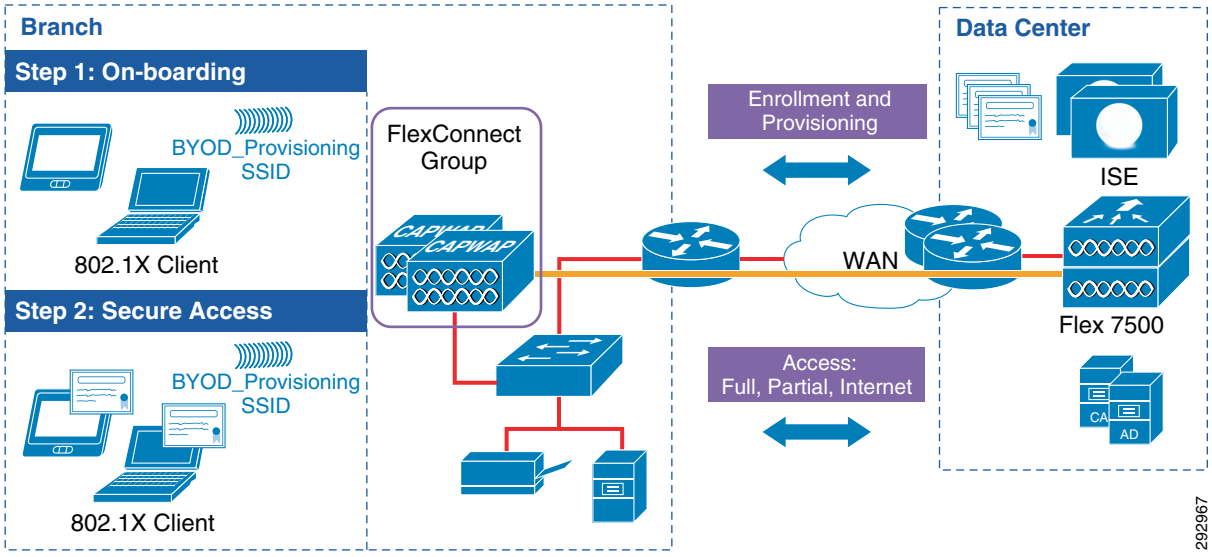
```
interface GigabitEthernet0/1
 description Trunk to branch bn22-3750x-1
 no ip address
 media-type sfp
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.200.10.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 10 ip 10.200.10.1
 standby 10 priority 110
 standby 10 preempt
!
interface GigabitEthernet0/1.11
 encapsulation dot1Q 11
 ip address 10.200.11.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 11 ip 10.200.11.1
 standby 11 priority 110
 standby 11 preempt
!
interface GigabitEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.200.12.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 12 ip 10.200.12.1
 standby 12 priority 110
 standby 12 preempt
```

Branch—Dual SSID Design

Two SSIDs are used in this design: one provides enrollment/provisioning and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides secure network access.

Figure 20 shows the dual SSID design for the branch APs.

Figure 20 Branch—Dual SSIDs



In a dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID.
- After the user is provisioned, it is assumed that they will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list that provides access only to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of this SSID are discussed in Client Provisioning.
- For the purpose of this design guide, the following two SSIDs are used: BYOD_Provisioning and BYOD_Employee.

The properties of these two SSIDs are highlighted in Table 5.

Table 5 WLAN Parameters

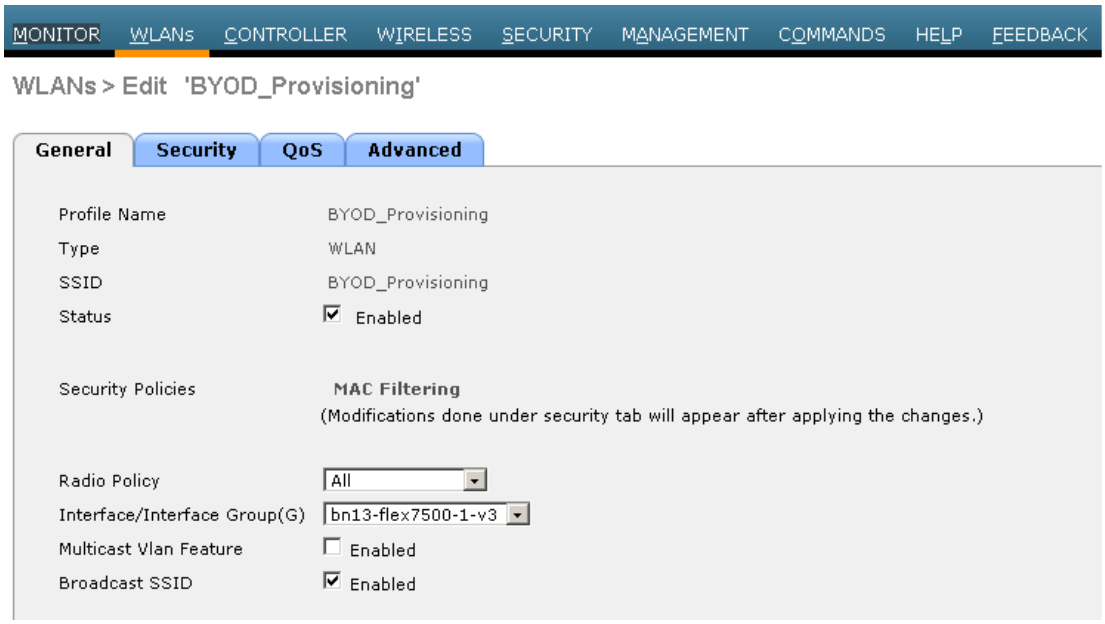
Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used only for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None	WPA+WPA2
MAC Filtering	Enabled	Disabled
WPA+WPA2 Parameters	None	WPA2 Policy, AES, 802.1X

Table 5 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Layer 3 Security	None	None
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State—RADIUS NAC	NAC State—RADIUS NAC
Advanced—FlexConnect Local Switching	Disabled for Central Switching Provisioning Enabled for Local Switching Provisioning	Enabled

To create a WLAN, click **WLANs > Create New > Go** and provide the SSID and profile details. Figure 21 shows the general configuration details of the BYOD_Provisioning SSID.

Figure 21 Creating the Branch BYOD_Provisioning SSID



The Layer 2 security settings are configured as **None** because BYOD_PROVISIONING is an open SSID. If the provisioning SSID is to be password protected, then the Layer 2 security settings must be configured as WPA+WPA2 Enterprise.

Figure 22 Layer 2 Security Settings

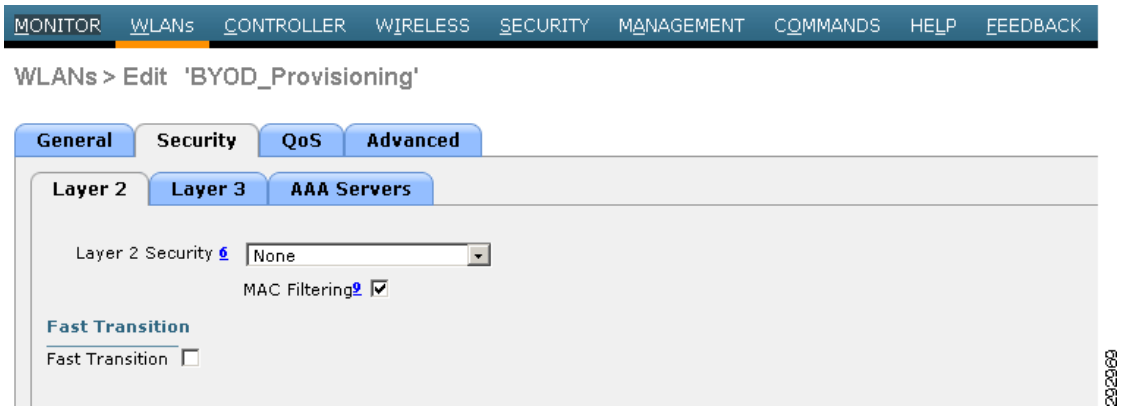
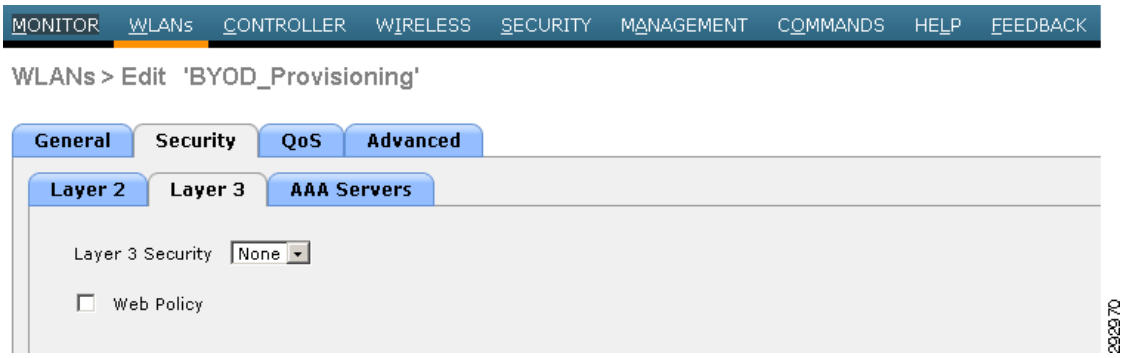
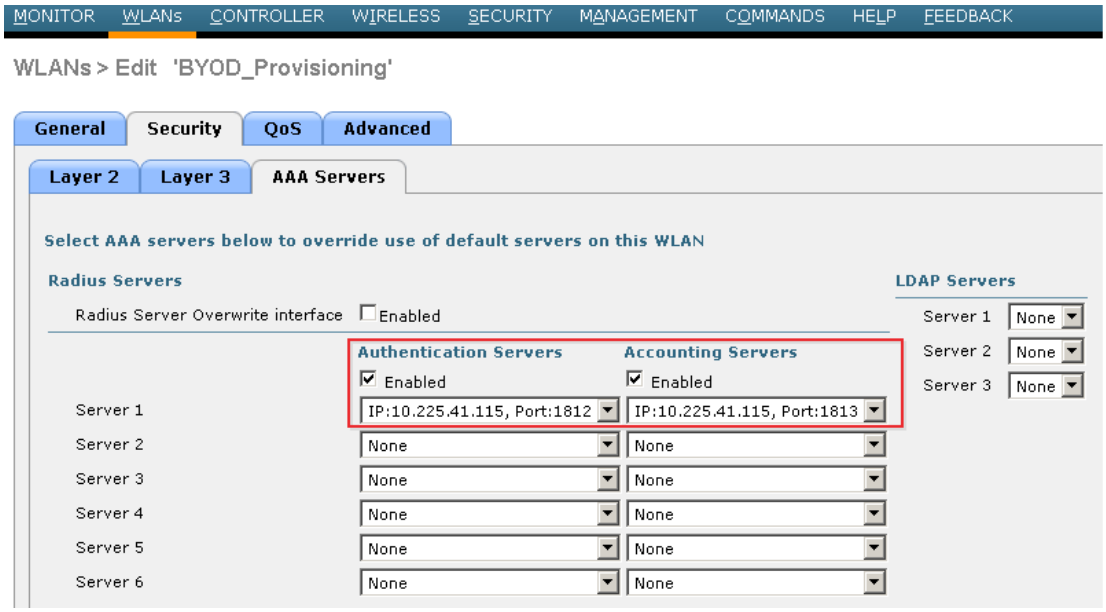


Figure 23 Layer 3 Security Settings



The main configuration in the security settings is to specify the RADIUS server configuration details. Figure 24 shows how the ISE's IP address is configured for Authentication and Authorization.

Figure 24 AAA Security Settings



Within the dual SSID deployment there are two possible ways to direct provisioning traffic:

- From the campus or data center—The endpoint receives an IP address from the data center and the provisioning traffic is directed through the CAPWAPP tunnel between the branch and the Flex 7500 controller.
- At the branch—The endpoint receives an IP address from the branch and the provisioning traffic uses the switching and WAN infrastructure for connectivity to data center resources.

Dual SSID—Central Switching Provisioning

Figure 25 shows how with central switching provisioning, the endpoint communicates with ISE and data center resources using the CAPWAP tunnel.

Figure 25 Central Switching Provisioning

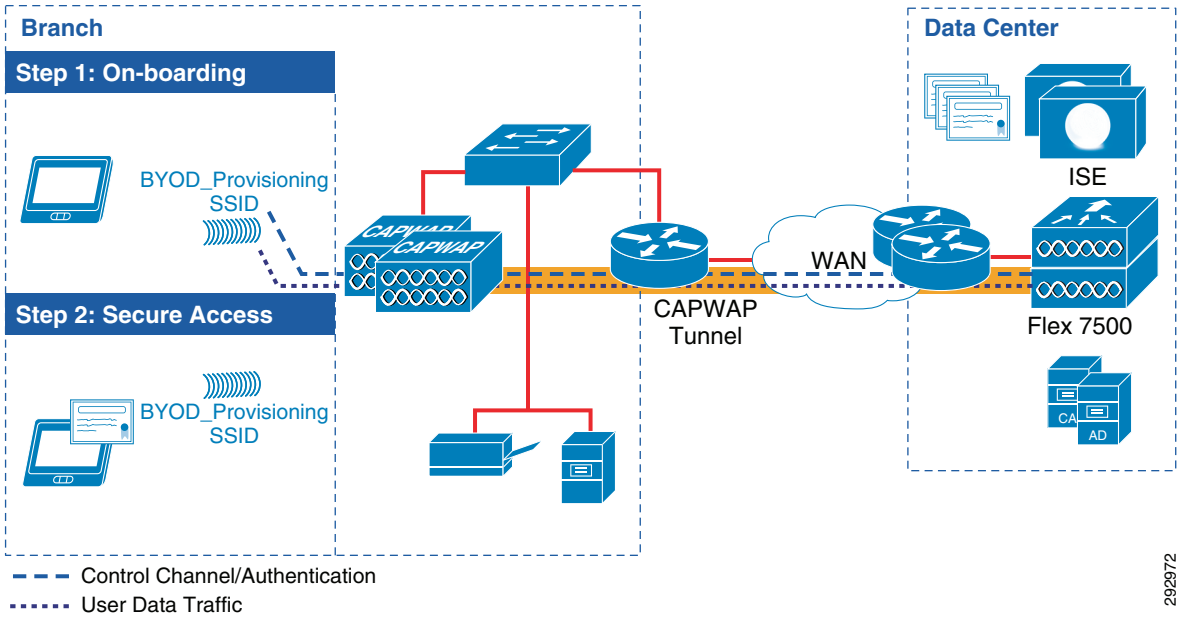
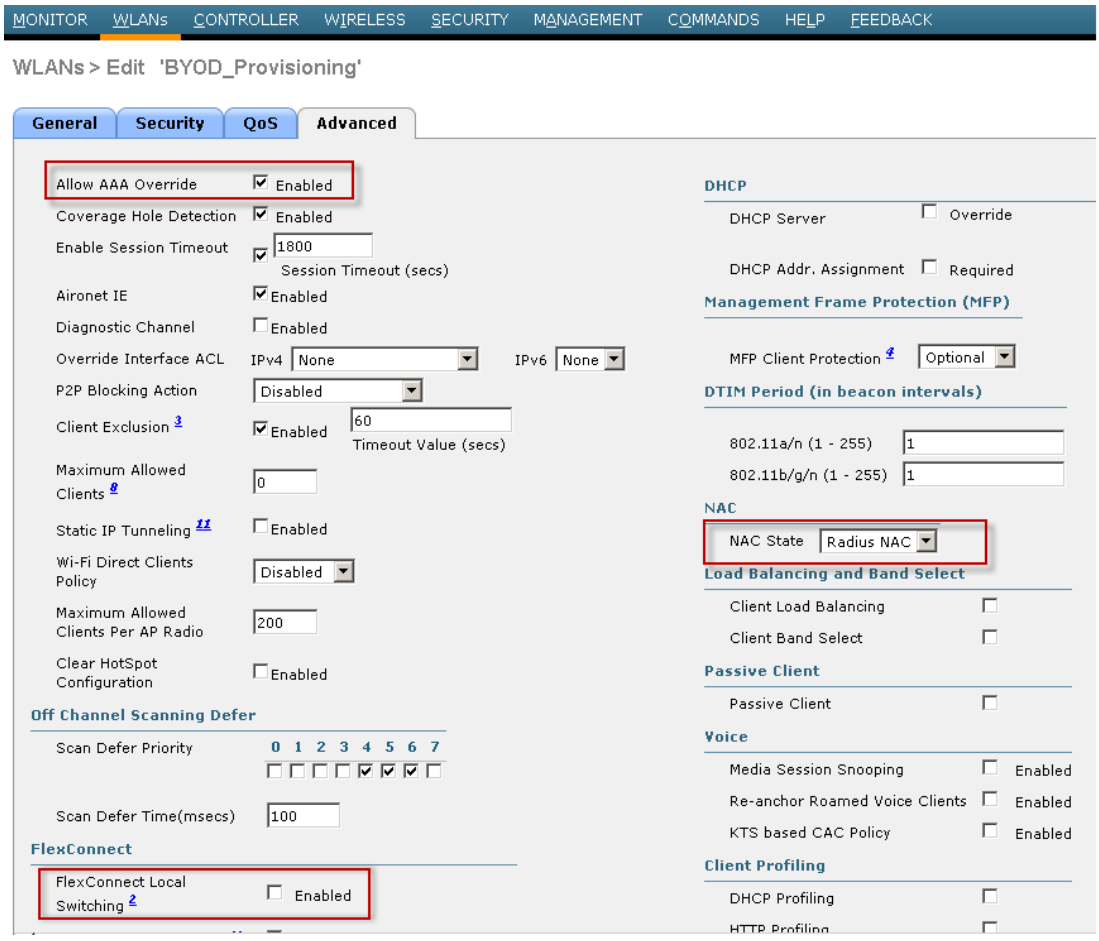


Figure 26 shows the advanced settings for BYOD_Provisioning, including the AAA Override and NAC State. The FlexConnect Local Switching setting is disabled for central switching provisioning.

Figure 26 Advanced Settings for Local Switching Provisioning



Dual SSID—Local Switching Provisioning

Figure 27 shows provisioning with local switching mode. The user data traffic is sent to the switch interface and the endpoint relies on the normal router/WAN infrastructure to reach the ISE and data center resources.

Figure 27 Local Switching Provisioning

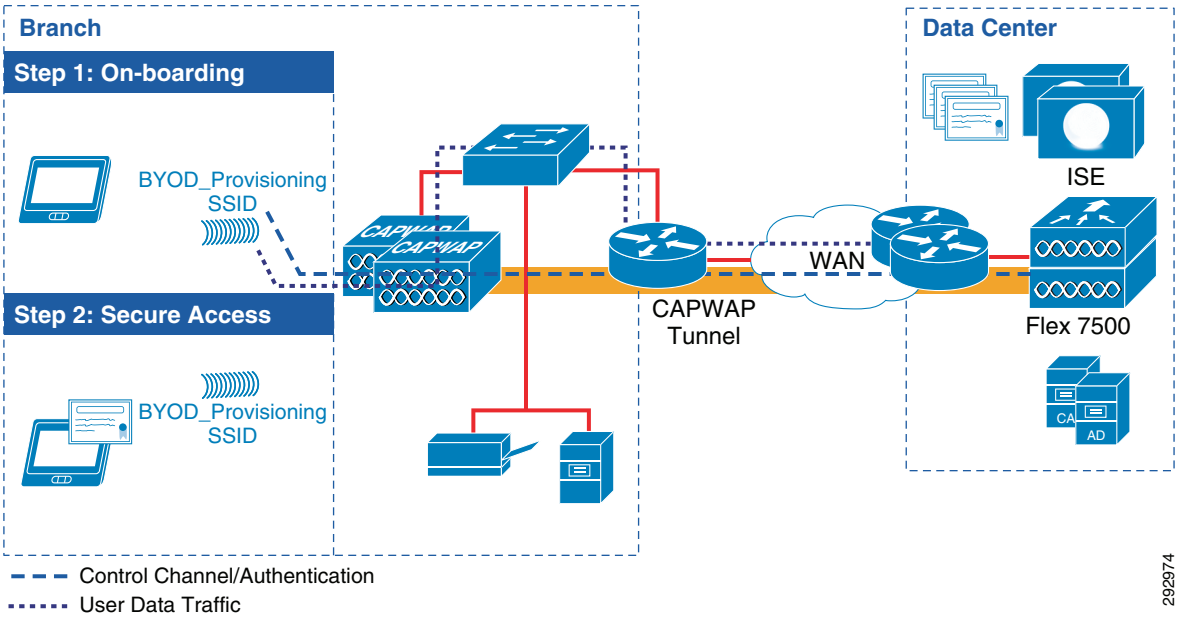
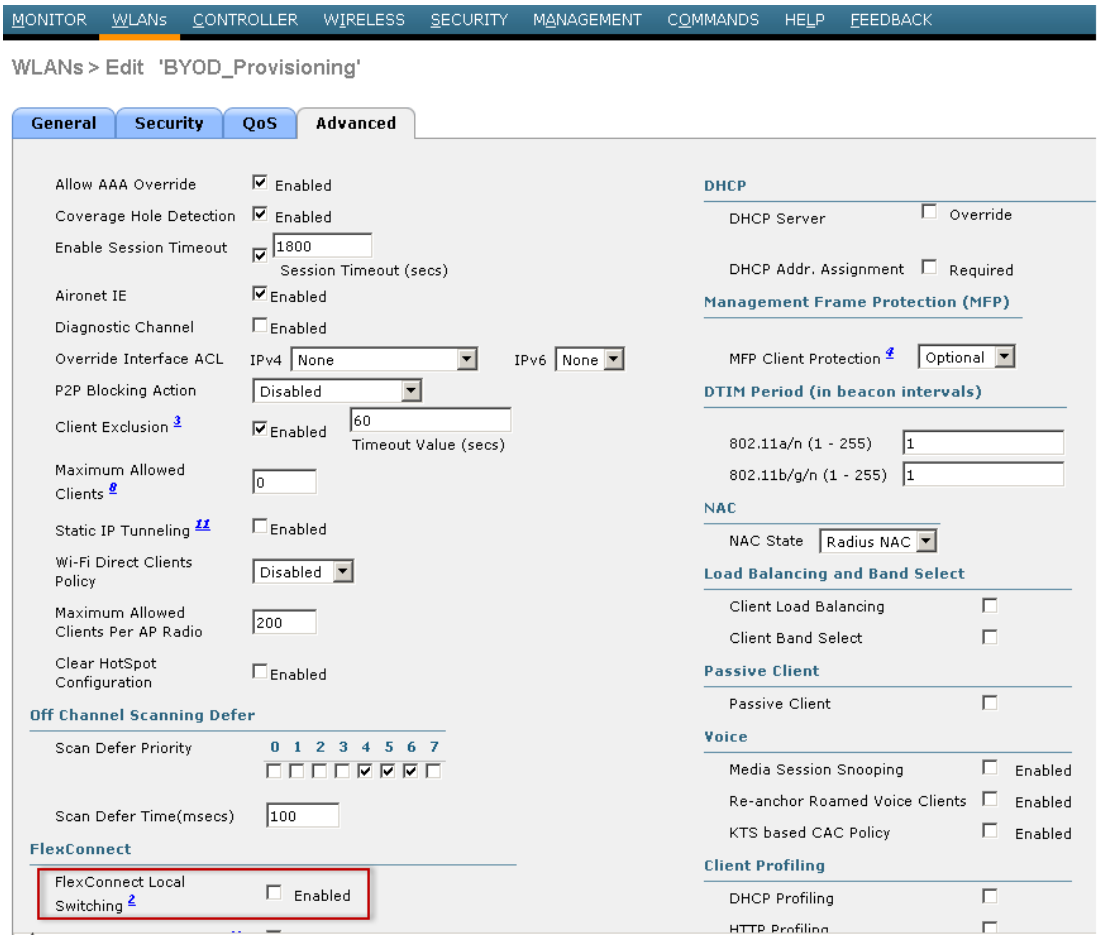


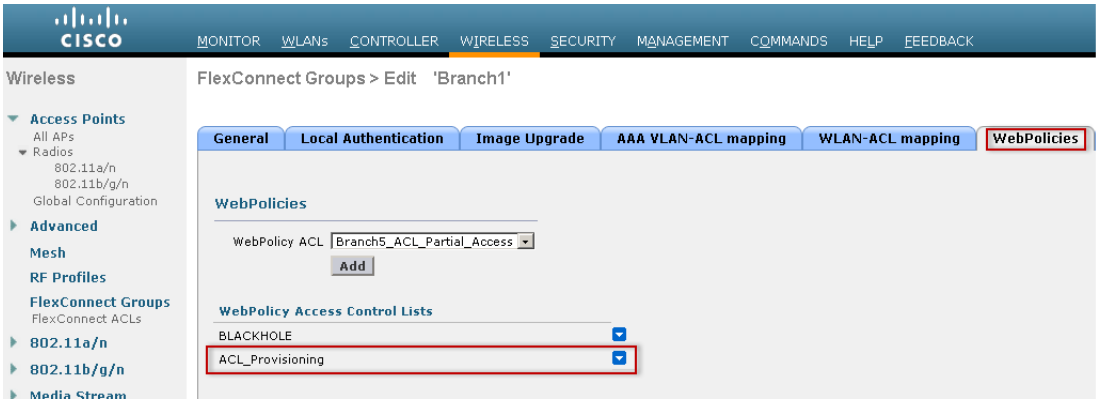
Figure 28 shows the advanced settings for BYOD_Provisioning, including the AAA Override and NAC State. The FlexConnect Local Switching is enabled for local switching provisioning.

Figure 28 Advanced Settings for Local Switching Provisioning



To enforce the redirection to the self-registration portal, a FlexConnect ACL is defined under the WebPolicies tab, as shown in Figure 29.

Figure 29 WebPolicies for FlexConnect Group



The ACL_Provisioning FlexConnect ACL shown in Figure 30 allows access to ISE, DNS, the Google Play Store, and denies all other traffic. Android devices require access to the Google Play Store to download the SPW package.

Figure 30 ACL_Provisioning FlexConnect ACL

General

Access List Name ACL_Provisioning

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.46	/ 255.255.255.255	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.41.114	/ 255.255.255.255	Any	Any	Any
4	Permit	0.0.0.0	/ 0.0.0.0	10.225.41.115	/ 255.255.255.255	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	173.194.0.0	/ 255.255.0.0	Any	Any	Any
6	Permit	0.0.0.0	/ 0.0.0.0	74.125.0.0	/ 255.255.0.0	Any	Any	Any
7	Permit	0.0.0.0	/ 0.0.0.0	206.111.0.0	/ 255.255.0.0	Any	Any	Any
8	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

292977

The following is a detailed explanation of the ACE entries shown above:

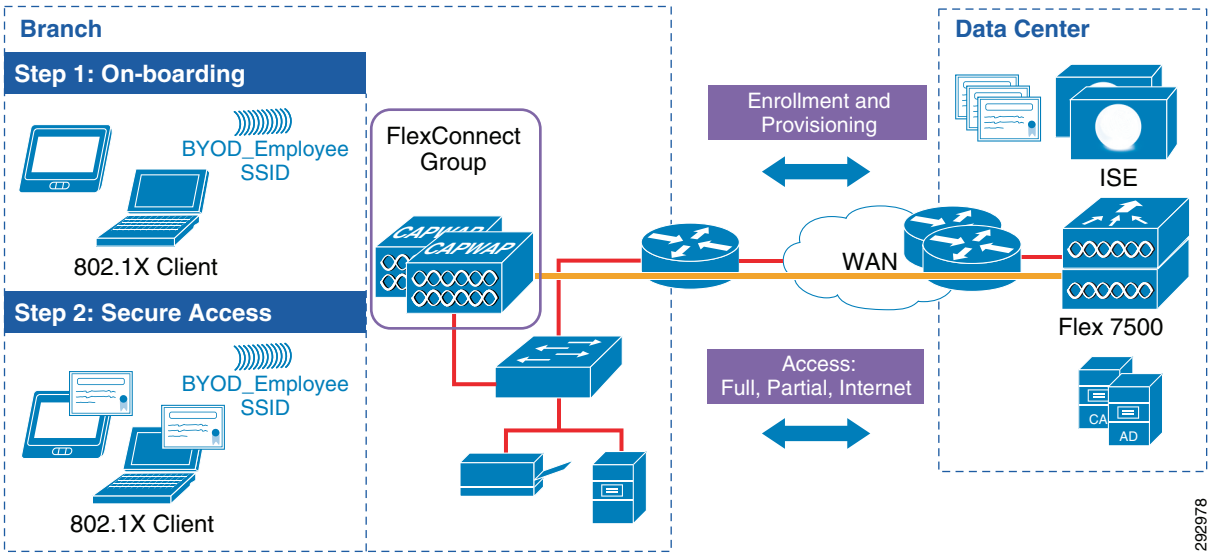
- 10.225.41.114, 10.225.41.115 are IP addresses of ISE.
- 173.194.0.0, 74.125.0.0 are subnets that allow access to Google Play Store.

Note The purpose of the ACL shown below is to provide an example that network administrators can use to deploy in the network. The Google Play store changes their addresses, so it is advisable to validate the Google Play store addresses before deploying this ACL.

Branch—Single SSID Design

In a single SSID design, the same WLAN is used for certificate enrollment, provisioning (on-boarding process), and secure network access. Figure 31 shows how this design may be implemented using the 7500 Flex Controller cluster, which is dedicated to manage the APs in the branch locations.

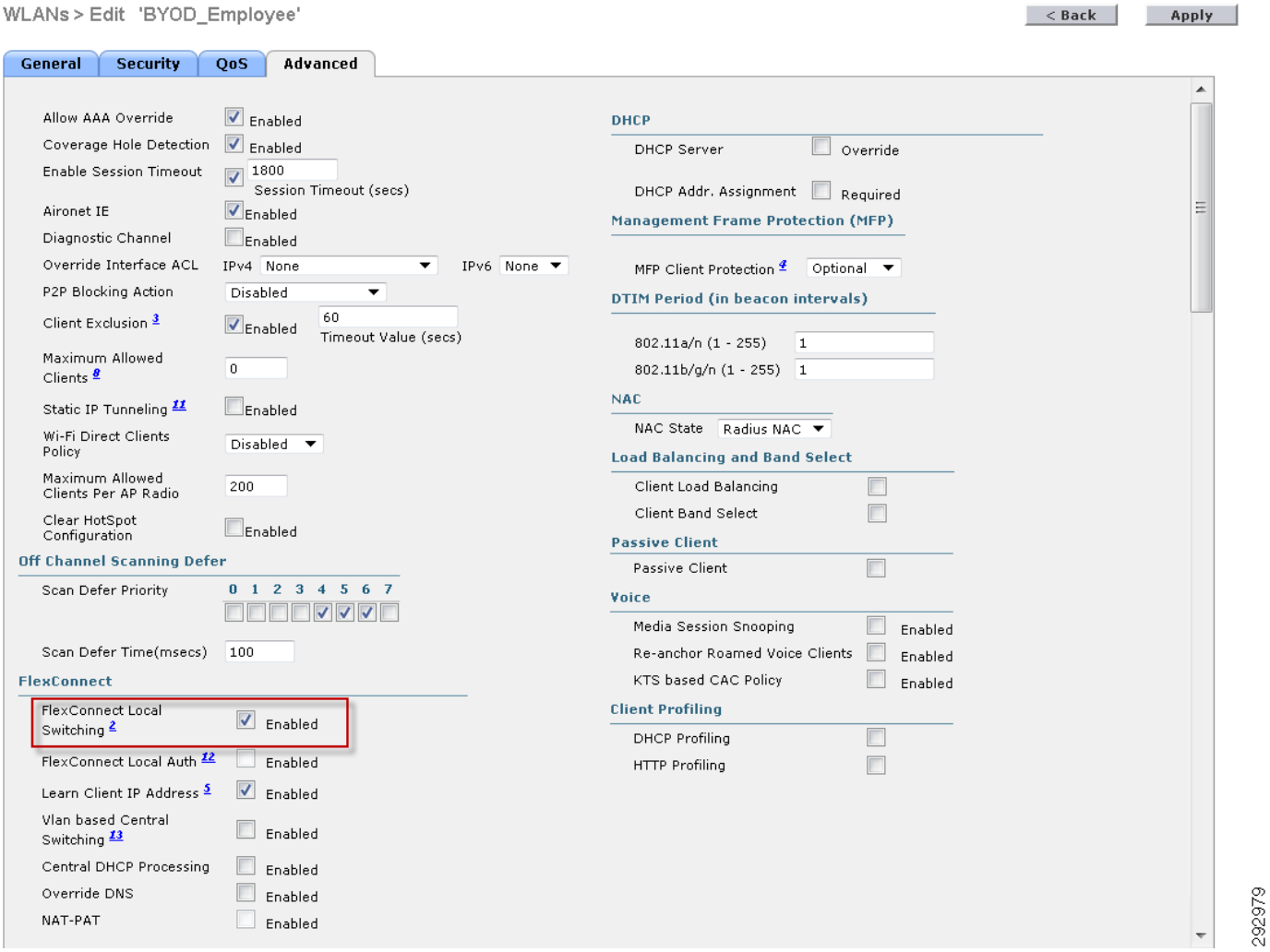
Figure 31 Branch—Single SSID



In this scenario the APs associate with the Flex 7500 controller and the FlexConnect capabilities allow the on-boarding and secure access capabilities to be handled by the single BYOD_Employee SSID.

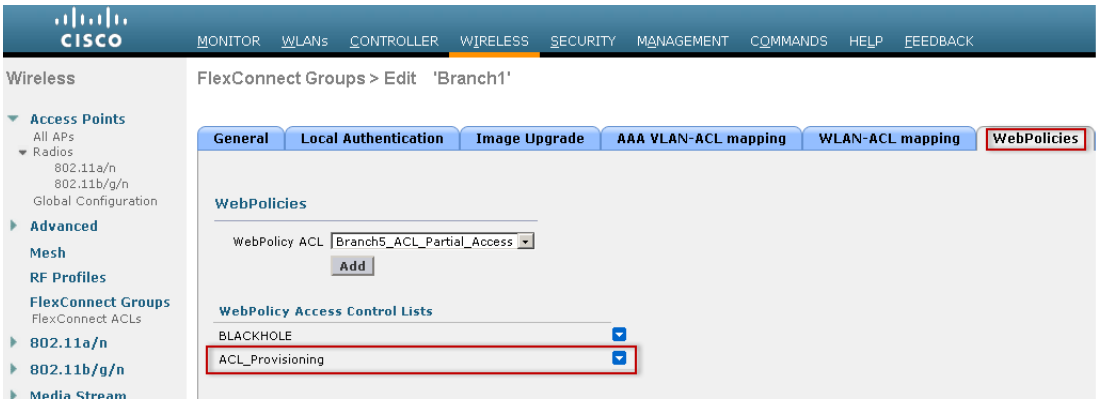
The steps to configure the BYOD_Employee WLAN are similar, following the parameters outlined in Table 5. It is important to note that FlexConnect Local Switching is enabled on the BYOD_Employee WLAN, as highlighted in Figure 32.

Figure 32 FlexConnect Local Switching



To enforce the redirection to the self-registration portal, a FlexConnect ACL is defined under the WebPolicies tab, as shown in Figure 33.

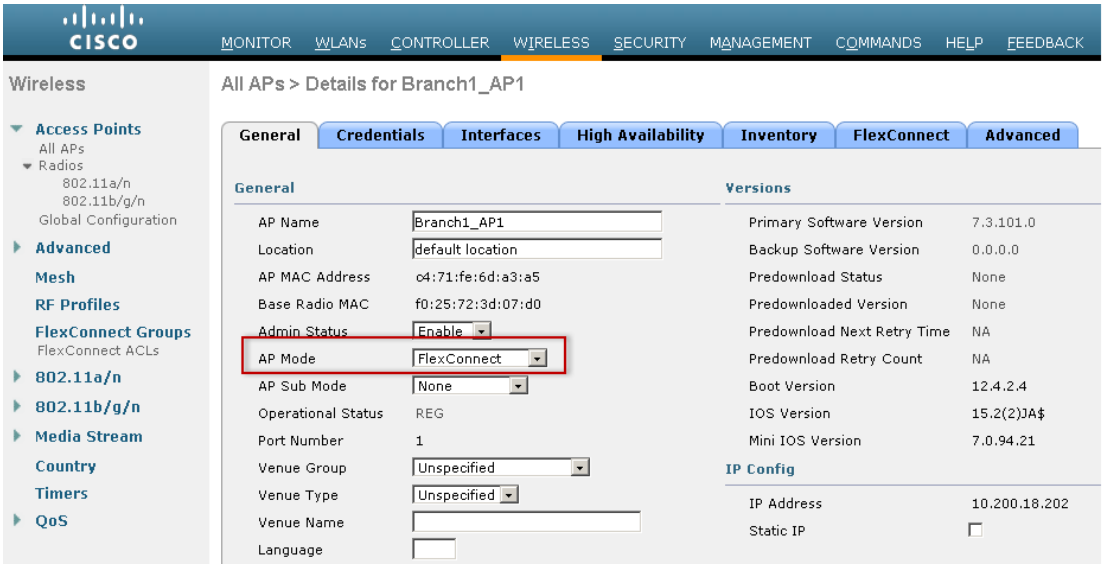
Figure 33 WebPolicies for FlexConnect Group



FlexConnect Access Point Configuration

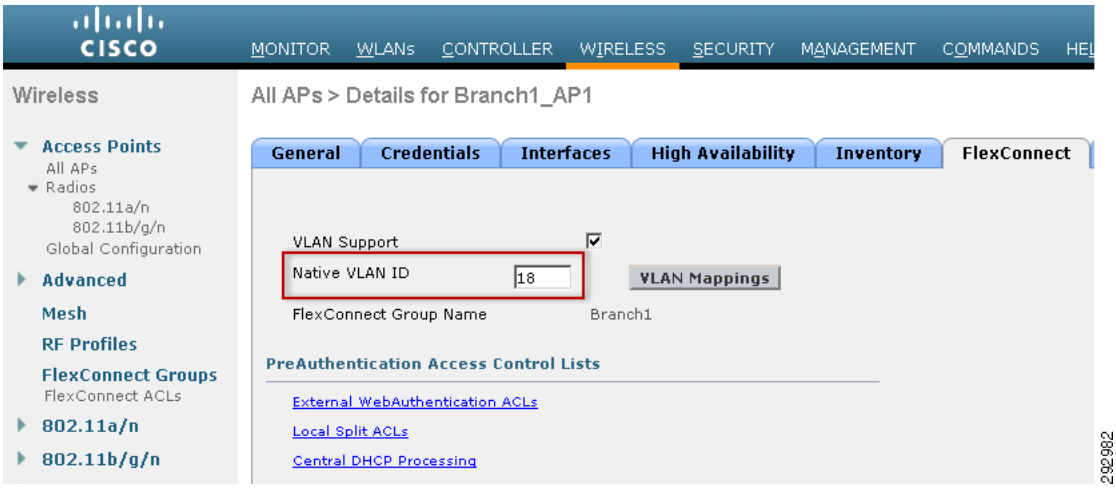
Configure the Access Point in FlexConnect mode by changing the AP Mode to FlexConnect. Click **Wireless > Access Points** and select the proper branch AP. Figure 34 shows this setting.

Figure 34 FlexConnect AP Mode



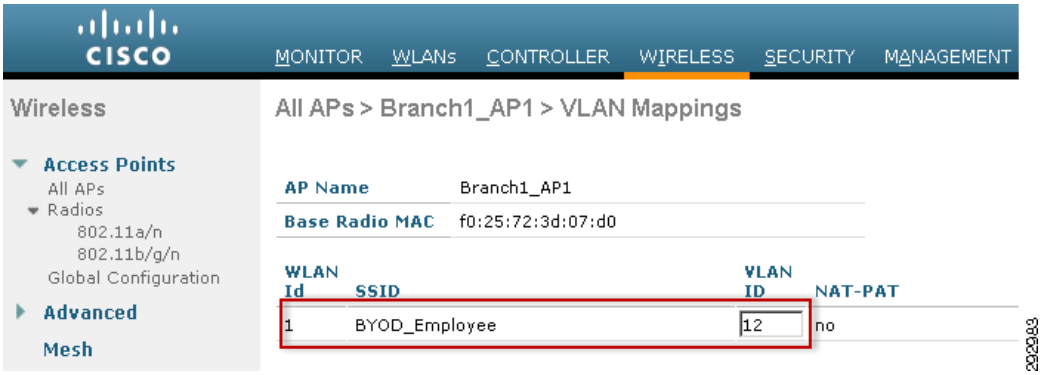
Click the **FlexConnect** tab and specify the Native VLAN for the branch, as shown in Figure 35. The access point relies on the native VLAN for IP connectivity.

Figure 35 Native VLAN ID



Define the VLAN ID to be used for local switching. In Figure 36, clients obtain an IP address from VLAN 12 (Internet access) when doing local switching. When using the AAA Overrides for FlexConnect feature, the client is moved to a different VLAN dynamically, based on the matched authorization profile and will obtain an IP address from the defined VLAN.

Figure 36 BYOD_Employee VLAN ID



FlexConnect Groups

FlexConnect groups provide a convenient way to group access points that share the same configuration settings. This is particularly helpful when grouping several FlexConnect access points in remote or branch locations. Instead of configuring each access point separately, FlexConnect groups allow the configuration parameters to be applied to all access points at once. For example, a FlexConnect ACL can be applied to a particular VLAN across all access points within a branch simply by adding the access points to the same FlexConnect group.

For the purpose of this guide, a unique FlexConnect group was defined for each branch, as shown in Figure 37.

Figure 37 FlexConnect Groups

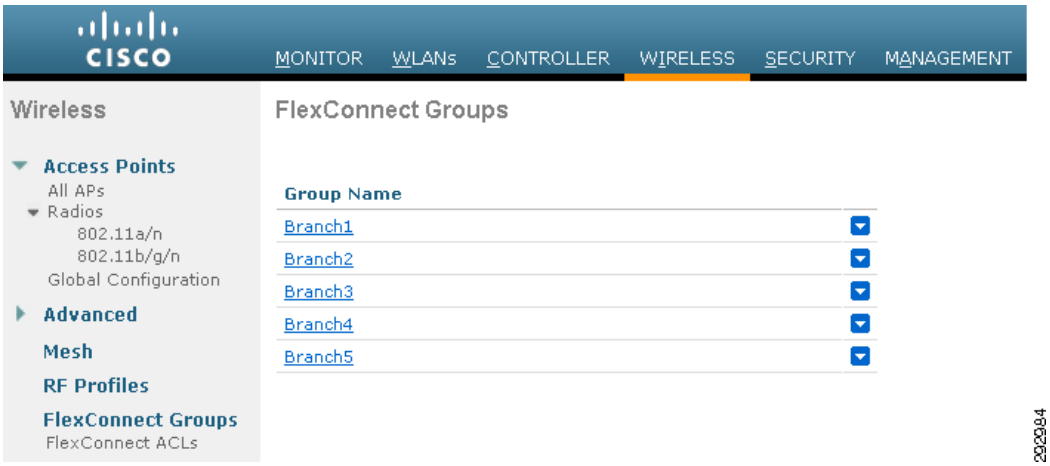
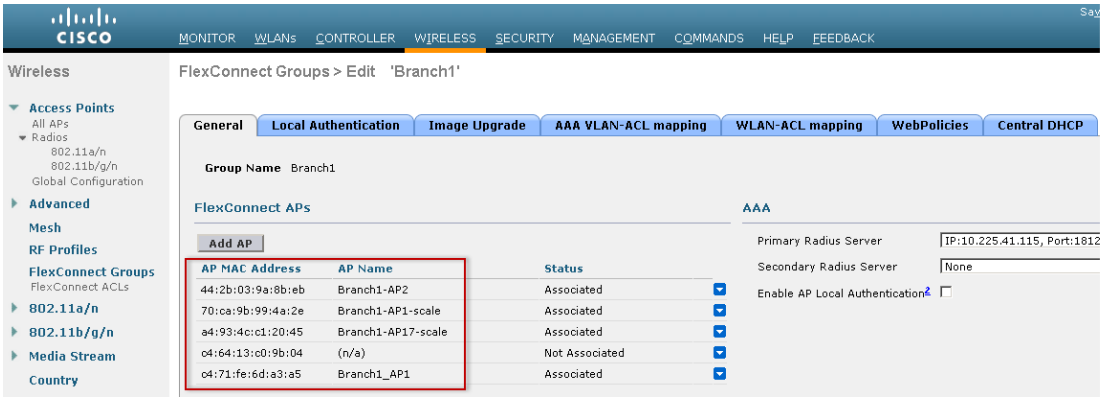


Figure 38 shows the access points that have been added to the Branch1 FlexConnect group.

Figure 38 Branch1 FlexConnect Group

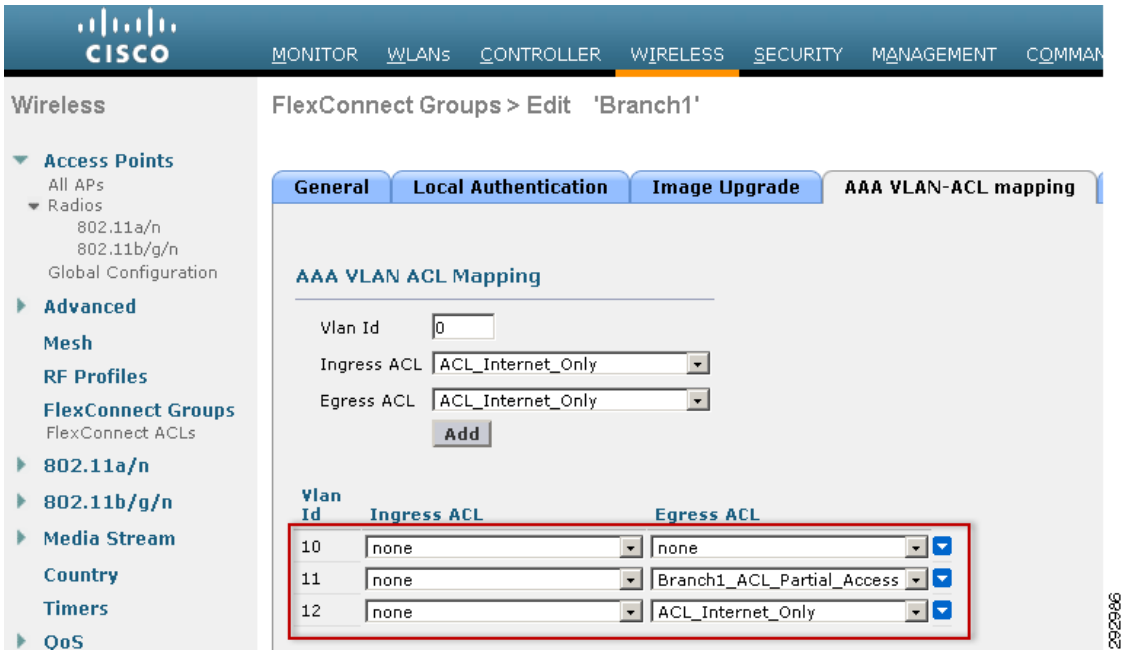


Before ISE can enforce an authorization policy, FlexConnect ACLs must be defined and assigned to each VLAN. By clicking the AAA VLAN-ACL mapping tab, the FlexConnect ACL may be enforced for each VLAN ID. This assumes that every branch location shares the same VLAN ID numbers:

- VLAN 10 for full access
- VLAN 11 for partial access
- VLAN 12 for Internet only access

Figure 39 shows how the different FlexConnect ACLs have been mapped to each VLAN.

Figure 39 VLAN-ACL Mapping



The FlexConnect ACLS shown in Figure 40 and Figure 41 are explained in more detail in Enhanced BYOD Access.

Figure 40 Branch1_ACL_Partial_Access FlexConnect ACL

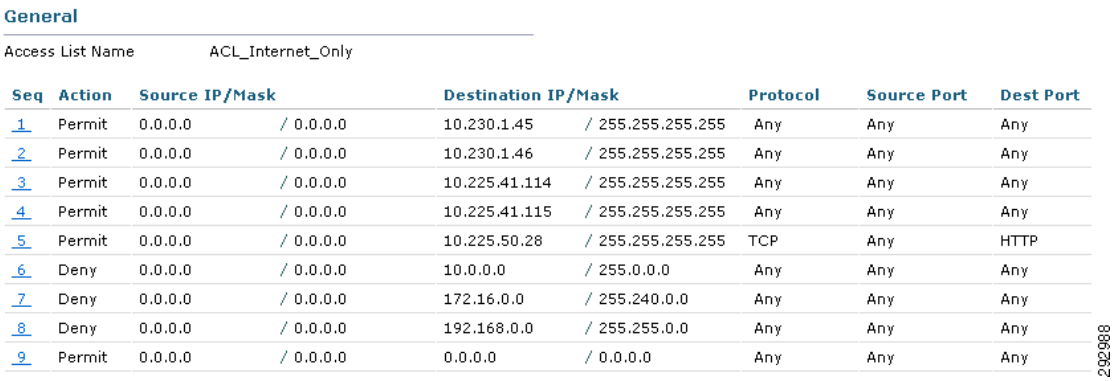
General

Access List Name Branch1_ACL_Partial_Access

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.46	/ 255.255.255.255	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.41.114	/ 255.255.255.255	Any	Any	Any
4	Permit	0.0.0.0	/ 0.0.0.0	10.225.41.115	/ 255.255.255.255	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.225.50.28	/ 255.255.255.255	TCP	Any	HTTP
6	Deny	0.0.0.0	/ 0.0.0.0	10.230.0.0	/ 255.255.0.0	Any	Any	Any
7	Deny	0.0.0.0	/ 0.0.0.0	10.225.0.0	/ 255.255.0.0	Any	Any	Any
8	Permit	0.0.0.0	/ 0.0.0.0	10.200.16.0	/ 255.255.255.0	Any	Any	Any
9	Deny	0.0.0.0	/ 0.0.0.0	10.200.0.0	/ 255.255.0.0	Any	Any	Any
10	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

292987

Figure 41 ACL_Internet_Only



General

Access List Name ACL_Internet_Only

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.46	/ 255.255.255.255	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.41.114	/ 255.255.255.255	Any	Any	Any
4	Permit	0.0.0.0	/ 0.0.0.0	10.225.41.115	/ 255.255.255.255	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.225.50.28	/ 255.255.255.255	TCP	Any	HTTP
6	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any
7	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any
8	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

292988

FlexConnect VLAN Override

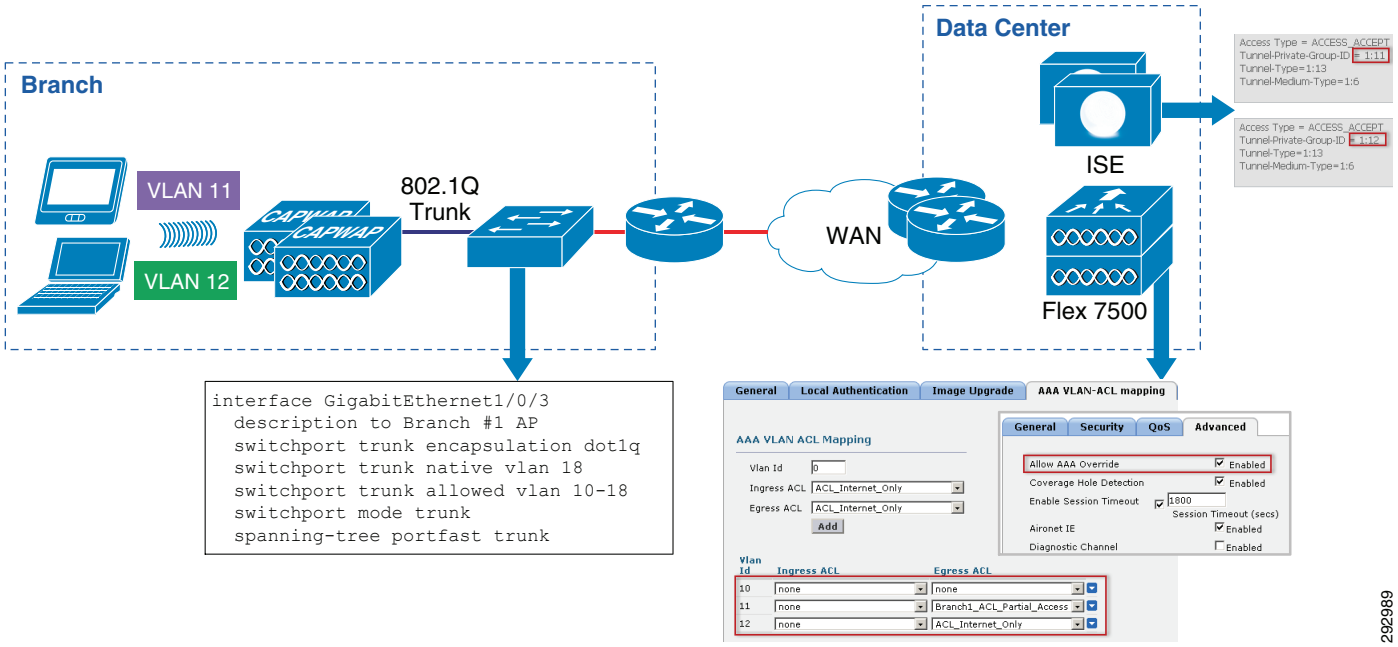
In the current FlexConnect architecture, there is a strict mapping of WLAN to VLAN, so the client getting associated on a particular WLAN on FlexConnect AP has to abide by the VLAN which is mapped to it. This method has limitations because it requires clients to associate with different SSIDs in order to inherit different VLAN-based policies.

Starting on WLC release 7.2, AAA Override (Dynamic VLAN assignment) of VLANs on individual WLANs configured for local switching is supported. To assign endpoints dynamically to a VLAN, the VLAN IDs are pre-created and the corresponding WLAN-VLAN Mapping on a FlexConnect group is configured. Figure 39 shows this setting.

Figure 42 shows the different configuration settings required to dynamically assign endpoints to a branch VLAN, which include:

- WLAN at the branch configured for local switching mode
- 802.1Q trunk between the Catalyst switch and the access point
- Define the correct native vlan and allowed VLANs for the trunk
- The ISE authorization profile defines what VLAN is assigned to the endpoint.
- The WLAN is configured at the controller to allow AAA Override
- The VLANs are pre-defined and the VLAN-ACL mapping is defined for the FlexConnect group

Figure 42 FlexConnect VLAN Override



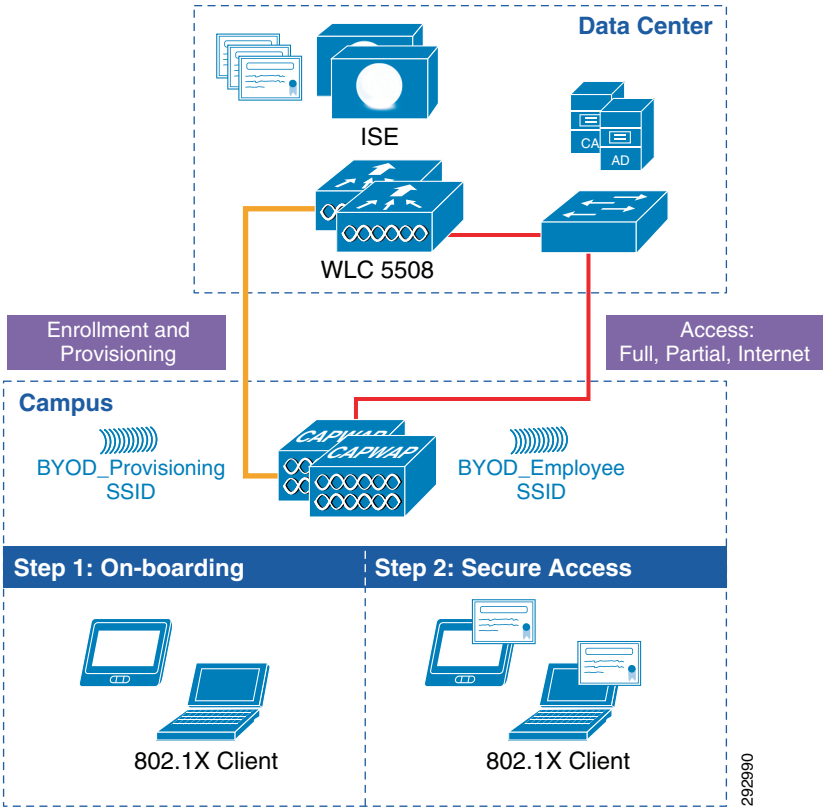
Campus Wireless LAN Design

Clients connecting from the campus wireless infrastructure are served by a dedicated Wireless Controller cluster operating in local mode (central switching). The controllers are configured with the proper SSIDs to provide device on-boarding and secure access. This functionality may be provided via single or dual SSIDs.

Campus—Single SSID Design

In a single SSID design the same WLAN is used for certificate enrollment, provisioning (on-boarding process), and secure network access. Figure 43 shows how this design may be implemented using the 5508 Wireless LAN Controller. In this case, the controllers are dedicated to manage the APs in the campus.

Figure 43 Campus—Single SSID

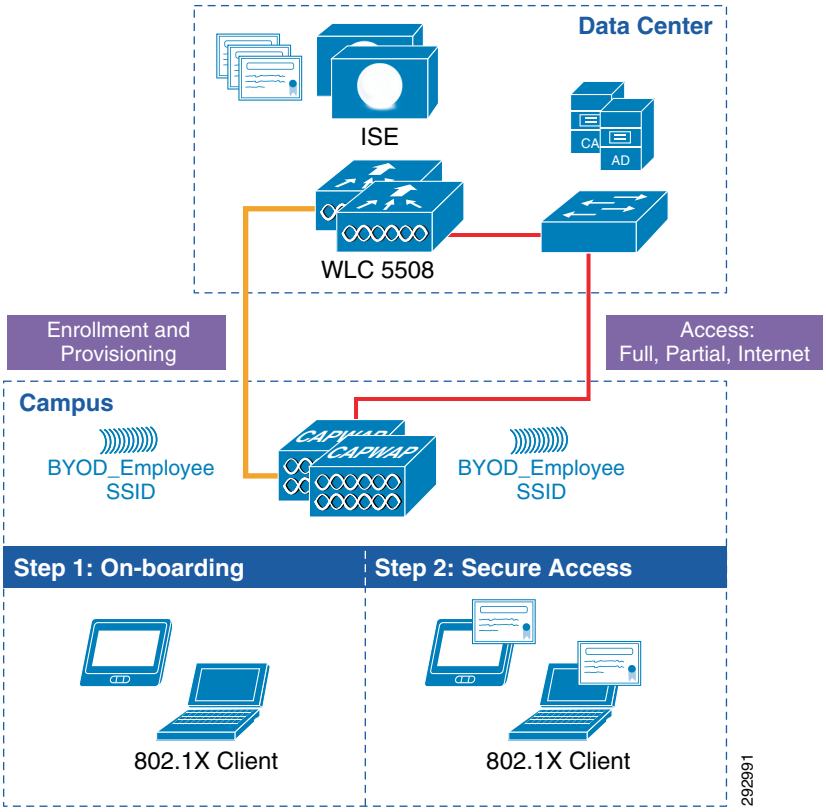


Campus—Dual SSID Design

In this design there are two SSIDs: one provides enrollment/provisioning and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides the network access.

Figure 44 shows the dual SSID design for the campus APs.

Figure 44 Campus—Dual SSIDs



In a dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID.
- After the user is provisioned, it is assumed that they will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list that provides only access to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of this SSID are discussed in Client Provisioning.
- For the purpose of this design guide, the following two SSIDs are used: BYOD_Provisioning and BYOD_Employee.

The properties of these two SSIDs are highlighted in Table 6.

Table 6 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used only for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None	WPA+WPA2
MAC Filtering	Enabled	Disabled
WPA+WPA2 Parameters	None	WPA2 Policy, AES, 802.1X
Layer 3 Security	None	None

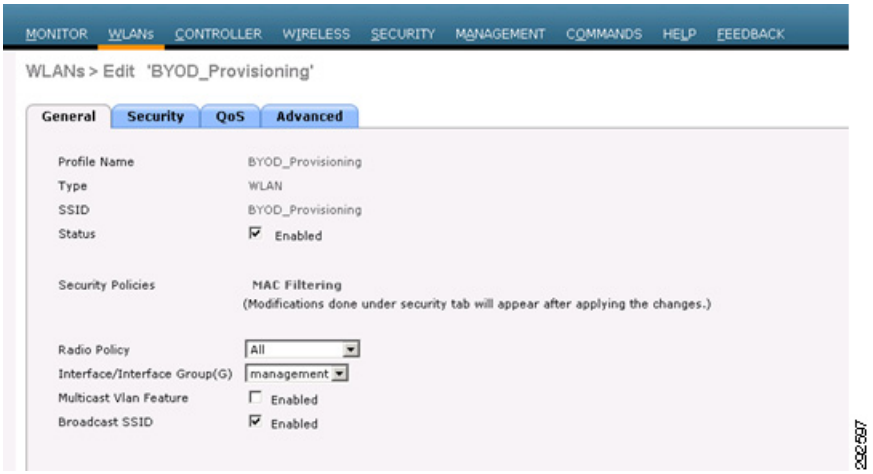
Table 6 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State-RADIUS NAC	NAC State-RADIUS NAC

To create a WLAN, click **WLANs > Create New > Go** and provide the SSID and profile details. Starting from Figure 46, the general configuration steps of the BYOD_Provisioning SSID are highlighted. The steps to configure the BYOD_Employee WLAN are similar, following the settings in Table 6.

Note When implementing BYOD solutions using more than one WLC (Wireless LAN Controller), WLAN IDs must be kept consistent. WLAN ID is used by ISE in determining which WLAN (SSID) clients are using to connect to the network. Ensuring each WLAN has the same WLAN ID on each WLC is essential for proper operation and security. When creating a new WLAN, the WLAN ID is auto-created by the WLC unless specifically set. After creation, it cannot be changed.

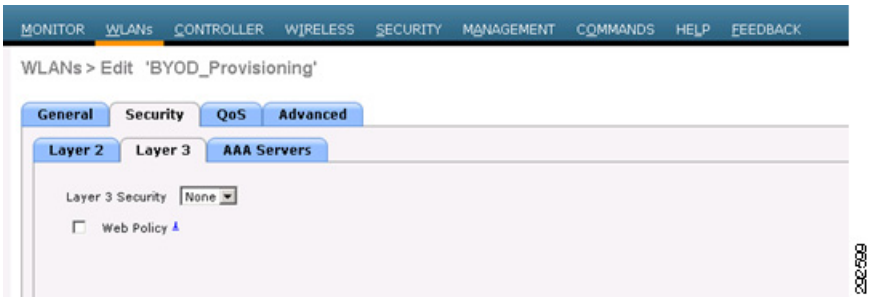
Figure 45 Creating the BYOD_Provisioning SSID



The Layer 2 security settings are configured as **None** because BYOD_PROVISIONING is an open SSID. If the provisioning SSID has to be defined as password protected, then the Layer 2 security settings must be configured as WPA+WPA2 Enterprise.

Figure 46 Layer 2 Security Settings

Figure 47 Layer 3 Security Settings



The main configuration in the security settings is to specify the RADIUS server configuration details. Figure 48 shows how the ISE's IP address is configured for Authentication and Authorization.

Figure 48 AAA Security Settings

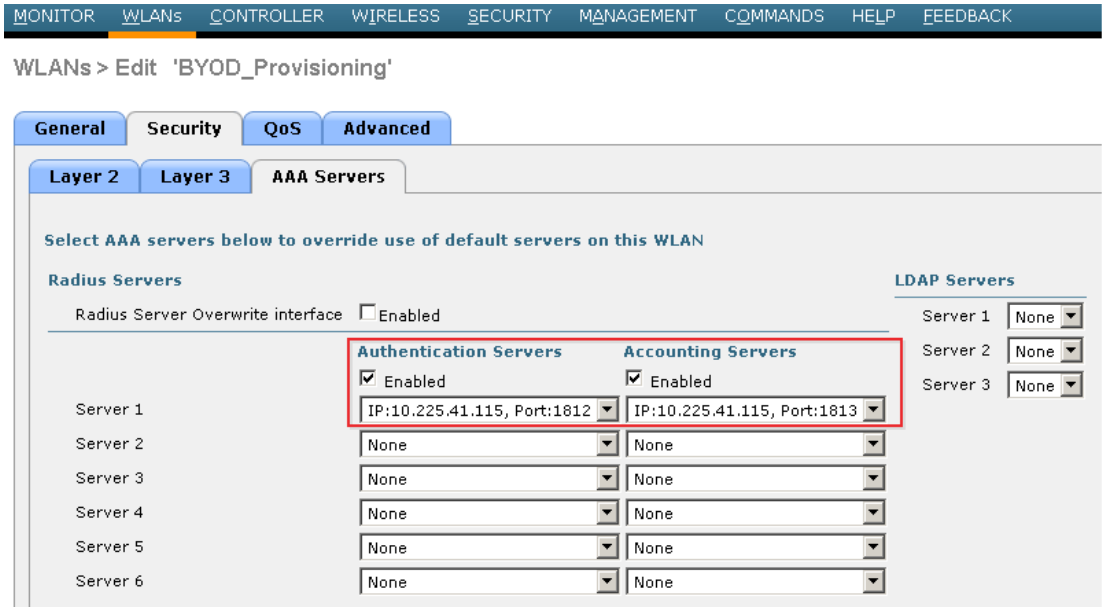
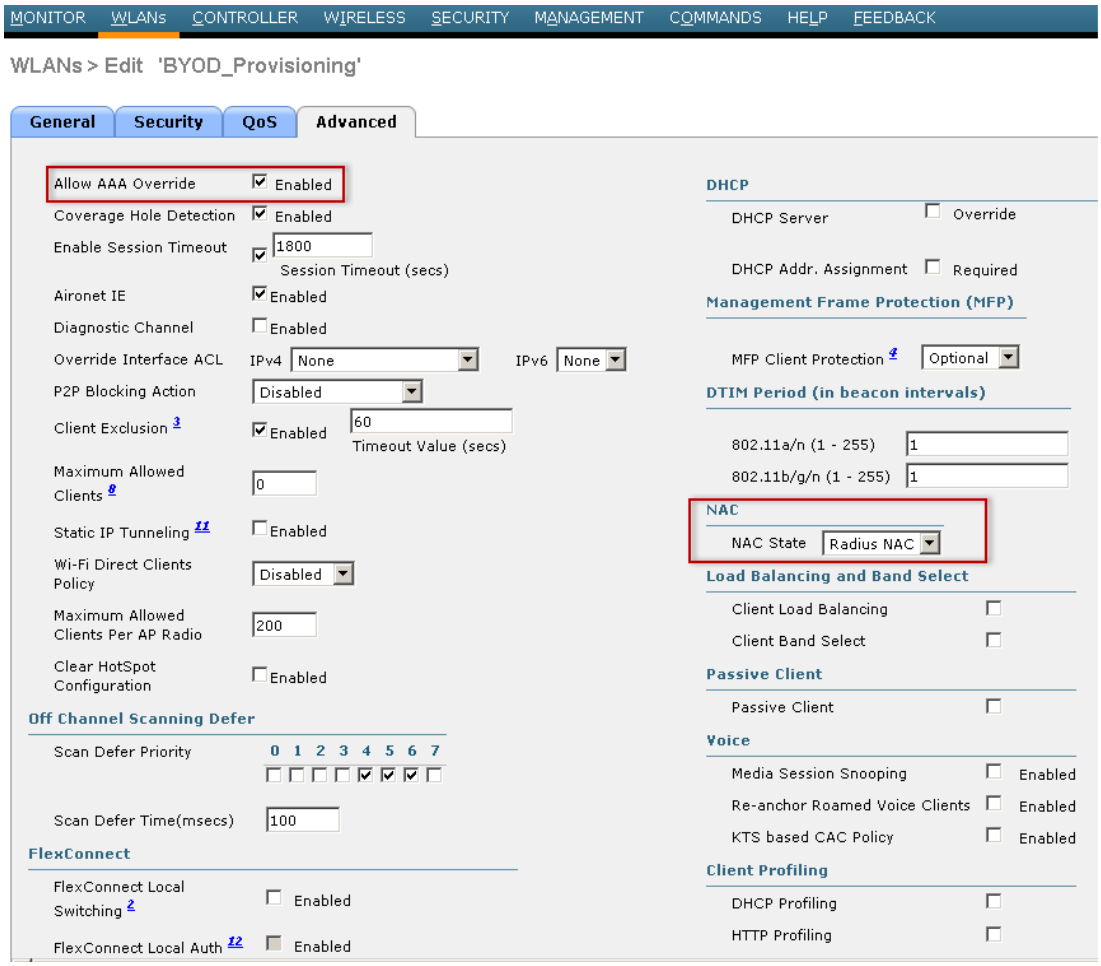


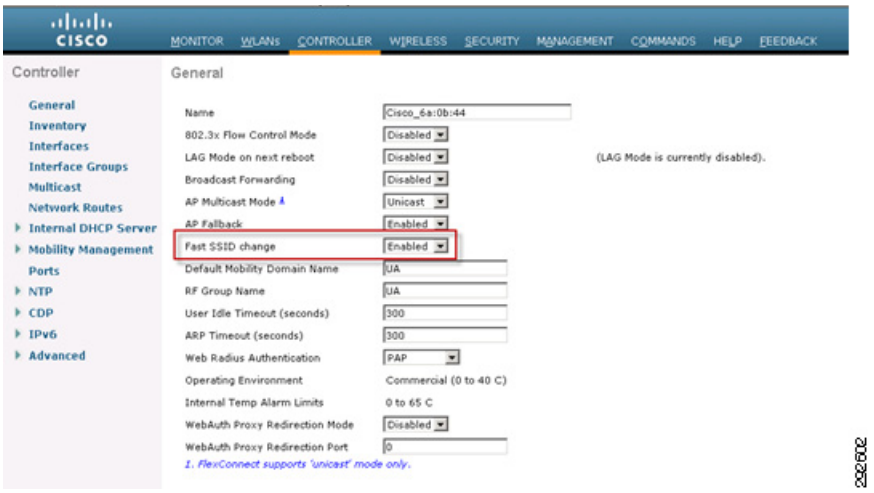
Figure 49 shows the advanced settings, including AAA Override and NAC State.

Figure 49 Advanced Settings



The Fast SSID Change feature is useful when a device needs to switch from one SSID to another. This applies to the dual SSID BYOD design. After the user completes registration with BYOD_Provisioning, the user is switched to BYOD_Employee SSID. By enabling the "FAST SSID Change" feature, the user switches immediately to the new SSID without experiencing delays. To enable Fast SSID Change, click **Controller > General > Fast SSID change**, as shown in Figure 50.

Figure 50 Fast SSID Change



Identity Services Engine

The Cisco Identity Services Engine (ISE) allows for enforcement of centrally configured policies across wired and wireless networks to help organizations provide secure unified access. The Cisco ISE plays a critical role in enabling the BYOD model, where employees are allowed to connect their personal devices securely to the network.

Cisco ISE provides a highly scalable architecture that supports both standalone and distributed deployments. The configuration guidelines shown in this document reflect a distributed architecture with multiple nodes.

For small BYOD deployments, one or two ISE nodes can be configured in standalone mode. Depending on how the AAA connections are configured across the Access Layer Switches and Wireless LAN Controllers, either an active/backup or load balancing of AAA workflows can be enabled across the redundant standalone ISE nodes.

For larger BYOD deployments, the ISE functionality can be distributed across multiple nodes. Distributed deployments support the following three different ISE personas:

- Administration—The administration node handles all system level configuration. There can be one primary and one secondary Administration Node in a distributed deployment.
- Monitoring—The monitoring node handles log collection and provides monitoring and troubleshooting tools. There can be one primary and one secondary Monitoring node in a distributed deployment.
- Policy Service—The policy Service node provides authentication, authorization, guest access, client provisioning, and profiling services. There can be multiple Policy Services Nodes in a distributed deployment.

To support a medium size BYOD deployment, both Administration and Monitoring personas can be deployed on a single node while dedicated Policy Services nodes can handle AAA functions. For a large BYOD deployment, the Monitoring persona can be implemented on a dedicated node providing centralized logging functions.

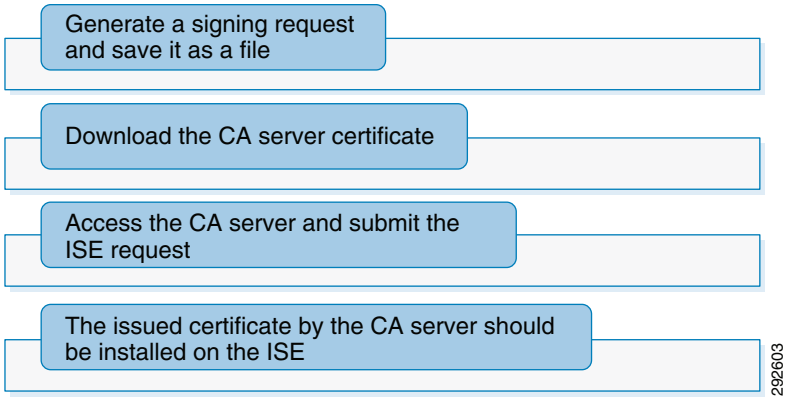
For additional information on Cisco ISE Network deployment, see:
http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_deploy.html.

For information on how to setup ISE in a distributed environment, see: http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_dis_deploy.html.

Identity Certificate for ISE

ISE needs an identity certificate that is signed by a CA server so that it can be trusted by endpoints, gateways, and servers. Figure 51 illustrates the steps at a high level.

Figure 51 High-Level Steps for Deploying Identity Certificates on ISE



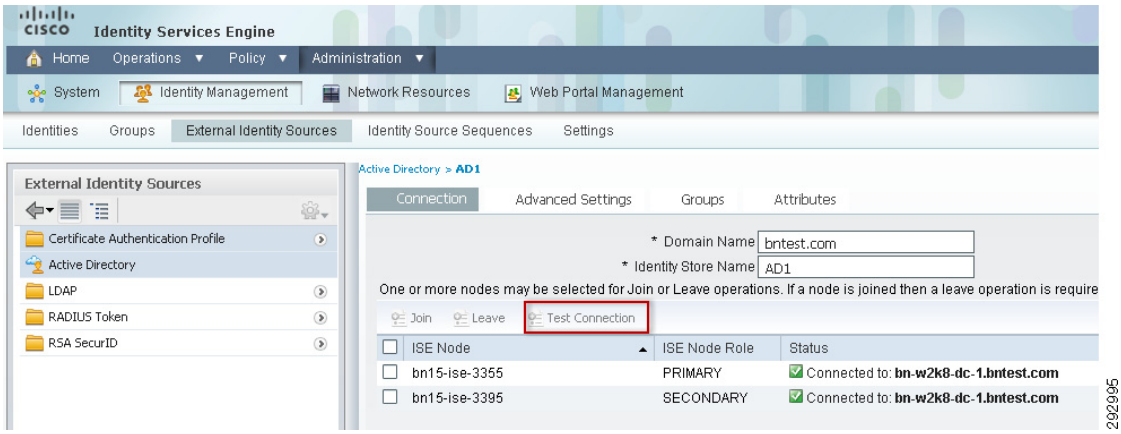
For more details on installing a digital certificate on the Cisco ISE, refer to the *TrustSec How-To Guide*: http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

ISE Integration with Active Directory

While the 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's Active Directory, objects such as users and groups become critical in the authorization process and can be accessed from a single source.

To integrate with Active Directory, choose **Administration > External Identity Sources > Active Directory** and specify the domain name, as shown in Figure 52. To verify that the ISE node can connect to the Active Directory domain, click **Test Connection** and authenticate with an AD username and password, as shown in Figure 52. Click **Join** to join the ISE node to Active Directory.

Figure 52 Active Directory Integration



Note The Cisco Identity Services Engine User Guide has detailed configuration steps (http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html).

Guest and Self-Registration Portals

The Cisco ISE server has the capability to host multiple portals. The BYOD system design relies on the Guest Portal to provide wireless guest access and, for provisioning purposes, the redirection of employees to the Self-Registration portal to on-board their devices. BYOD Guest Wireless Access discusses the use of the Guest Portal for guest wireless access. The default ISE portals have standard Cisco branding that may be customized to identify unique portals for different purposes and with individual policies.

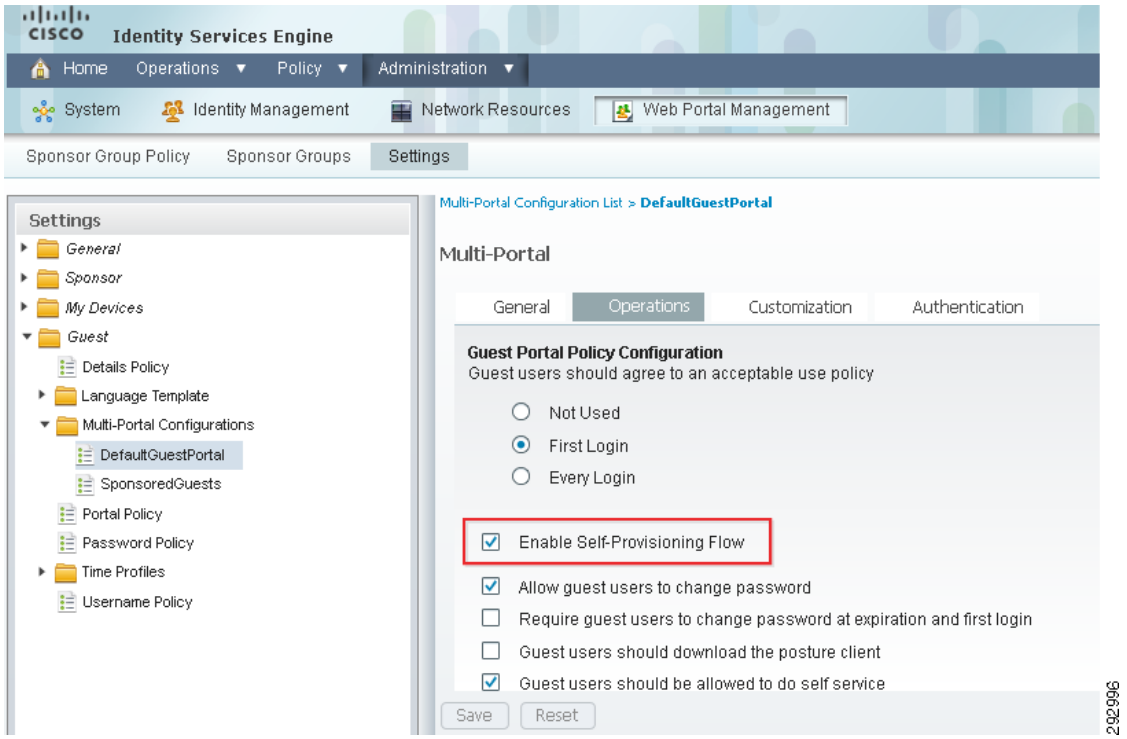
ISE enables self-provisioning, which allows employees to register their personal wireless device. The ISE provisions the device with its native supplicant during device registration.

The BYOD system leads the employee through the following provisioning steps the first time they bring their personal device to work and register:

1. The employee connects the device to the open SSID (this is the BYOD_Provisioning SSID).
2. The device is redirected to the Guest Registration portal.
3. The employee enters credentials and ISE authenticates against Active Directory.
4. If the device is not yet registered on the network, the session is redirected to the self-registration portal.
5. The employee is asked to enter a unique device description and complete the device registration.

To enable Self-Provisioning, configure these portals as follows: click **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations**, as shown in Figure 53.

Figure 53 Portal Settings—Operations

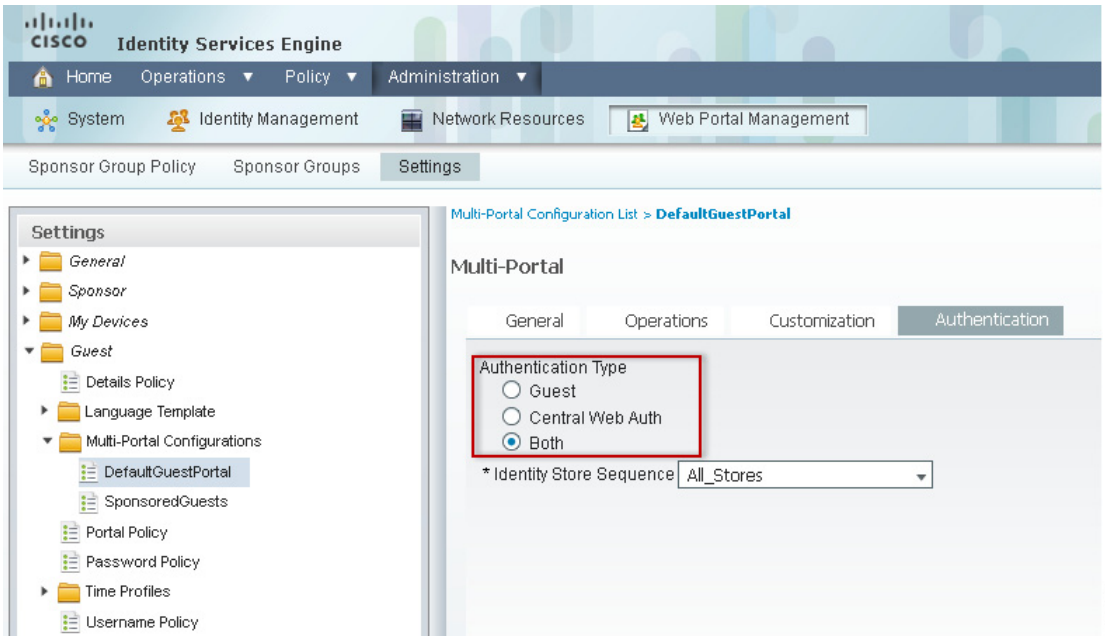


In the figure above, the SponsoredGuests portal refers to the portal used for wireless guest access—otherwise known as the Guest Portal in this document. The DefaultGuestPortal refers to the portal used for self-registration—otherwise known as the Self-Registration portal in this document.

To specify how the portal authenticates users, select the Authentication tab within the particular portal, as shown in Figure 54, and select the appropriate option:

- Guest—The portal authenticates guest user accounts stored in the local database.
- Central WebAuth—The user is authenticated against the databases specified in the Identity Store Sequence.
- Both—The user is authenticated against a local guest database first. If the user is not found, authentication is attempted using additional databases defined in the Identity Store Sequence.

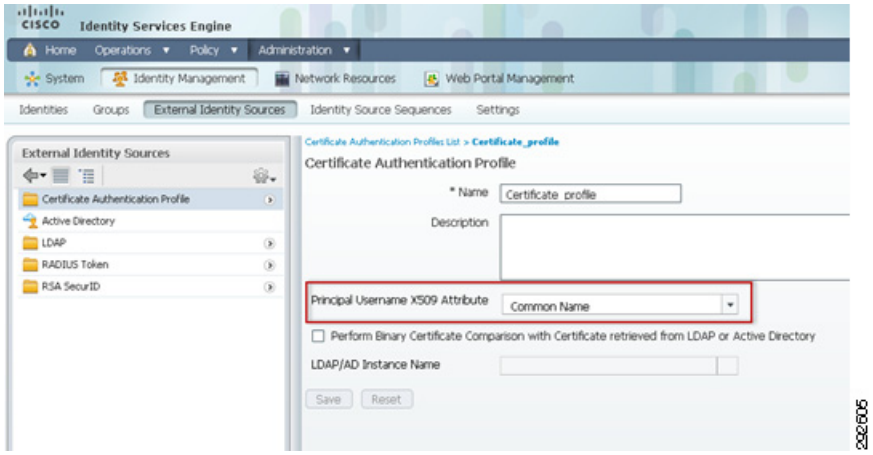
Figure 54 Authentication Portal Settings



ISE Using Certificates as an Identity Store

To configure ISE to use certificates as an identity store, choose **Administration > External Identity Sources > Certificate Authentication Profile > Add** and define the Certificate Authentication Profile, as shown in Figure 55.

Figure 55 Certificate Authentication Profile

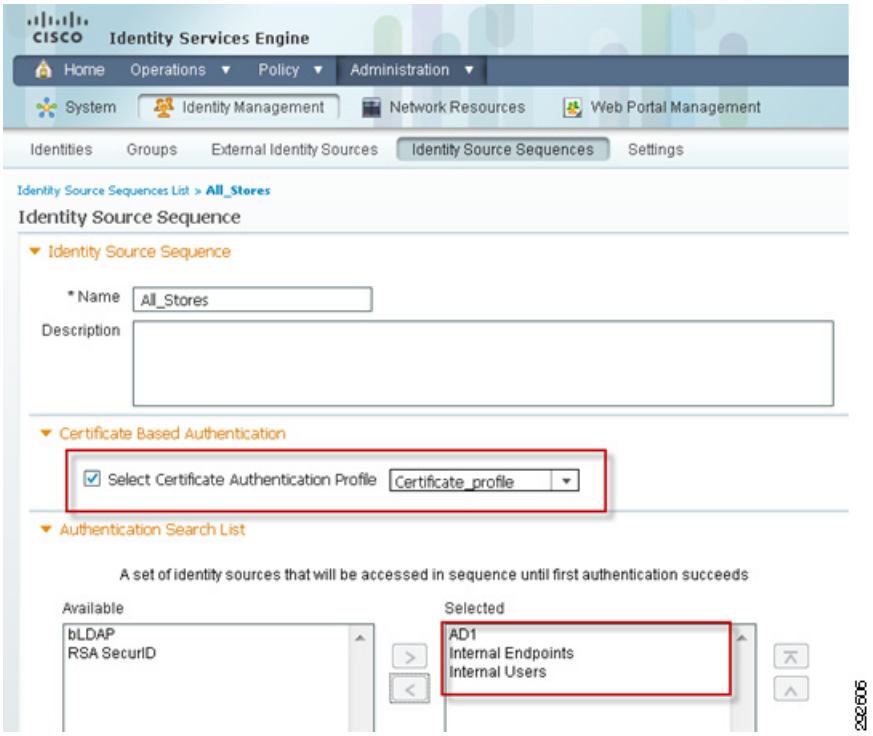


Identity Source Sequences

Identity Source Sequences define the order in which ISE will look for user credentials in the different databases. These databases include Internal Users, Active Directory, LDAP, RSA, etc.

To add a new Identity Source Sequence, click **Administration > Identity Source Sequences > Add**. The configuration shown in Figure 56 creates a new Identity Source Sequence named All_Stores. It relies on Active Directory (AD1), a certificate profile named "Certificate_profile", Internal Endpoints, and Internal Users.

Figure 56 Identity Source Sequence

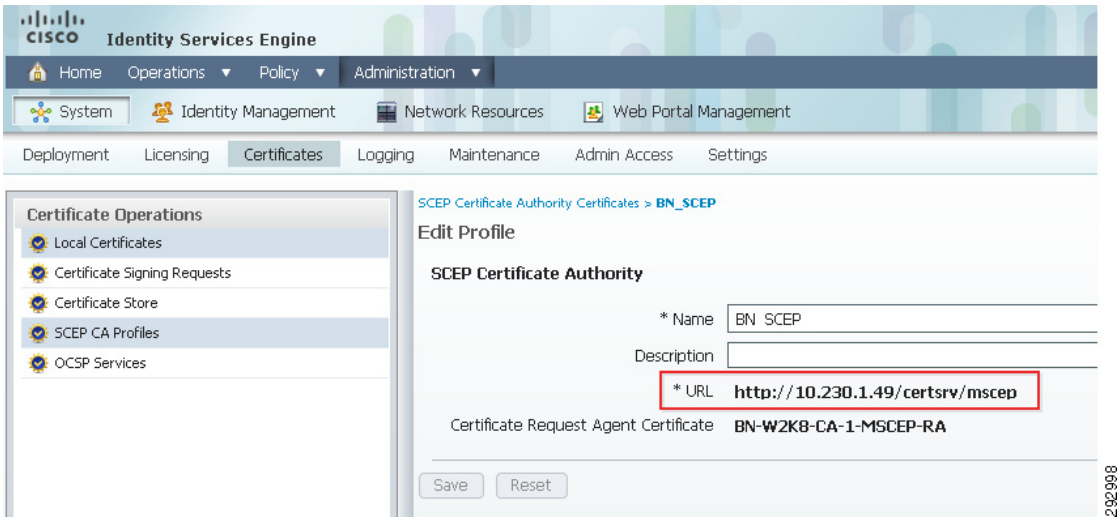


SCEP Profile Configuration on ISE

Within this design, ISE is acting as a Simple Certificate Enrollment Protocol (SCEP) proxy server, thereby allowing mobile clients to obtain their digital certificates from the CA server. This important feature of ISE allows all the end points, such as iOS, Android, Windows, and MAC, to obtain digital certificates through the ISE. This feature combined with the initial registration process greatly simplifies the provisioning of digital certificates on end points.

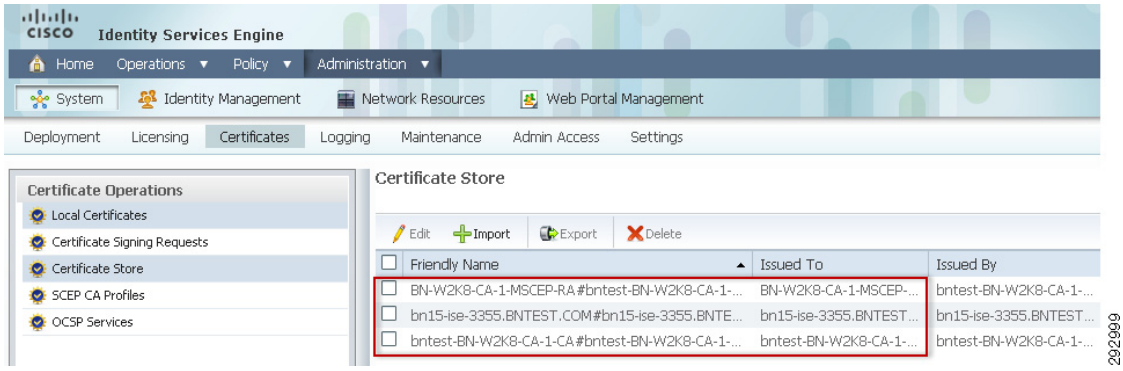
To configure SCEP profile on the ISE, click **Administration > Certificates > SCEP CA Profiles > Add**. Define the SCEP profile, as shown in Figure 57.

Figure 57 SCEP Profile Configuration



After the configuration is successful, ISE downloads the RA certificate and the root CA certificate of the CA server, as shown in Figure 58.

Figure 58 Certificate Store



Authentication Policies

Authentication policies are used to define the protocols used by the ISE to communicate with the endpoints and the identity sources to be used for authentication. 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 protocol service, such as PEAP, EAP-TLS, etc.
- An identity source used for authentication

Like access lists, 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:

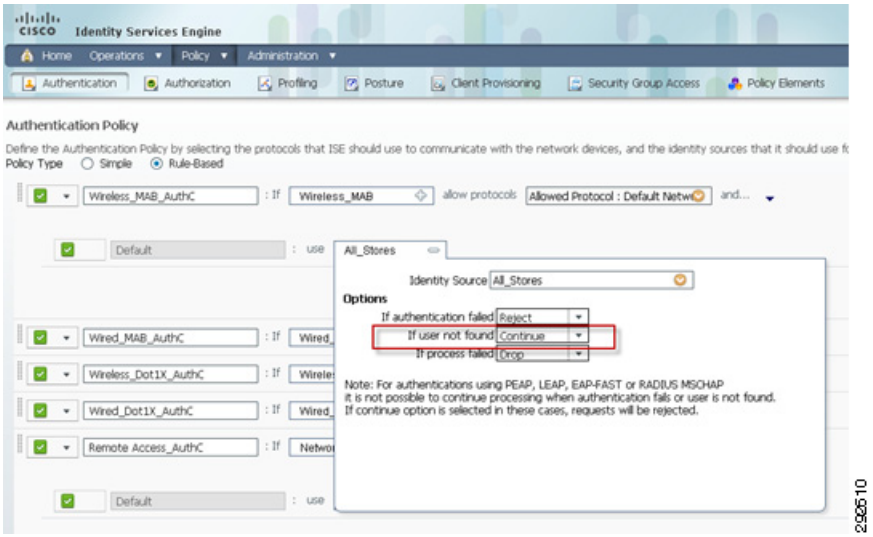
```
IF Wired_802.1X   Then
     Allow default protocols
Elseif   next condition
     Take action
```

```
Else
     Use Default Rule
```

In BYOD designs discussed throughout this document, ISE authenticates several protocols such as MAB and dot1x against all the Identity Stores. The Identity Stores could be AD, Certificate_Profile, RSA, Internal Users, and Internal Endpoints. The network access medium could be either wired, wireless, or remote connection. The network device uses any of the mediums mentioned before, using different protocols to connect to ISE.

MAC Authentication Bypass (MAB) protocol is used by wired and wireless endpoints to authenticate devices that do not have dot1x configured. When a brand new device accesses the network it communicates using MAB protocol and uses its own MAC address as its identity. In a normal scenario, ISE would validate if the MAC address is present in any of its identity stores; if not, then reject the connection. However in this BYOD design the MAB protocol is used by new devices for on-boarding purposes and it may not be feasible to know the MAC address of the device in advance. To circumvent this problem, ISE continues the authentication process and redirects the device to the next stage, even if the device's MAC address is not present in any of its identity stores. Figure 59 highlights this configuration.

Figure 59 Authentication Rule for MAB



In a normal deployment scenario, the end points would primarily use dot1x protocol to communicate with ISE. The network access medium could be either wired or wireless. ISE authenticates these endpoints against an Active Directory or authenticates them via digital certificates. In addition to wired and wireless connections, ISE also authenticates remote end points using RSA SecurID as an identity store. Figure 60 depicts the different protocols and how these protocols use different identity stores for authentication.

Figure 60 Authentication Policy

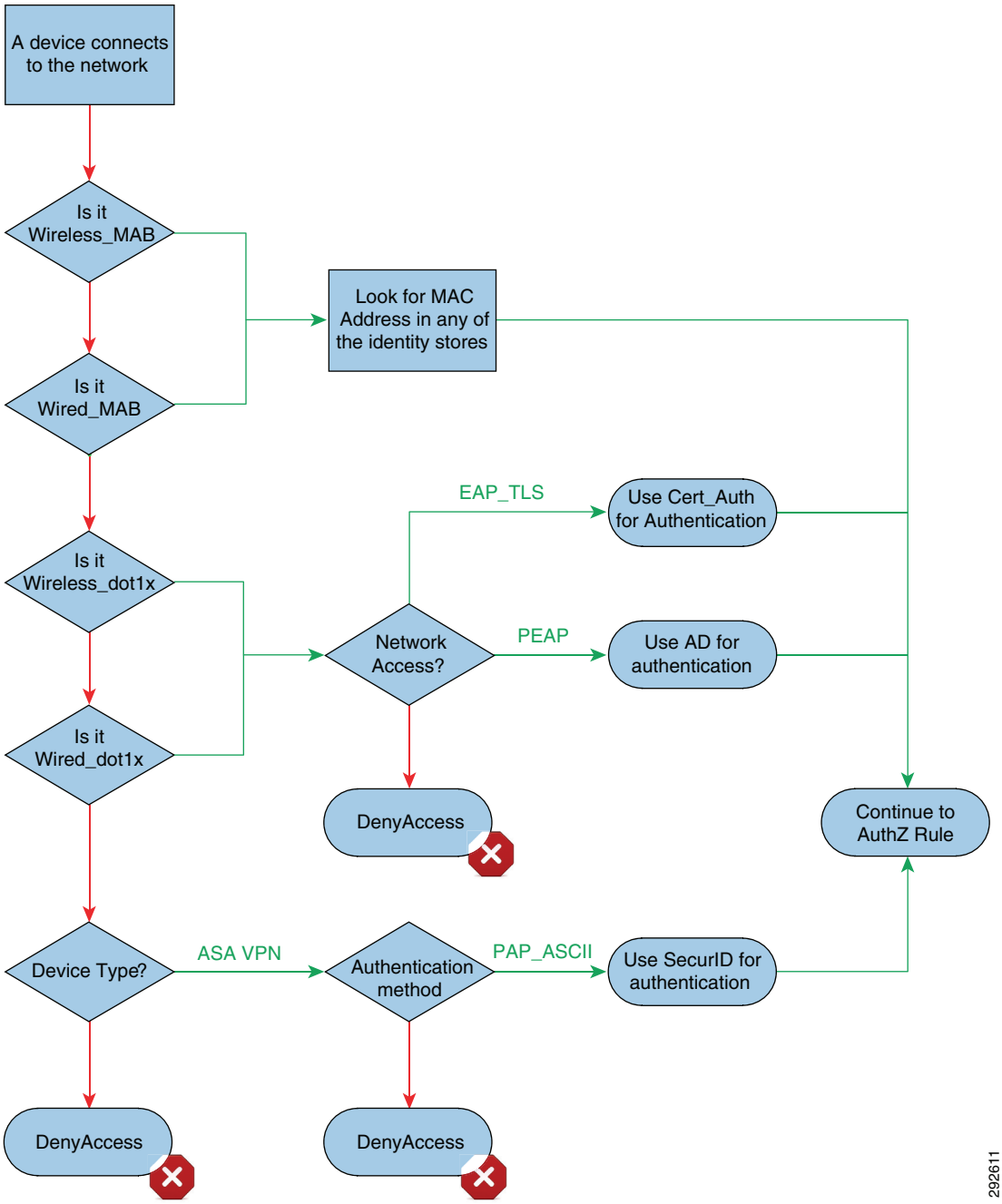


Table 7 explains how these rules are implemented in ISE design.

Table 7 Authentication Rules

Rule Name	Network Access Medium	Allowed Protocols	Conditions	Identity Store
Wired_MAB_AuthC	Wired_MAB	All	Default	All_Stores

Table 7 Authentication Rules

Wireless_Dot1X_AuthC	Wireless_8021X	All	Wireless_Certificate	EAP_TLS	Certificate_Profile AD
			Wireless_Password	PEAP	
Wired_Dot1X_AuthC	Wired_802.1X	All	Wired_Certificate	EAP_TLS	Certificate_Profile AD
			Wired_Password	PEAP	
Remote_Access	DeviceType:ASA	All	Remote_ASA	PAP_ASCII	RSA SecureID
Default					Deny Access

Authentication Policy for Wireless

The endpoint devices could use either MAB or dot1x protocol when connecting to the wireless network. The authentication policy for wireless networks using MAB is explained in the previous section. This section explains the authentication policy for wireless medium using dot1X protocol. As shown in Table 7, Wireless_Dot1X_AuthC is the rule name for wireless_dot1x protocol. This rule matches wireless_dot1x protocol and has two inner rules: 1) Wireless_Certificate 2) Wireless_Password. The Wireless_Ceritificate matches when the authentication protocol is EAP_TLS and it verifies the digital certificate using the identity store Ceritificate_Profile. The second inner rule Wireless_Password matches on the authentication protocol PEAP and uses Active Directory as an Identity Store.

Authentication Policy for Wired Devices

The authentication policy for wired devices is very similar to wireless policy. The main rule name for wired policy is Wired_Dot1X_AuthC and this rule matches on the wired_dot1x protocol. This rule also has two inner rules: 1) Wired_Certificate 2)Wired_Password. The first rule matches when the authentication protocol used by endpoint is EAP_TLS and authenticates the digital certificate using an identity store Certificate_Profile. The second rule matches when the endpoint uses PEAP as an authentication protocol and authenticates against an Active Directory.

Authentication Policy for Remote Devices

The authentication for remote devices happens in two steps:

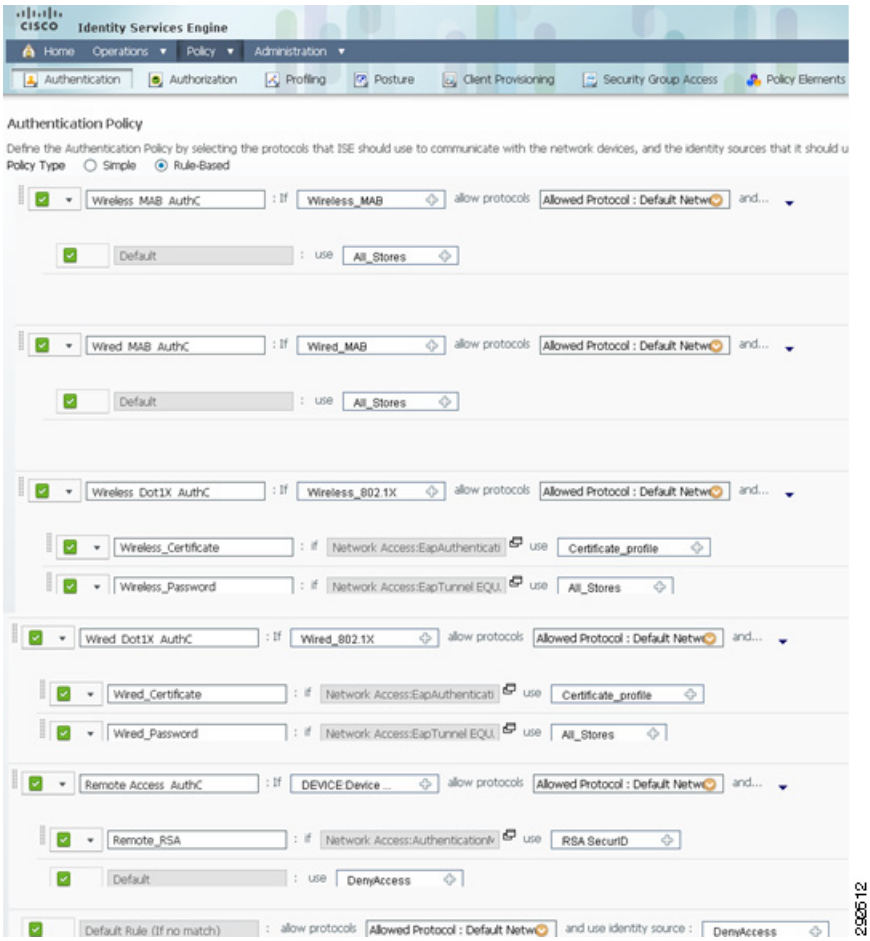
1. ASA, which is acting as VPN gateway, authenticates the digital certificate of the endpoint.
2. The One Time Passwords used by remote devices is validated by ISE using RSA Secure ID as an Identity Store.

The configuration of the ASA as the VPN gateway is discussed in Basic Access Design. In this section the second part of the authentication flow is discussed.

ISE validates if the Device Type is equal to ASA VPN and then it verifies if the authentication protocol is PAP_ASCII. If these two conditions are met then it authenticates using the Identity Store RSA_Secure ID.

Figure 61 shows how these rules were configured on the ISE for this design guide.

Figure 61 Authentication Rules



Client Provisioning

The Cisco ISE looks at various elements when classifying the type of login session through which users access the network, including client machine OS and version, client machine browser type and version, and others. Once the ISE classifies the client machine, it uses client provisioning resource policies to ensure 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 ISE Profiling service is discussed in Enabling the DHCP Probe.

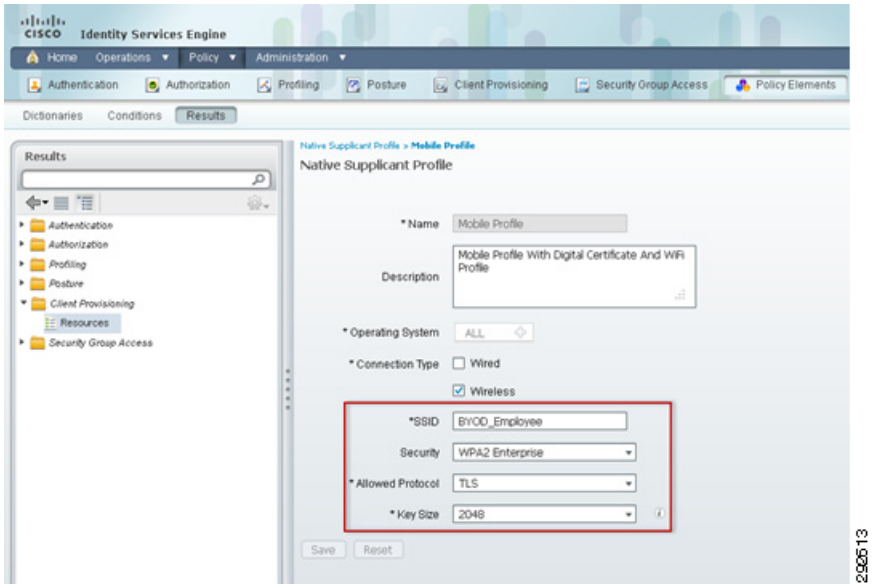
The following are considerations for Client Provisioning on the endpoints:

- Based on the endpoint, push an appropriate Software Provisioning Wizard (SPW) to the device. This Wizard configures the dot1x 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 SPW package because for iOS devices the native operating system is used to configure the dot1x settings.
- For Android devices, the SPW package needs to be downloaded from Google Play Store.
- The SPW packages are developed by Cisco and they can be downloaded from: http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_client_prov.html#wp1053223.

Client Provisioning Resources—iOS and Android

To configure a client provisioning resource for mobile devices, click **Policy Elements > Results > Client Provisioning > Resources > Add**. Figure 62 shows the configuration details for the Mobile Profile profile, which is used to configure access to the BYOD_Employee SSID after on-boarding.

Figure 62 Mobile Profile NSP

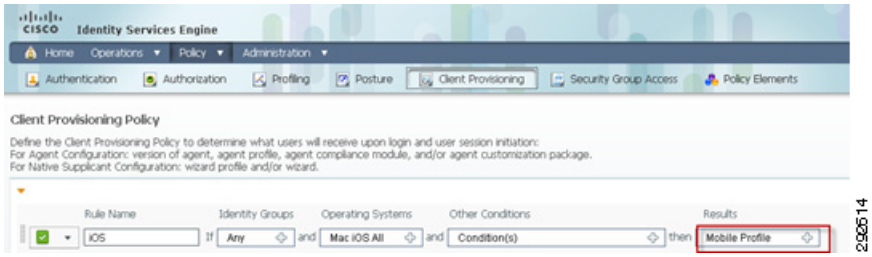


Client Provisioning Resource Policy for iOS Devices

Client provisioning resource policies determine which users receive which version of resources. After defining the Native Supplicant Profile, the next step is to use this profile when iOS devices connect to the network by clicking **Policy > Client Provisioning**.

The configuration in Figure 63 determines the operating system running on the device and defines which resources to distribute. In this case the previously defined Mobile Profile is distributed.

Figure 63 Client Provisioning Resource Policy for iOS Devices

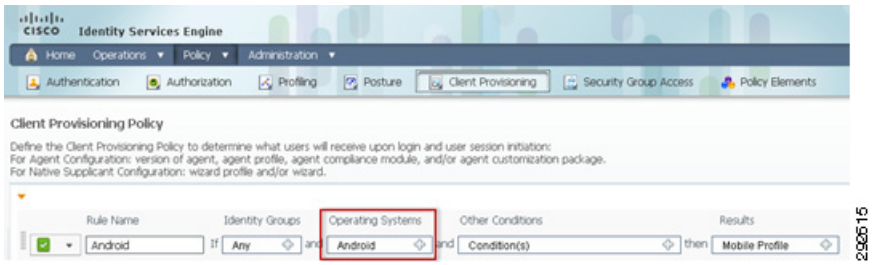


Client Provisioning Resource Policy for Android Devices

The Native Supplicant Profile Mobile Profile can also be used for Android devices. The key difference is that the user is also required to download the Software from Google's Play Store, since it cannot be distributed by ISE. Click **Policy > Client Provisioning** to define the Client Provisioning policy for

Android devices. The Operating System should be selected as Android and the Results selected as Mobile Profile, as illustrated in Figure 64.

Figure 64 Client Provisioning Resource Policy for Android Devices



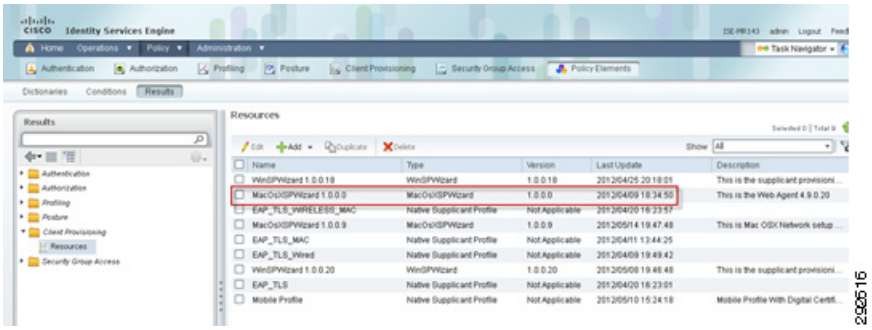
Client Provisioning Resources—Mac OS

For workstations, the following is required:

- Native Supplicant profile, similar to the one used by iOS and Android devices above.
- A Wizard Profile. The Supplicant Provisioning Wizard profile is a software agent that may be downloaded from the Cisco site. To obtain more information on how to download SPW packages, see: https://www.cisco.com/web/secure/pmbu/provisioning-update.xml.

To define the client provisioning resources, click **Policy Elements > Results > Client Provisioning > Resources > Add**. Figure 65 shows the MacOsXSPWizard profile.

Figure 65 Mac OsXSPWizard Profile



Client Provisioning Resource Policy for Mac OS Devices—Wireless

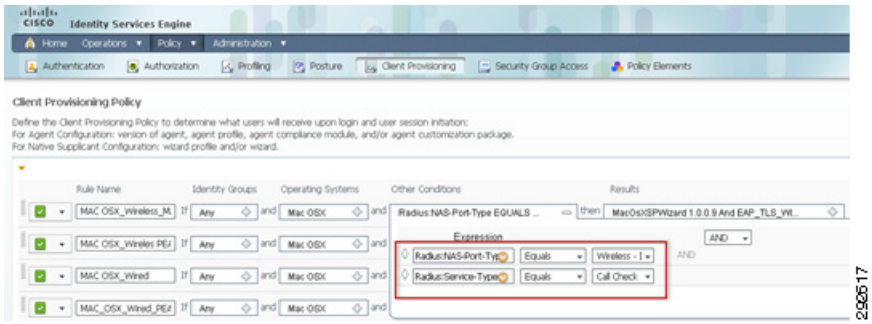
The protocol used by Mac OS X devices can be MAB or PEAP protocol. Therefore, different conditions have to be configured to match either one of them.

The MAB protocol is matched by the following two conditions:

- RADIUS:NAS-Port-Type EQUALS Wireless - IEEE 802.11
- RADIUS:Service-Type EQUALS Call Check

Figure 66 shows the conditions to match on the MAB protocol.

Figure 66 Client Provisioning Resource Policy for MAB

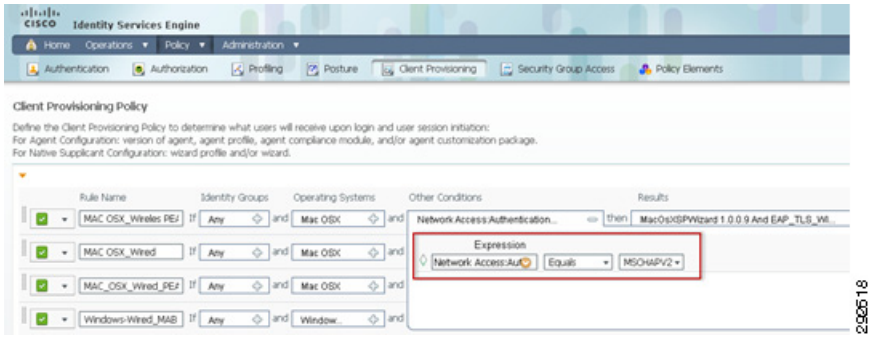


To match a Mac device using the PEAP protocol, a single condition is needed:

- Network Access:AuthenticationMethod EQUALS MSCHAPV2

Figure 67 shows the condition to match on the PEAP protocol.

Figure 67 Client Provisioning Resource Policy for PEAP

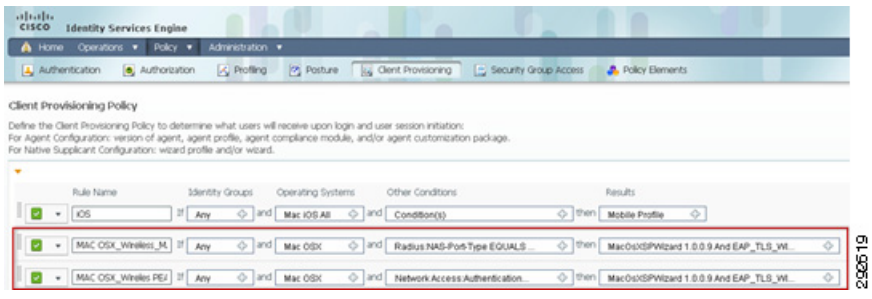


To complete a Client Provisioning policy for MAC_OSX_Wireless devices, the following must be defined:

- The Operating System must be selected as Mac OSX.
- The Conditions should be used to match either MAB or PEAP protocol.
- The result section must contain the Native Supplicant profile and the SPW for Mac OS X devices.

The complete policy is shown in Figure 68.

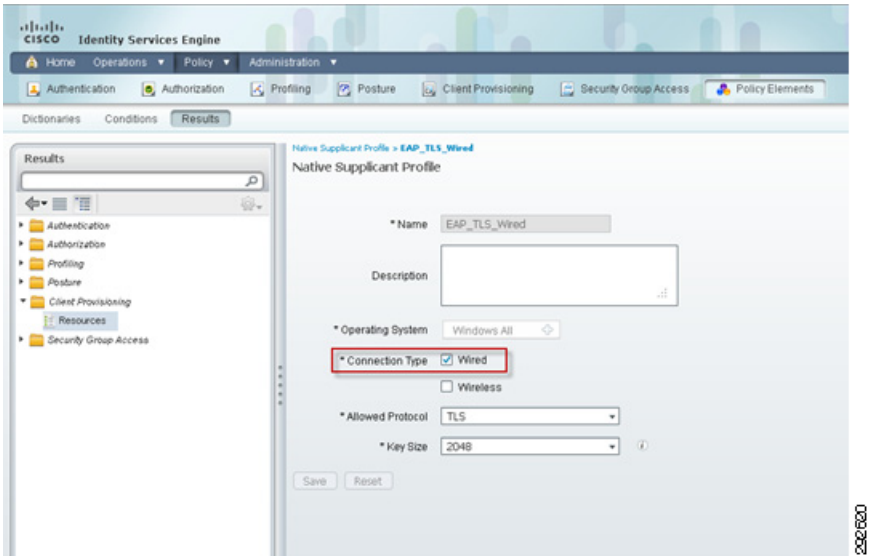
Figure 68 Client Provisioning Resource Policy for Mac OS X



Client Provisioning Resource Policy for Mac OS Devices—Wired

The configuration policy for MAC wired devices is similar to the previous section. The only difference is in configuring the Native Supplicant Profile. The Connection type must be selected as Wired, as shown in Figure 69.

Figure 69 NSP For Wired



MAC wired devices can also use either MAB or PEAP protocol to connect. Hence, both protocols must be defined in the Client Provisioning policy. Refer to Client Provisioning Resource Policy for Mac OS Devices—Wireless on how to identify MAB or PEAP protocol. The Client Provisioning Policy must be defined:

- The Operating System must be selected as Mac OS X.
- The Conditions should be used to match either MAB or PEAP protocol.
- The result section must contain the Native Supplicant profile and the SPW for Mac OS X devices.

Client Provisioning Resource Policy for Windows Devices—Wireless/Wired

The configuration steps for defining the provisioning policy for Windows devices is very similar to Mac OS X or iOS devices. Hence, the same configuration steps are not repeated here. The only difference to point out is that for Windows devices a different SPW package is needed. Figure 70 depicts the Client Provisioning Policy for Windows devices that includes Windows wireless or wired connection using either MAB protocol or PEAP.

Figure 70 Client Provisioning Resource Policy for Windows

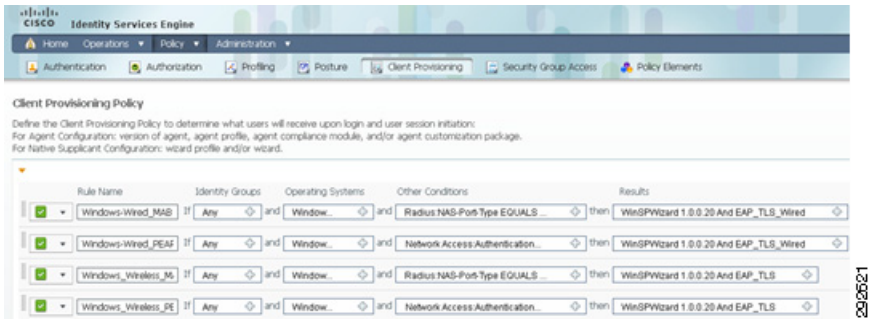
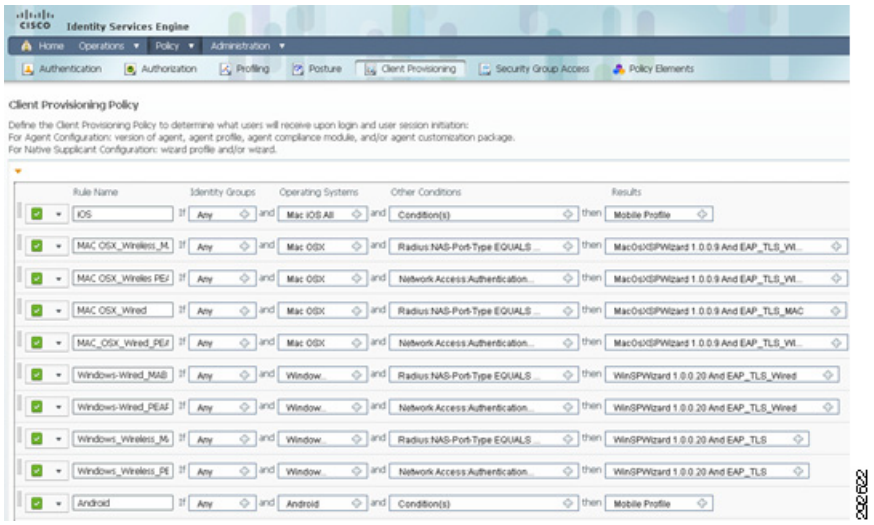


Figure 71 shows the complete client provisioning policy used during testing.

Figure 71 Complete Client Provisioning Policy



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

There are two main methods to collect endpoint information:

- The ISE acting as the collector and analyzer.
- Staring in version 7.3, the WLC can act as the collector and send the required attributes to the ISE, which acts as the analyzer.

Client profiling from a controller running 7.3 or later is supported on access points that are in Local mode and FlexConnect mode. Table 8 shows the main differences between the WLC and ISE profiling.

Note This design guide uses the profiling capabilities of the ISE and did not test the controller client profiling capabilities.

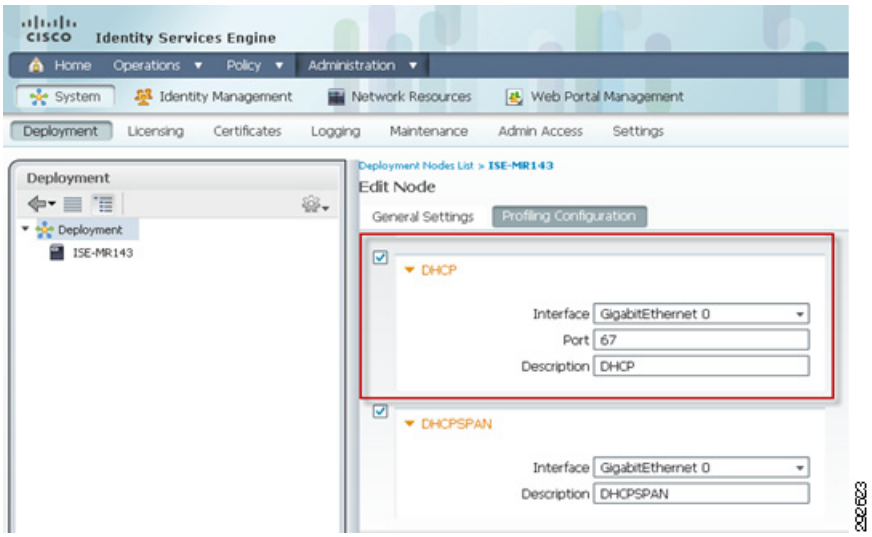
The ISE supports a number of sensors to capture endpoint attributes and classify them according to their profiles. The sensors rely on a number of probes that capture network packets by querying network access devices. Once the endpoints are profiled, different authentication and authorization policies may be enforced. Some examples of using different policies based on the device's profile include:

- Allow employee-owned iPads to access the network, but only for HTTP traffic.
- If the iOS device connecting to the network is a company-owned device, grant full access to the network.
- If an employee-owned iPad has been provisioned with a digital certificate, grant full access to the network.
- Deny access to all iPads or Android devices.

Enabling the DHCP Probe

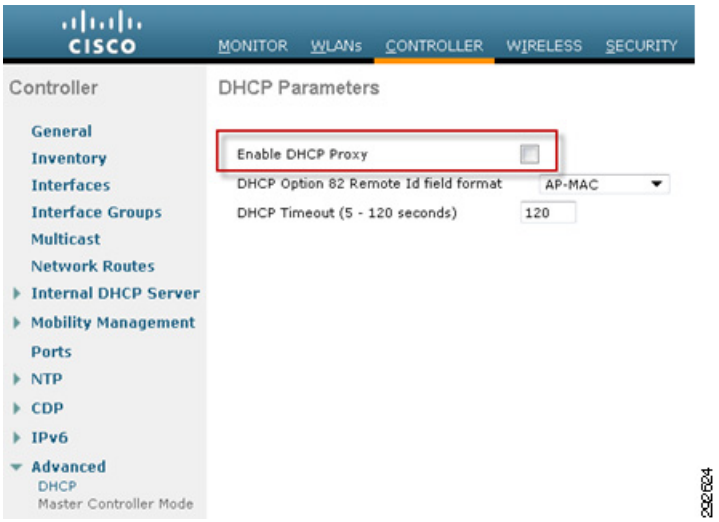
To enable profiling on the ISE, click **Administration > System > Deployment**. Click the ISE hostname and click **Profiling Configuration**. Enable the DHCP probe to listen to packets forwarded from the LAN switch or Wireless LAN Controller, as shown in Figure 72.

Figure 72 DHCP Probe



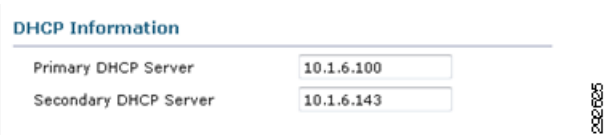
The Wireless LAN Controller should be configured in DHCP bridging mode to forward DHCP packets from the wireless endpoints to the ISE. Click **Controller > Advanced > DHCP** and clear the **Enable DHCP Proxy** check box, as shown in Figure 73.

Figure 73 Disable DHCP Proxy



Specify the ISE's IP address as the secondary DHCP server in the WLC by clicking **Controller > Interfaces > Secondary DHCP**, as shown in Figure 74.

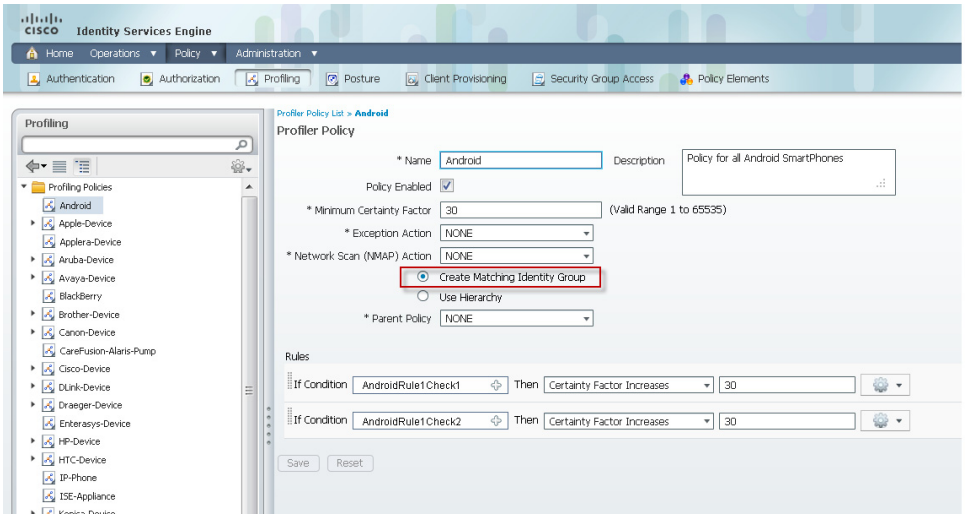
Figure 74 Secondary DHCP Server



Profiling Android Devices

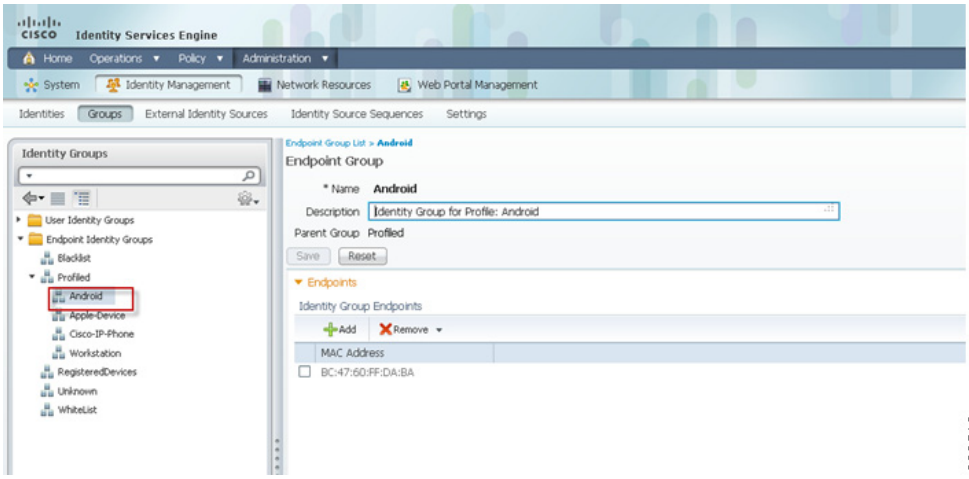
To create an identity group based on the Android policy, click **Policy > Profiling > Profiling Policies > Android** and enable the **Create Matching Identity Group**, as shown in Figure 75.

Figure 75 Android Profiling Policy



The Android profiling policy should be listed under the Endpoint Identity Groups/Profiled. Click **Administration > Identity Management > Groups** to see a list of Android devices that have been profiled by the ISE, as shown in Figure 76.

Figure 76 Android Identity Group



Authorization Policies

Authorization policies are critical to determine which users can access the ISE network and its resources and what each user is allowed to do on the system. 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 a container for specific permissions.

Authorization Profiles

Authorization profiles group the specific permissions granted to a user or device and can include tasks such as:

- An associated VLAN
- An associated downloadable ACL (dACL)
- Wireless LAN Controller attributes
- Advanced settings using attributes contained in dictionaries

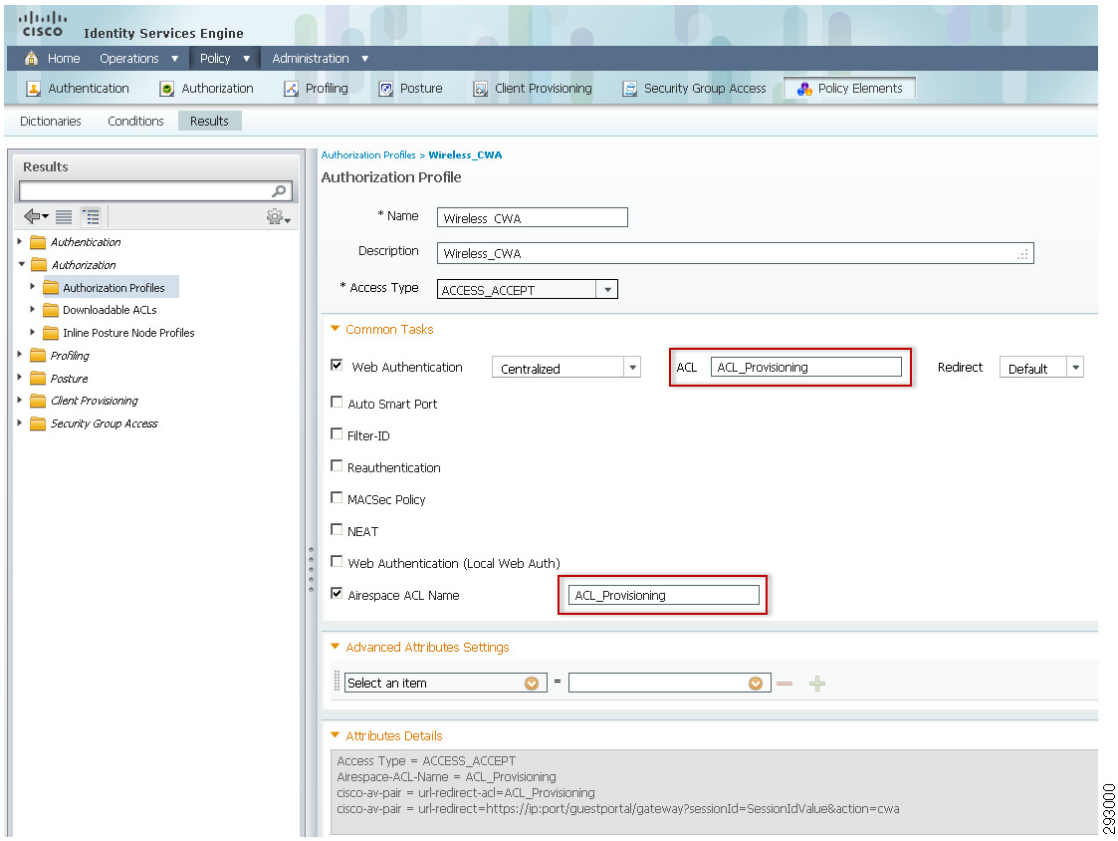
In addition to the standard PermitAccess and DenyAccess authorization profiles, the following are some of the profiles that are defined within this design guide:

- Wireless_CWA—This profile is used for redirection of wireless devices to the registration portal for devices using MAB.
- Wired_CWA—This profile is used for redirection of wired devices to the registration portal when they access the network using MAB.
- Wireless_NSP—This profile is used to redirect wireless users to registration portal when they access the network using dot1x or a single SSID.

Wireless_CWA

This policy is used to redirect Wireless MAB users to a registration portal when they connect to the network. There is also an ACL that is enforced as part of enforcing this policy. As explained in the WLC design, the provisioning SSID needs to be enforced with an ACL to prevent registered users from accessing any internal resources if they continue to stay associated to a Provisioning SSID without switching to a secure SSID. To configure this authorization policy, click **Policy > Policy Elements > Results > Authorization Profiles**, as shown in Figure 77.

Figure 77 Wireless_CWA Authorization Profile



The objective of Provisioning_ACL is:

- Permit access for endpoints to reach ISE in both directions.
- Permit access for endpoints to reach DNS, DHCP server.
- Deny everything else.

Figure 78 displays how to configure the Provisioning ACL on the WLC. This is just an example, since each organization will have unique business policies and security requirements.

Figure 78 WLC Access List for Provisioning

General

Access List Name ACL_Provisioning

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.225.41.114 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
2	Permit	10.225.41.114 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
3	Permit	0.0.0.0 / 0.0.0.0	10.225.41.115 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
4	Permit	10.225.41.115 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
5	Permit	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
6	Permit	173.194.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
7	Permit	0.0.0.0 / 0.0.0.0	74.125.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Permit	74.125.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
9	Permit	0.0.0.0 / 0.0.0.0	206.111.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
10	Permit	206.111.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
11	Permit	0.0.0.0 / 0.0.0.0	10.225.50.28 / 255.255.255.255	TCP	Any	HTTP	Any	Inbound	0
12	Permit	10.225.50.28 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Outbound	0
13	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

293001

In this case, the IP addresses 10.225.41.114 and 10.225.41.115 are the ISE's IP addresses and 10.230.1.45 and 10.230.1.46 are the DNS/DHCP server addresses.

Note Android devices require access to Google's Play Store to download the SPW package. Modify the ACL to allow endpoints to download the SPW.

Once the authorization profile is defined on the ISE and the ACL is configured on the WLC, then the next logical step is to tie them together in the authorization policy. Define the authorization rule for MAB by clicking **Policy > Authorization**, as shown in Figure 79.

Figure 79 Authorization Rule

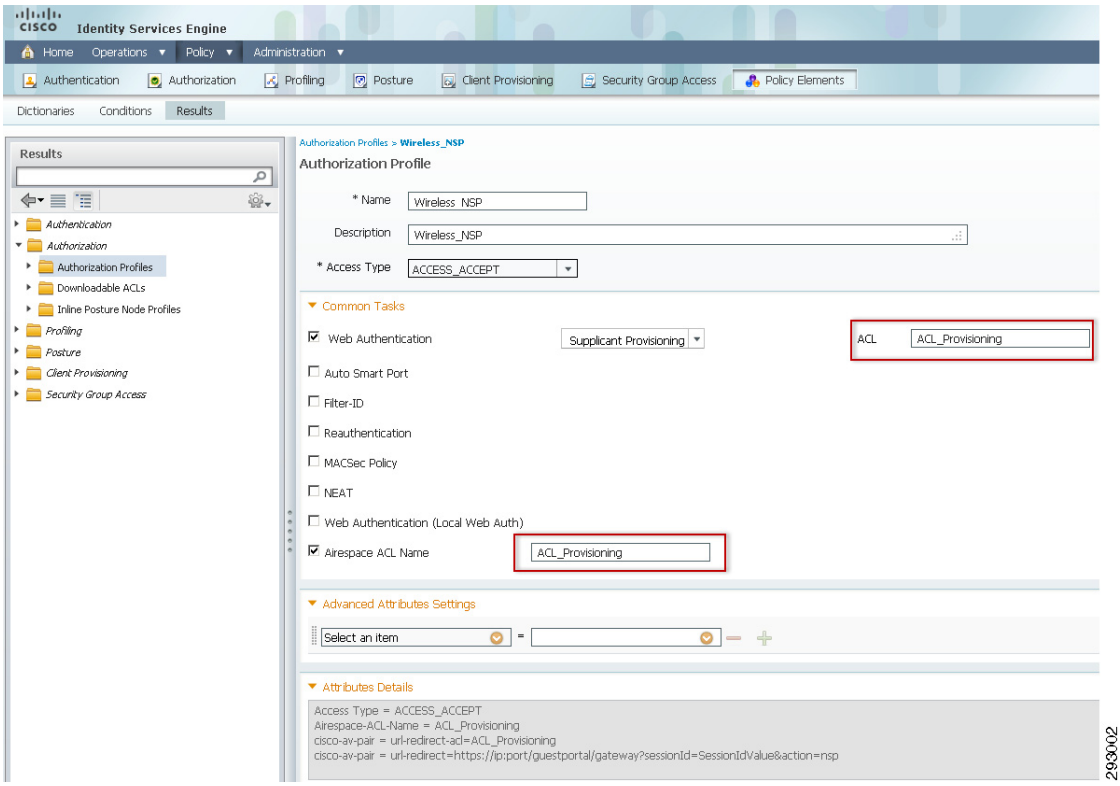
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless_MAB_AuthZ	if Wireless_MAB	then Wireless_CWA

292630

Wireless_NSP

This authorization profile is used to redirect the devices that connect to the network using authentication protocol as PEAP. The difference between the previous authorization profile, "Wireless_CWA", and this profile is that the Web Authentication needs to be configured as supplicant provisioning. To configure this authorization policy, click **Policy > Policy Elements > Results > Authorization Profiles**, as shown in Figure 80.

Figure 80 Wireless_NSP Authorization Profile



The ACL_Provisioning is same as the one shown in Figure 78.

The next logical step is to use the authorization profile in the authorization policy. Figure 81 shows the authorization rule defined under the authorization policies.

Figure 81 Authorization Rule

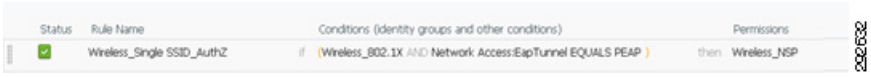
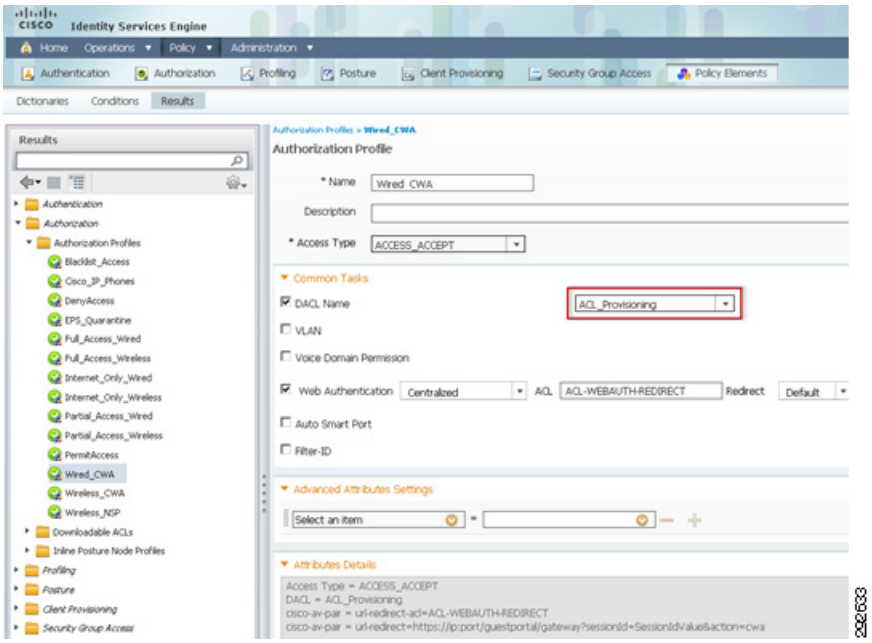


Figure 82 Wired_CWA Authorization Profile

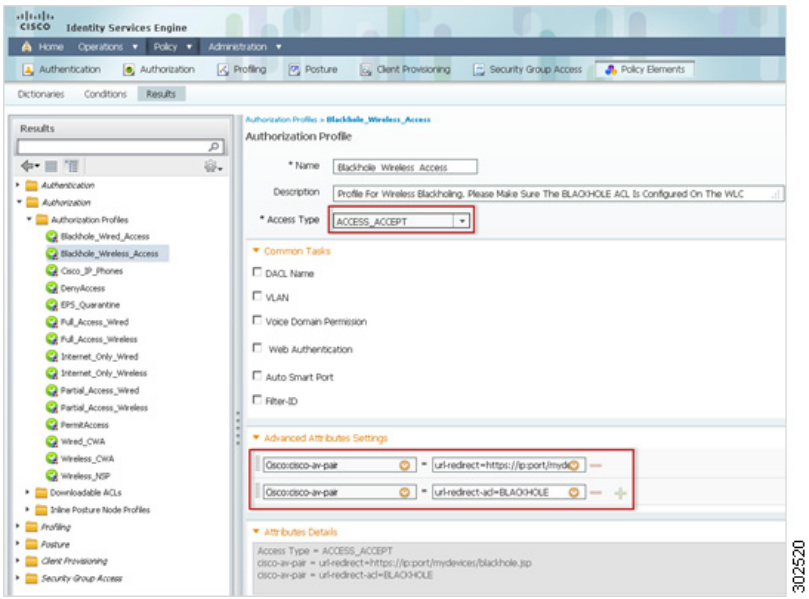


The ACL-WEBAUTH-REDIRECT needs to be defined on the access layer switch.

Blackhole_Wireless_Access

This authorization profile is primarily used to reject the connection initiated by the user. This is required when a user reports a lost or stolen device and the device needs to be removed from the network or prevented from initiating connection to the network. This authorization profile is system generated. Figure 83 shows the Blackhole_Wireless_Access authorization profile.

Figure 83 Blackhole_Wireless_Access



The next logical step is to tie this authorization profile to the authorization policy. Figure 84 shows the authorization rule defined under the authorization policies.

Figure 84 Authorization Rule

Certificate Authority Server

The Certificate Authority server is the central authority for distributing digital certificates. A Windows 2008 CA server was used as the CA server for this solution. The following are important design considerations that should be taken into account:

- Network Device Enrollment Service, which is Microsoft's implementation of SCEP.
- Certificate Templates and how to design them.

NDES Server Configuration for SCEP

The Network Device Enrollment Service (NDES) is the Microsoft implementation of the SCEP, a communication protocol that makes it possible for network devices to enroll for X.509 certificates from a CA. To distribute and deploy digital x.509 client certificates to users, the Microsoft Network Device Enrollment Service (NDES) was utilized in conjunction with a Microsoft CA Server. For more details on how to implement NDES, see: http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx.

By default, the NDES service is configured to present one-time enrollment passwords for certificate enrollment. The use of one-time passwords by the NDES service is typically used to allow network and IT administrators to enroll certificates for network devices within the IT organization. However, in this solution this feature is disabled because remote endpoints are authenticated by using their RSA SecurID tokens.

Disabling the "one-time password" on the NDES server is configured in the following registry key: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword.

EnforcePassword value data is set to "0", which ensures no password is requested by NDES.

Note Windows Server 2003, Microsoft SCEP (MSCEP) required a Resource Kit add-on to be installed on the same computer as the CA. In Windows Server 2008, MSCEP support has been renamed NDES and is part of the operating system. NDES may be installed on a different computer than the CA (http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx).

The NDES extension to IIS uses the registry to store configuration settings. All settings are stored under one registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP

Important

It is possible for the ISE to generate URLs which are too long for the IIS. To avoid this problem, the default IIS configuration may be modified to allow longer URLs. The following command should be run on a command line with administrative privileges:

```
%systemroot%\system32\inetsrv\appcmd.exe set config
  /section:system.webServer/security/requestFiltering
  /requestLimits.maxQueryString:"6044"
  /commit:apphost
```

Certificate Template

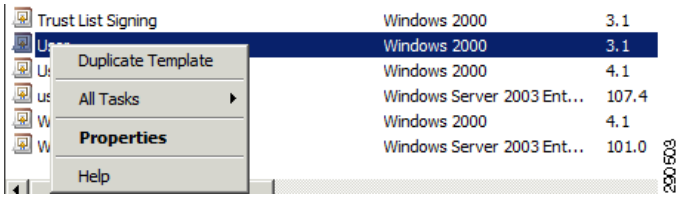
Digital certificates can be used for different purposes like server authentication, secure E-mail, encrypting the file system, and client authentication. Hence, it is important that a client is issued a certificate which serves its purpose. For example, a Web server may need a certificate for server authentication. Similarly, a normal client needs a certificate mainly for client authentication. Therefore, certificate templates are needed to properly distribute certificates to users based on their specific needs. In this solution, a security template has been created on the Microsoft Windows 2008 CA server so that users can obtain the proper certificate. This section describes important steps to set up the certificate template on the Windows CA server and specific actions needed by the user.

For more information on certificate templates, see:
http://technet.microsoft.com/en-us/library/cc730826%28WS.10%29.aspx.

SCEP is used as a protocol by the endpoints to obtain their digital certificates from the CA server. The endpoints send the certificate requests to ISE, which forwards the requests to the CA server. ISE is configured as SCEP Proxy to handle these requests and once the CA server issues the certificates, ISE sends the certificates back to the clients. The properties of the "User" template are being used. That is a default template in the Microsoft Server 2008 R2 CA Server deployment. Default templates in Microsoft Server 2008 R2 cannot be edited. Therefore, a customized template can be built that gives an administrator more flexibility in defining the certificate options. This section describes how to create a customized template named "user2" in this example.

The first step is to create a duplicate template from the pre-defined list of templates. Figure 85 shows how to create a duplicate template.

Figure 85 Creating a Duplicate Template

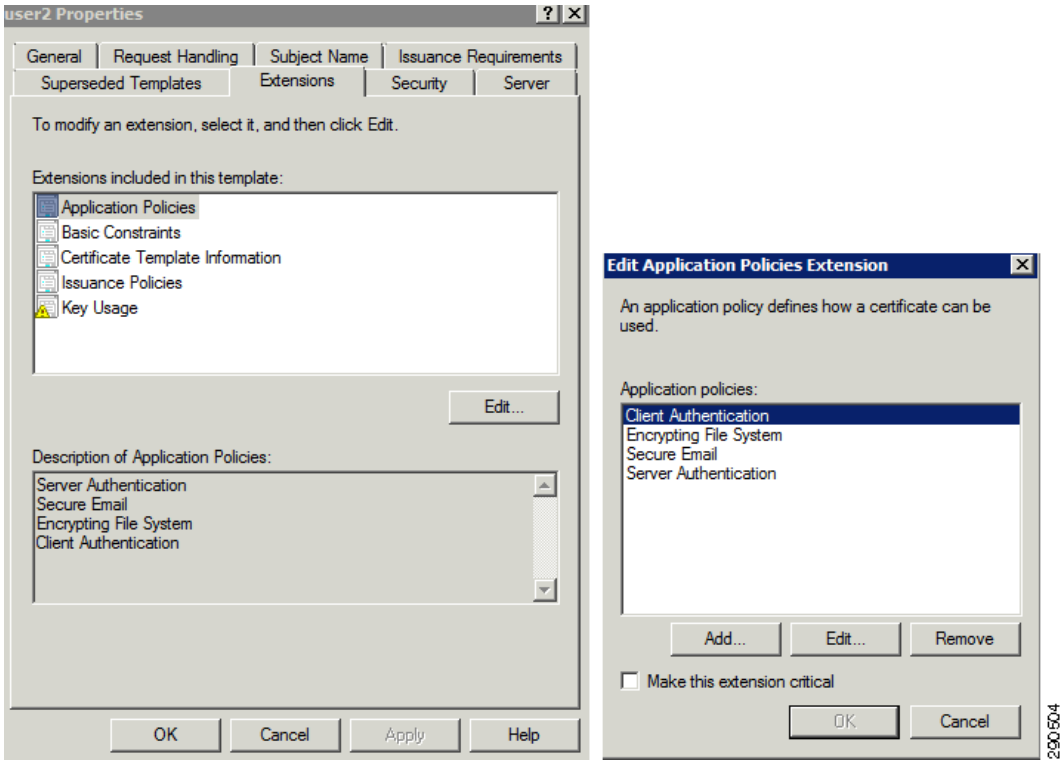


The default "User" template was copied and renamed "user2". Then the "user2" template was used to auto-enroll AnyConnect VPN clients with client certificates using this newly created template.

The next step is to configure the extensions of the certificates that are derived from the "user2" template. The EKU extension and extended property specify and limit the valid uses of a certificate. The extensions are part of the certificate itself. They are set by the issuer of the certificate and are read-only. Certificate-extended properties are values associated with a certificate that can be set in an application. To obtain more information about extended properties, see:
http://msdn.microsoft.com/en-us/library/aa380252%28v=vs.85%29.aspx.

Figure 86 describes how to configure the extended properties for the certificates.

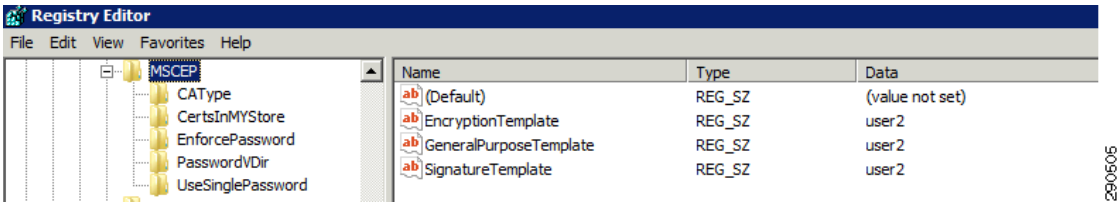
Figure 86 Configuring Extended Properties for Certificates



Notice the template named “user2”. This value must be set in the registry as it correlates to the “user2” template, which was copied from the “User” template in the “Certificate Templates Console” on the CA Server.

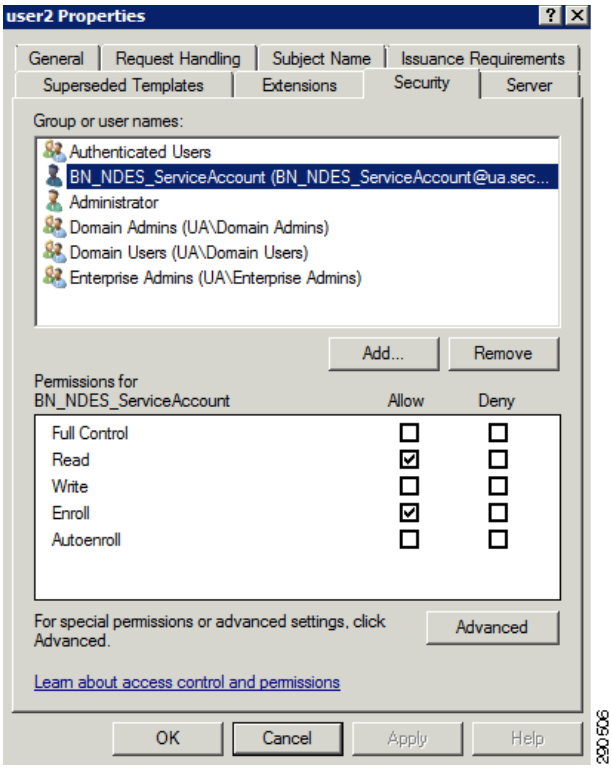
Figure 87 describes how the registry setting must be modified to reflect the newly-created template “user2”.

Figure 87 Modifying the Registry



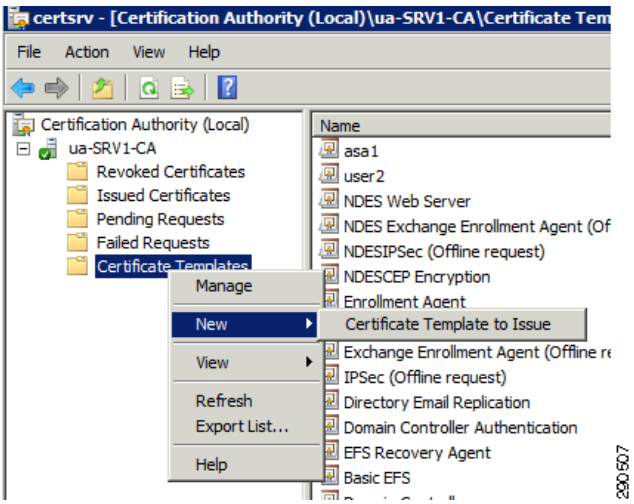
Once the template has been duplicated, the permissions are set for the NDES_ServiceAccount on the “user2” template to Read and Enroll. Figure 88 displays the Read and Enroll permissions that have been set for the NDES_ServiceAccount on the “user2” template.

Figure 88 Read and Enroll Permissions



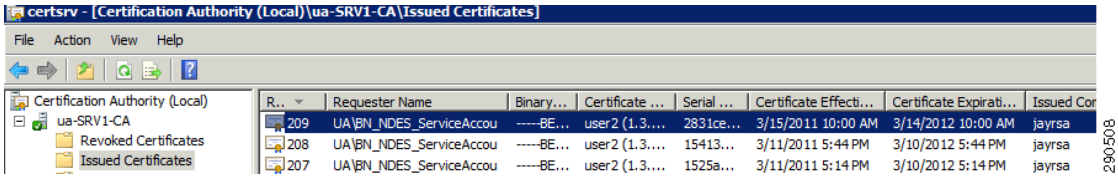
Ensure that the newly created "user2" template is available to be issued via the CA. Right click **Certificate Templates > New > Certificate Template to Issue** and choose the newly-created "User2 Certificate", as shown in Figure 89.

Figure 89 Ensuring Template is Available From CA



Now the certificate template is fully configured and can be used by users to submit enrollment requests. Figure 90 shows a successful enrollment request to the "user2" template that was submitted by a user, "jayrsa".

Figure 90 Successful Enrollment Request



A successful auto-enrollment request has occurred on the CA Server. Notice that the requester name is the NDES Service Account that is configured for Read and Enroll permissions and also notice that the "user2" certificate template was chosen.

Wired Infrastructure Design

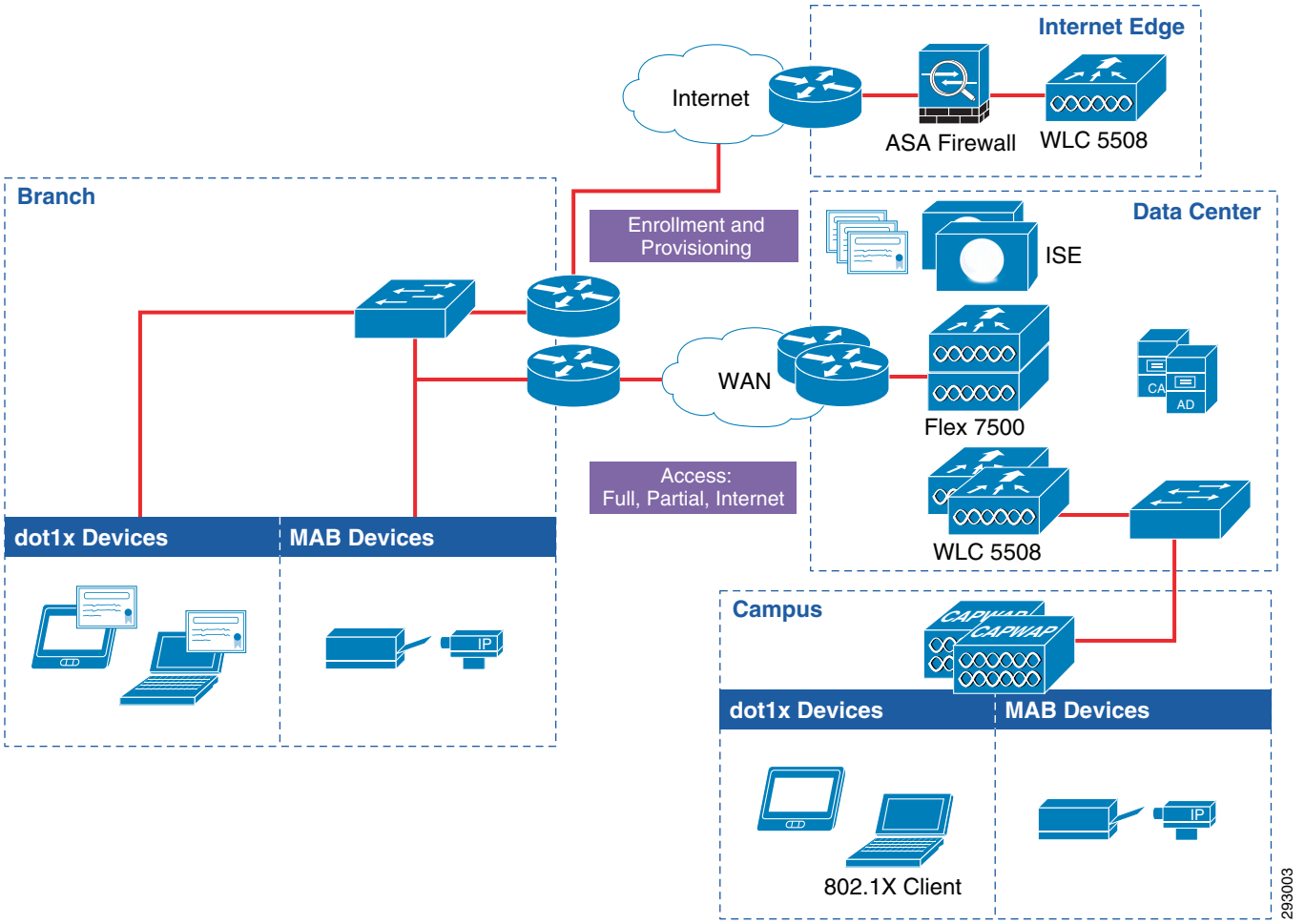
Various devices connect to the branch access layer switch, such as Access Points, laptops, computers, and MAB devices like printers, cameras, and so on. Regardless of the device type, the key requirement of wired infrastructure is to identify the device/user combination and enforce different policies on the device. This design also addresses the requirement of providing access to servers at the branch locations with different security policies, e.g. full, partial, or denies access. This section discusses the key infrastructure requirements.

At a branch location, there are 802.1X capable clients that go through the provisioning/enrollment process and there are other types of devices like printers, cameras, etc. which do not have 802.1 X capabilities and can only provide their MAC address as their source of authentication. These devices also will need to access the network and this design allows them to authenticate/authorize and obtain their authorization policy from ISE.

Network Architecture

Figure 91 shows an end-to-end network architecture diagram that includes wired device access from the branch or campus locations.

Figure 91 Network Access Protocols at Branch Location



VLAN Design at Branch Locations

Four VLANs are implemented at the branch location. Table 9 illustrates the names of these VLANs and the purpose of each.

Table 9 VLANs and Purpose

VLAN Name	VLAN Number	Description
Wired_Full	13	Devices placed in this VLAN get full access to corporate resources and branch local servers.
Wired_Partial	14	Devices placed in this VLAN get restricted access to resources.
Wired_Internet	15	Devices placed in this VLAN get only Internet access only.
Branch_Server	16	Local Servers at branch location are placed in this VLAN.

IP Address Allocation at Branch Location

In the branch network design discussed in this design guide, the switch performs Layer 2 functions only and the branch router performs Layer 3 routing. Hence, all the Layer 3 interfaces for the VLANs mentioned above are implemented at the branch router. The following is an example configuration of the branch router:

```
interface GigabitEthernet0/1.13
 encapsulation dot1Q 13
 ip address 10.200.13.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 13 ip 10.200.13.1
 standby 13 priority 110
 standby 13 preempt
!
interface GigabitEthernet0/1.14
 encapsulation dot1Q 14
 ip address 10.200.14.2 255.255.255.0
 ip access-group Branch1_ACL_Partial_Access i
 ip helper-address 10.230.1.61
 standby 14 ip 10.200.14.1
 standby 14 priority 110
 standby 14 preempt
!
interface GigabitEthernet0/1.15
 encapsulation dot1Q 15
 ip address 10.200.15.2 255.255.255.0
 ip access-group ACL_Internet_Only in
 ip helper-address 10.230.1.61
 standby 15 ip 10.200.15.1
 standby 15 priority 110
 standby 15 preempt
!
interface GigabitEthernet0/1.16
 encapsulation dot1Q 16
 ip address 10.200.16.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 16 ip 10.200.16.1
 standby 16 priority 110
 standby 16 preempt
!
```

As seen above, the Layer 3 interfaces are configured with the **ip-helper address** command, which helps branch clients obtain an IP address. For the purposes of this design guide, the DHCP server is in a data center location.

ACL Design at Branch Location

ACLs are very important at the branch location, since they are the main method used to enforce policies. Some ACLs are defined on the Layer 2 switch for provisioning purposes, while others are defined on the branch router. In addition, some ACLs may be downloaded from the ISE.

Table 10 summarizes the various ACLs at branch location and their purpose.

ACL-DEFAULT—This ACL is used as a default ACL on the port and its purpose is to prevent un-authorized access. In an 802.1X authentication/authorization scenario, after the device is authenticated and authorized, if there is no dACL applied to the port or if there is a mistake in the syntax of the downloadable ACL and the switch rejects the dACL sent by ISE, ACL-DEFAULT protects the port in the above mentioned scenarios. An example of a default ACL is shown below:

```
bn22-3750x-1#show ip access-lists
Load for five secs: 13%/0%; one minute: 16%; five minutes: 16%
Time source is NTP, 16:24:50.872 EDT Wed Sep 19 2012

Extended IP access list ACL-DEFAULT
  10 permit udp any eq bootpc any eq bootps
  20 permit udp any any eq domain
  30 permit icmp any any
  40 permit udp any any eq tftp
  50 deny ip any any log
```

As seen from the output above, ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

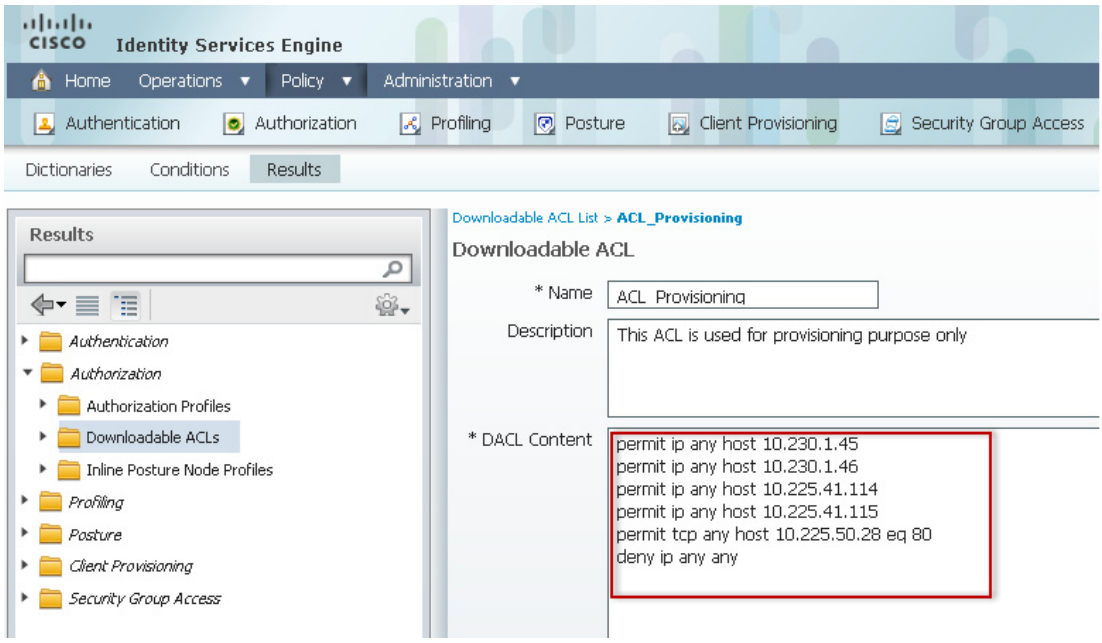
ACL-WEBAUTH-REDIRECT—This ACL triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere, which means that when the user opens a Web browser and attempts to access any Website, that traffic is re-directed. The example shown below redirects any Web traffic initiated by the user. However, this ACL can be modified to allow only certain traffic to be redirected to ISE portal. The underlying assumption in this design is that all the devices must be registered with ISE, therefore when an un-registered device accesses the network, it is redirected to ISE.

```
bn22-3750x-1#show ip access-lists | begin ACL-WEBAUTH-REDIRECT
Extended IP access list ACL-WEBAUTH-REDIRECT
  10 deny udp any any eq domain
  20 permit tcp any any eq www
  30 permit tcp any any eq 443
```

Provisioning ACL

This dACL is downloaded from the ISE and restricts access to only the ISE, DNS, and DHCP server. This ACL is defined on the ISE, as shown in Figure 92.

Figure 92 ACL_Provisioning



The following considerations need to be taken into account while designing the wired infrastructure:

- This design uses MAB protocol to provision all the wired devices. The authentication and authorization policies are designed to match for provisioning of these endpoints. The dot1x protocol is used by the endpoints after they have been provisioned. To support both MAB and dot1x protocols, every port is configured for both of the protocols.
- It is assumed that initially all the wired devices do not have dot1x configured and that after the device is provisioned, then the device starts communicating using dot1x protocol. After the device is authenticated, an authorization policy is downloaded to the switch from ISE in the form of a dACL. The authorization policy is based on the use cases and it changes based on the security policy. To obtain more information on authorization policy design, refer to Enhanced BYOD Access.

Port Configuration of Wired Switches

A Cisco Catalyst Switch is used to provide end user Ethernet connectivity into the network in this design guide. The access layer switch enables 802.1X authentication for the client devices and interacts with the Identity Services Engine using the RADIUS protocol. Based on the results from the authentication process, a user may be allowed restricted or full access into the network using a VLAN assignment and a downloadable Access Control List (dACL). The flex-authentication configuration described below allows for using both 802.1X and MAC Authentication Bypass (MAB) as a fallback mechanism. Flex-auth is useful for devices that do not have 802.1X support such as printers. The configuration for ISE to enable MAB is outside the scope of this document.

The following steps are required to configure the access switch for AAA:

Step 1 Enable Authentication, Authorization, and Accounting (AAA):

```
ACL(config)# aaa new-model
```

Step 2 Create an authentication method for 802.1X (default use all RADIUS servers for authentication):

```
ACL(config)# aaa authentication dot1x default group radius
```

Step 3 Create an authorization method for 802.1X (enables RADIUS for policy enforcement):

```
ACL(config)# aaa authorization network default group radius
```

Step 4 Create an accounting method for 802.1X (provides additional information about sessions to ISE):

```
ACL(config)# aaa accounting dot1x default start-stop group radius
```

The following steps are required to configure the access switch for RADIUS:

Step 1 Add ISE server to the RADIUS group:

```
ACL(config)# radius-server host 10.225.41.115 auth-port 1812 acct-port 1813 key
shared-secret
```

Step 2 Configure ISE server dead time (15 seconds total—3 retries of 5 second timeout):

```
ACL(config)# radius-server dead-criteria time 5 tries 3
```

Step 3 Configure the switch to send Cisco Vendor-Specific attributes:

```
ACL(config)# radius-server vsa send accounting
ACL(config)# radius-server vsa send authentication
```

Step 4 Configure the Cisco Vendor-Specific attributes:

```
ACL(config)# radius-server attribute 6 on-for-login-auth
ACL(config)# radius-server attribute 8 include-in-access-req
ACL(config)# radius-server attribute 25 access-request include
```

Step 5 Configure IP address to be used to source RADIUS messages:

```
ACL(config)# ip radius source-interface interface-name Vlan4093
```

The following steps are required to configure the access switch for 802.1X:

Step 1 Enable 802.1X globally (command by itself does not enable authentication on the switchports):

```
ACL(config)# dot1x system-auth-control
```

Step 2 Enable IP device tracking:

```
ACL(config)# ip device tracking
```

The following interface level commands enable 802.1X for Flex-Auth:

Step 1 Configure the authentication method priority (dot1x has higher priority over MAB):

```
ACL(config-if)# authentication priority dot1x mab
```

Step 2 Configure the authentication method order (dot1x first):

```
ACL(config-if)# authentication order dot1x mab
```

Step 3 Enable Flex-Auth:

```
ACL(config-if)# authentication event fail action next-method
```

Step 4 Enable support for more than one MAC address on the physical port:

```
ACL(config-if)# authentication host-mode multi-auth
```

Step 5 Configure the violation action (restrict access for additional devices that may fail authentication):

```
ACL(config-if)# authentication violation restrict
```

Step 6 Enable port for 802.1X:

```
ACL(config-if)# dot1x pae authenticator
```

Step 7 Enable port for MAB:

```
ACL(config-if)# mab
```

Step 8 Configure timers (30 seconds (10x3) until falling back to MAB):

```
ACL(config-if)# dot1x timeout tx-period 10
```

Step 9 Turn authentication on:

```
ACL(config-if)# authentication port-control auto
```

Step 10 Enable http and https server:

```
ACL (config)# ip http-server
ACL (config)# ip http secure-server
```

MAB Devices at Branch or at Campus Location

MAB devices are generally those devices that cannot run 802.1X and can only present their mac-address for authentication. It is important to note that the BYOD devices also use the MAB protocol during the provisioning process. During the provisioning process, BYOD devices are re-directed to the ISE guest port for completing the registration process. MAB devices do not need to be registered and therefore do not need to be re-directed. The requirement for MAB devices is to authenticate the device and apply an authorization policy. Here are the high level steps that need to be performed for MAB devices:

1. Configure the access layer switch port or WLC to support MAB protocol.
2. Import a mac-address list of all MAB devices as an Identity group in ISE.
3. Configure an authentication policy for Wired and Wireless MAB devices. This same policy will be used to authenticate BYOD devices during provisioning.
4. Configure an authorization policy rule in ISE for wired and wireless devices.

When a MAB device connects, the access layer switch sends the authentication request to the ISE using mac-address as the source of authentication. An example is shown below.

```
Sep 25 11:09:50.741: %DOT1X-5-FAIL: Authentication failed for client (0050.568f.
1bb2) on Interface Gi1/0/10 AuditSessionID 0AC81304000002212 92C2D59
Sep 25 11:09:50.741: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
 'dot1x' for client (0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC813
0400000221292C2D59
Sep 25 11:09:50.749: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (
0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC81304000002212 92C2D59
Sep 25 11:09:50.749: %AUTHMGR-5-START: Starting 'mab' for client (0050.568f.032b
) on Interface Gi1/0/10 AuditSessionID 0AC81304000002212 92C2D59
```

All the MAC addresses of the MAB design are placed in an internal identity group called MAB_DEVICES, so ISE will know this device in advance. To add new MAC addresses to the MAB_DEVICES identity group, click **Administration > Groups > Endpoint Identity Groups**, as shown in Figure 93.

Figure 93 MAB_DEVICES Identity Group

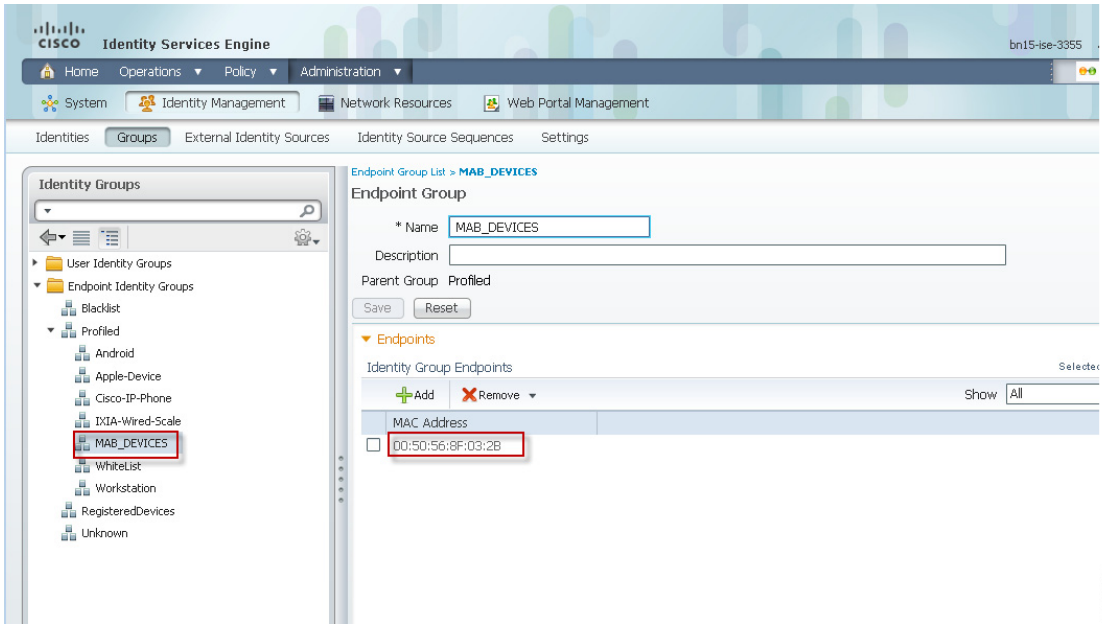
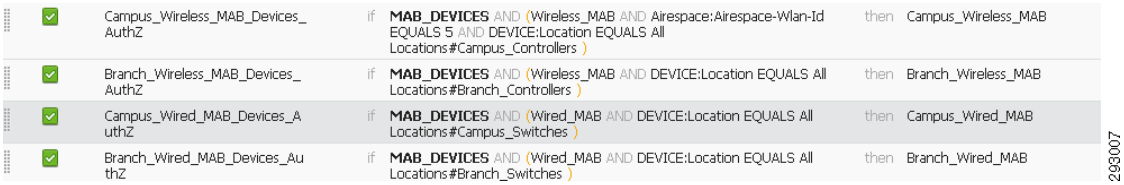


Figure 94 shows the authentication policy defined on the ISE for wired MAB devices.

Figure 94 WIRED_MAB_AuthC

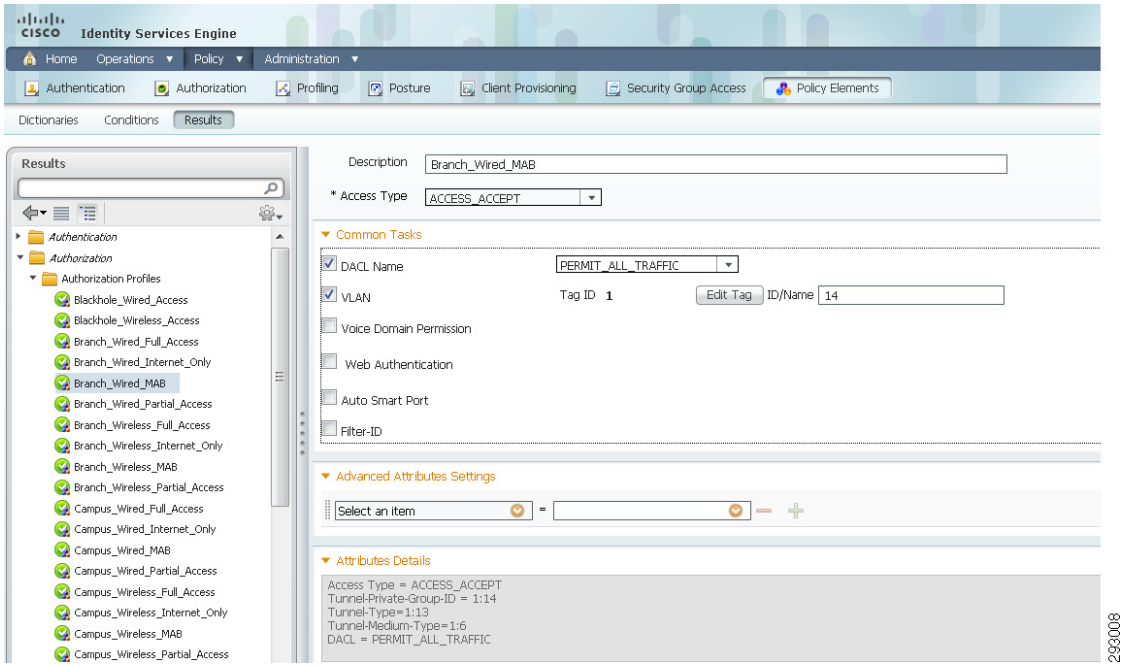
The authorization policy is different for MAB devices originating in the branch versus in the campus location. This is because in the branch, every device is placed in different VLANs, but this is not done in the campus. Hence there are different rules that are defined in the authZ policy to take care of location of the device—branch versus campus. The authorization policy is defined such that if authentication protocol is “Wired_MAB”, and the device belongs to the MAB_DEVICES identity group, then an appropriate authZ profile is applied. Figure 95 shows the defined authZ policy.

Figure 95 MAB_Wired_Devices AuthZ



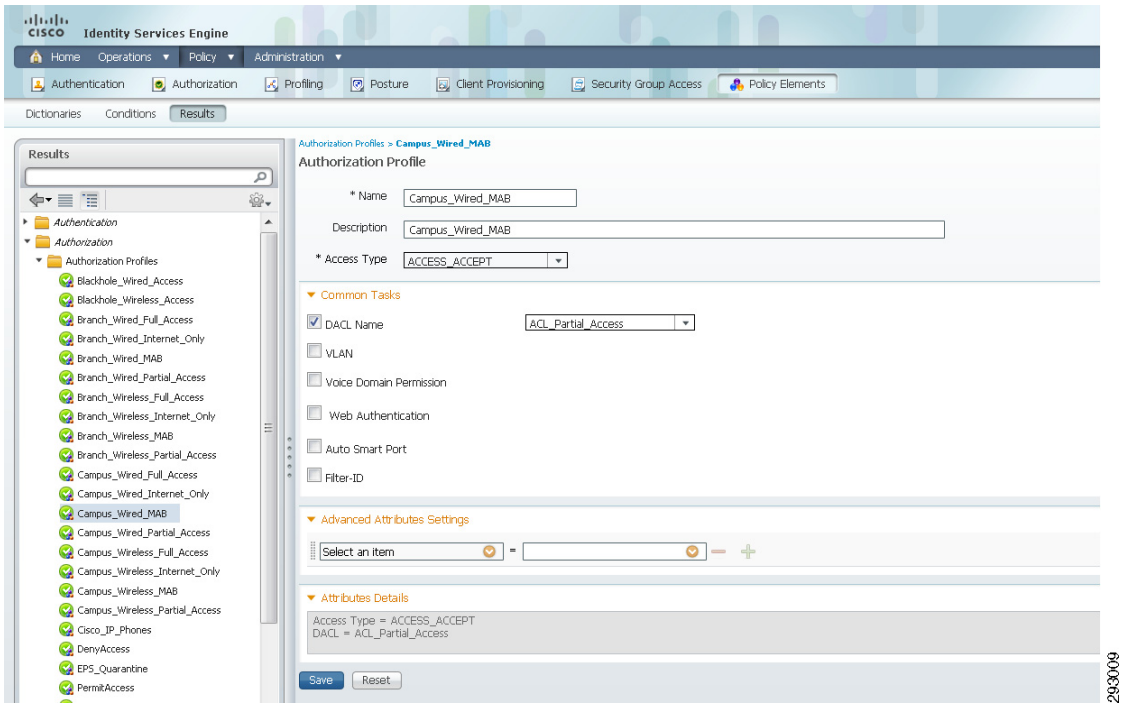
Branch_Wired_MAB is an authorization profile that pushes the appropriate settings to the access layer switch. Figure 96 shows the Branch_Wired_MAB Authorization Profile.

Figure 96 Branch_Wired_MAB



The Campus Authorization profile does not push VLAN information, but rather applies a dACL to the port. Figure 97 shows the authZ profile for MAB devices at the campus location.

Figure 97 authZ Profile for MAB Devices at the Campus



Wireless_MAB devices follow the same logic as wired devices. Wireless_MAB devices also need to be placed in the MAB identity group and, based on the location of the device, the appropriate authZ profile is pushed to the device.

Enhanced BYOD Access

This section defines the design scenarios for deploying BYOD for personal device access and the design considerations for each scenario. It also highlights how to deny access to personal devices based on the device type. The steps taken by the user to on-board the devices are explained at the end of the section.

One of the main objectives of a BYOD solution is to provide a simple way for employees to on-board their personal devices without requiring assistance from IT. Since the BYOD needs of the majority of employees will be met with either simple Internet access or Partial access, the only time an employee requires assistance from IT is when they require full access to corporate resources.

Cisco ISE provides different ways to define security policies and determine what network resources each employee is allowed to access. The security policies are then enforced throughout the network infrastructure. The ISE feature set is extremely flexible, enbaling different business policies to be enforced. This section explains the steps to on-board personal devices and how to apply different policies.

Figure 98 shows how a personal device is profiled and registered by ISE and the different network components (WLC, AD, CA) that play a role in the process. Different conditions are evaluated to provide the proper authorization and access to network resources, including digital certificates, Active Directory groups, etc.

Figure 98 Provisioning Personal Devices

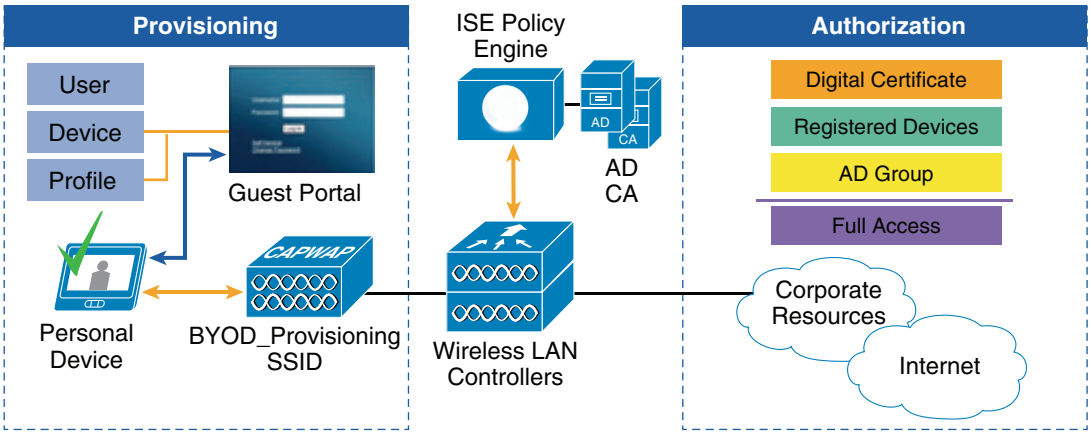


Figure 99 shows how a personal device is restricted from accessing the network. After the user authenticates, ISE profiles the device and enforces the DenyAccess authorization rule.

Figure 99 Deny Access

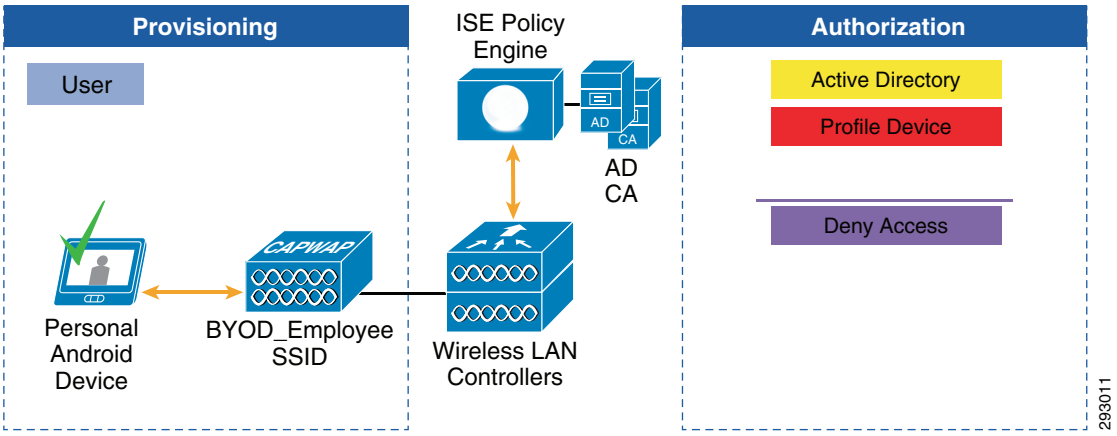


Figure 100 shows the different permission levels configured in this section. These access levels are enforced using various mechanisms, including Access Control Lists (ACLs) in the Wireless LAN Controller or Catalyst switches and VLAN assignment with FlexConnect ACLs in access points.

Figure 100 Permission Levels for Personal Devices

	Permission	Access
	Full Access	Internet plus all corporate resources
	Partial Access	Internet plus some corporate applications
	Internet Only	Internet Only
	Deny Access	Explicitly deny network access

292642

Identity Groups and Active Directory

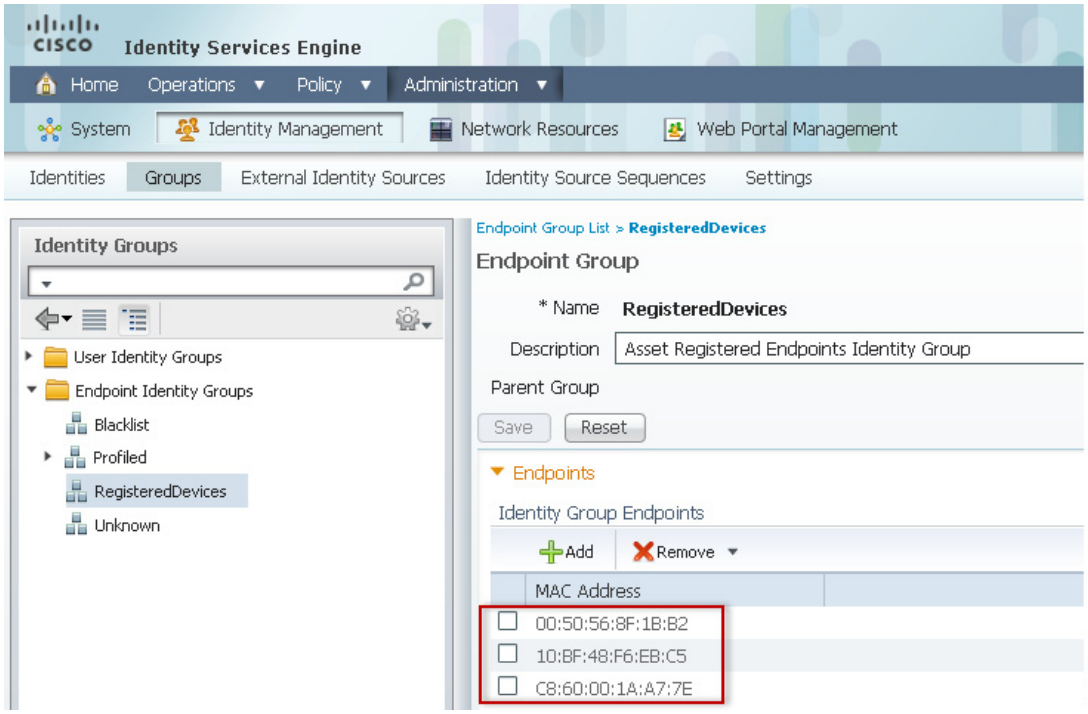
An identity group is a logical list used to group endpoints according to their profiles. Devices that have gone through the self-provisioning and registration process get added to the RegisteredDevices identity group in ISE. The identity group is used in the authorization policies to assign network access privileges for endpoints or enforce other rules.

Endpoints may be moved to other identity groups, such as the Blacklist identity group, used when a devices is lost or stolen. Managing a Lost or Stolen Device has more details on this identity group.

Note Endpoints can only be members of one identity group at a time.

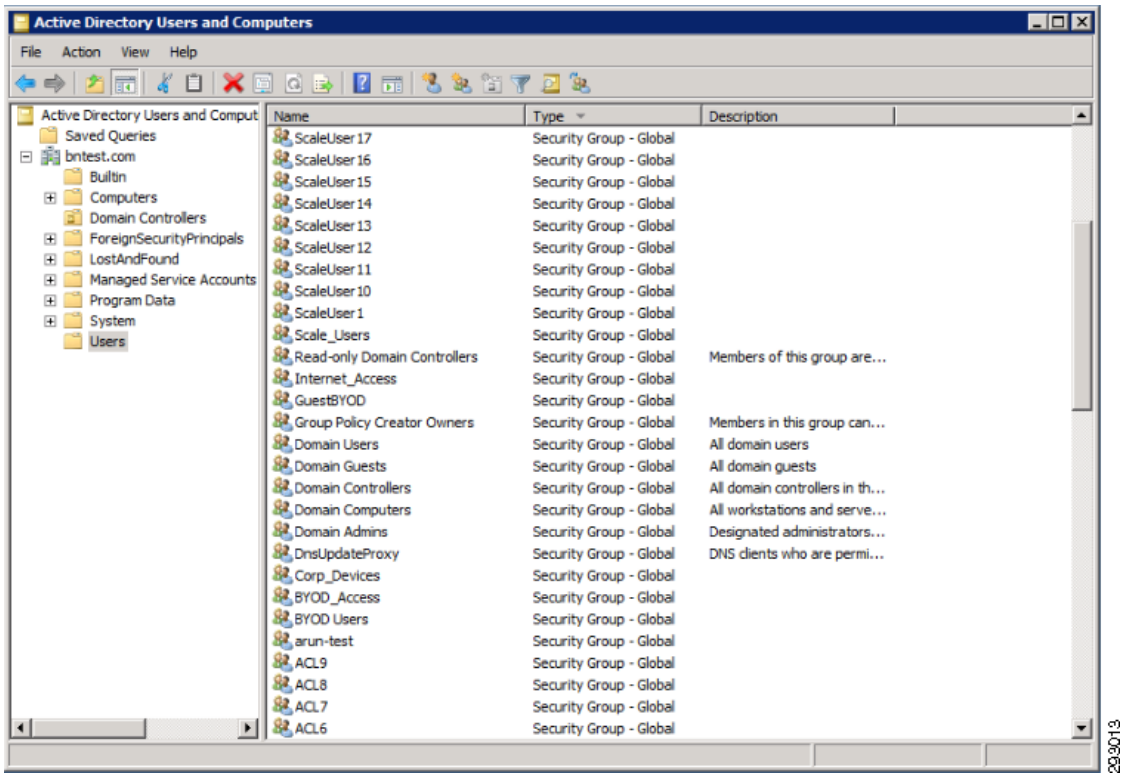
To update an endpoint's identity group, click **Administration > Groups > Endpoint Identity Groups**. Figure 101 shows three endpoints as members of the RegisteredDevices identity group.

Figure 101 RegisteredDevices Identity Group



Active Directory groups can be used as an additional way to grant access to different users. Figure 102 shows some of the Active Directory groups used in this section.

Figure 102 Active Directory Groups



This section relies on the following three AD groups:

- BYOD_Access—Members of this group are allowed full access. Since this group is maintained by an IT administrator, it is expected to have a small percentage of users.
- Domain Users—Since all employees are already members of this Active Directory group, employees that register their devices through the Guest Registration portal are automatically granted Partial Access. Users are able to access the Internet and a subset of corporate applications, such as E-mail, corporate directory, travel tools, etc.
- Internet_Access—Members of this group are granted only access to the Internet. For convenience, the administrator may decide to add a large number of employees to this group.

This model could easily be expanded to include other user groups with similar access requirements. A good example would be to create a new group and access list to grant access to contractors or partners.

Figure 103 highlights the different access policies tested in this section, along with the different requirements and permissions granted by each policy. These policies, along with detailed configurations, are explained later in this section.

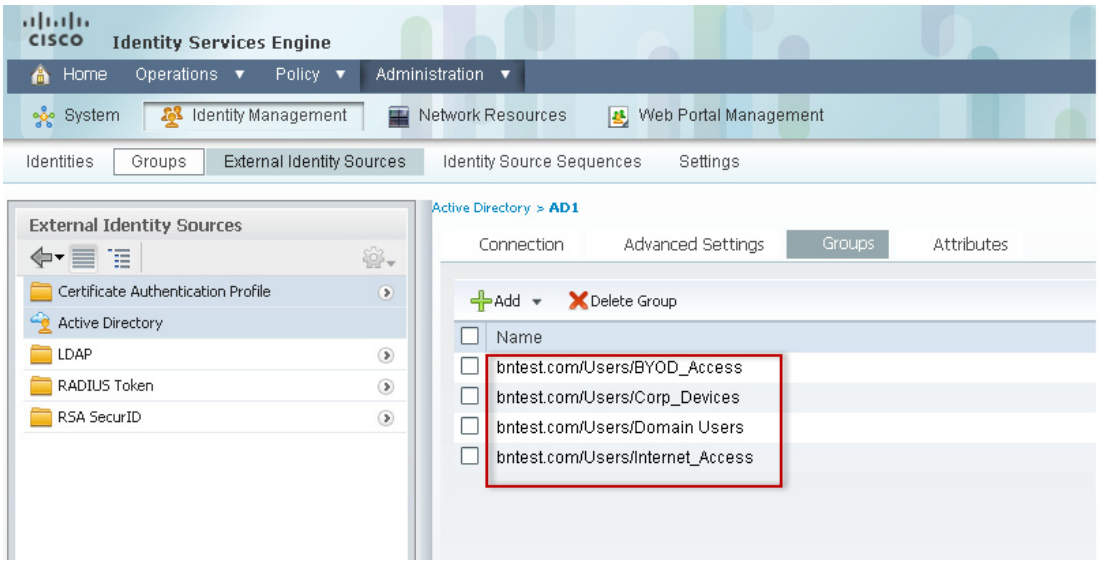
Figure 103 Access Policies and Permissions

Policy	Identity Group	AD Group	Profile	Permission	
Personal_Full Access	RegisteredDevices	BYOD_Access		Full	
Personal_Partial Access	RegisteredDevices	Domain Users		Partial	
Personal_Internet Only	RegisteredDevices	Internet_Access		Internet Only	
Deny Android Devices			Android	Deny	

292644

To configure the Active Directory groups that are available for use in the authorization policy conditions, click **Administration > Identity Management > External Identity Sources > Active Directory > Groups** and check the boxes next to the groups that will be used in the policy conditions and rules. Figure 104 includes the groups used in this design guide.

Figure 104 Active Directory Groups



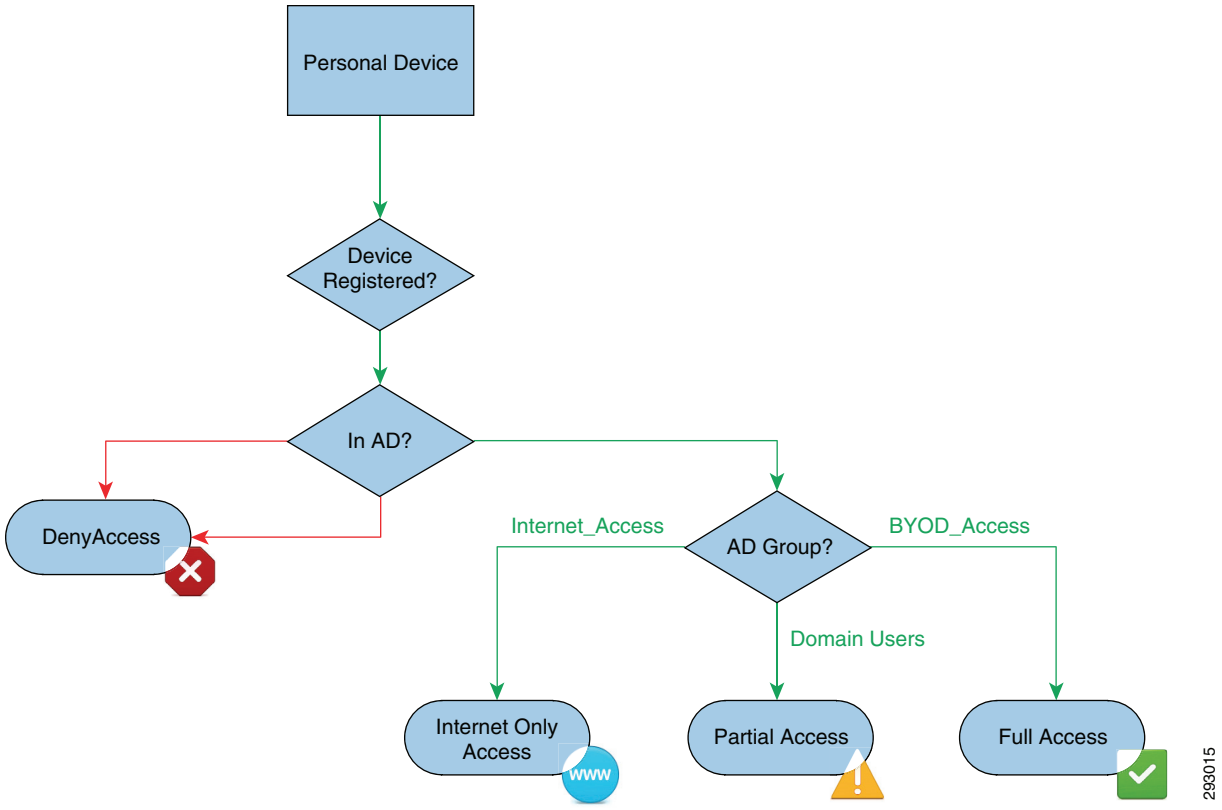
This section assumes that once employees on-board their devices:

- To obtain Full Access, the employee must be a member of the BYOD_Access Active Directory group.
- Employees are granted Partial Access based on their membership in the Domain Users group.
- Employees that belong to the Internet_Access group are granted Internet Only Access.

Figure 105 highlights the connectivity flow for personal devices. The first decision to evaluate is whether the endpoint belongs to the RegisteredDevices identity group, meaning the device has been on-boarded. If the device is not in the RegisteredDevices identity group, profile the device and deny access to Android devices.

If the endpoint is a member of the RegisteredDevices identity group and has been on-boarded with a digital certificate, the next step is to evaluate the AD group membership and enforce a permission for each group.

Figure 105 Personal Device BYOD Access



Distributing Digital Certificates

Digital signatures, enabled by public key cryptography, provide a means to authenticate devices and users. In public key cryptography, such as the RSA encryption system, each user has a key pair containing both a public and a private key. The keys act as complements and anything encrypted with one of the keys can be decrypted with the other.

A digital signature is encrypted with the sender's private key. The signature must be verified to confirm the sender's identity. This is done by the receiver, who decrypts the signature with the sender's public key. If the signature sent with the data matches the result of applying the public key to the data, the validity of the message is established.

This process relies on the receiver having a copy of the public key of the sender and a high degree of certainty that this key belongs to the sender, not to someone pretending to be the sender.

Deploying digital certificates on mobile devices requires a unique process, as many of these devices do not natively support all the features and functionality to create/download and install digital client certificates in the same manner as traditional PC-based devices. At the same time, some endpoints do not support Simple Certificate Enrollment Protocol (SCEP) natively.

For example, for users to install digital client certificates using SCEP on Apple iOS devices, the IT administrator needs to manually create the configuration profile using the iPhone Configuration Utility and distribute the profile to user devices via E-mail, USB, or Web pages.

Traditional full-featured PC-based devices are more apt to take advantage of the many services, such as Microsoft's NDES, to provide certificate enrollment. However, with the onset of so many Android and Apple iOS devices on the market, it cannot be assumed that these devices can natively interoperate with many of the enterprise services currently deployed.

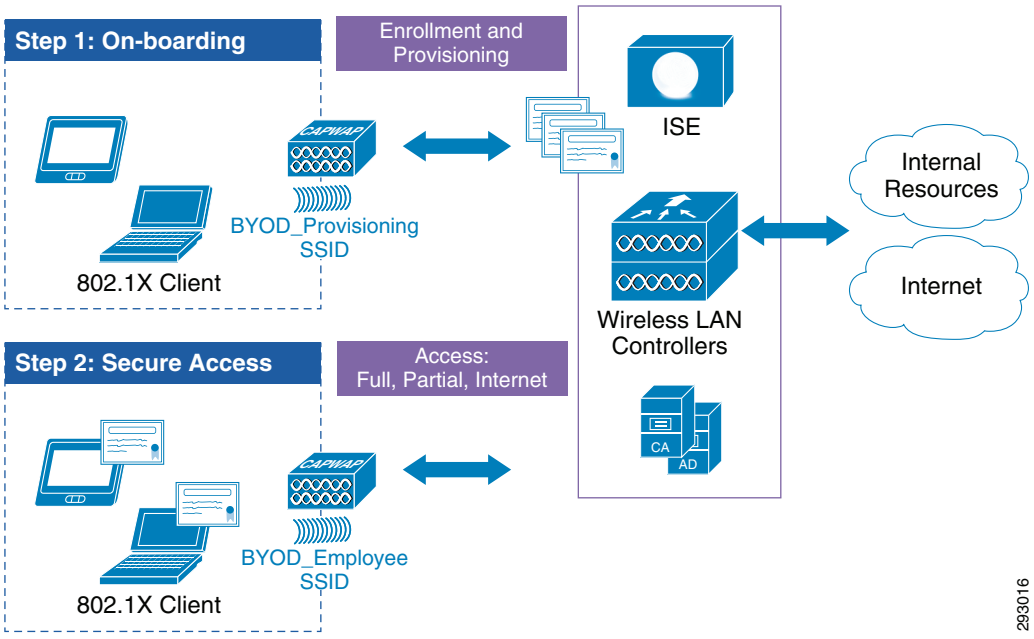
ISE solves this problem by distributing digital certificates to endpoints using the SCEP Proxy feature, which allows endpoints to obtain digital certificates through ISE. Moreover, this feature is combined during the initial registration process, thereby preventing different registration steps. The next section on mobile devices discusses how the endpoints obtain their digital certificates during the registration process.

Mobile Device Provisioning

Deploying digital certificates to endpoint devices requires a network infrastructure that provides the security and flexibility to enforce different security policies. Figure 106 highlights the general steps that are followed when a mobile device connects to the network:

1. A new device connects to a provisioning SSID. This SSID (open or secured with PEAP) is configured to redirect the user to the Guest Registration portal.
2. The certificate enrollment and profile provisioning begins after the user is properly authenticated.
3. The provisioning service requests information from the mobile device and provisions the configuration profile, which includes a WiFi profile with the parameters to connect to the secured Employee SSID.
4. For subsequent connections, the device uses the Employee SSID and is granted access to network resources based on different ISE authorization rules.

Figure 106 Enrollment and Provisioning—Dual SSID



The on-boarding steps may also be configured with a single SSID used for provisioning and secure access. The general steps followed when the mobile device connects are similar, redirecting the user to the Guest registration portal and provisioning the device with a digital certificate and configuration profiles.

Provisioning Flows

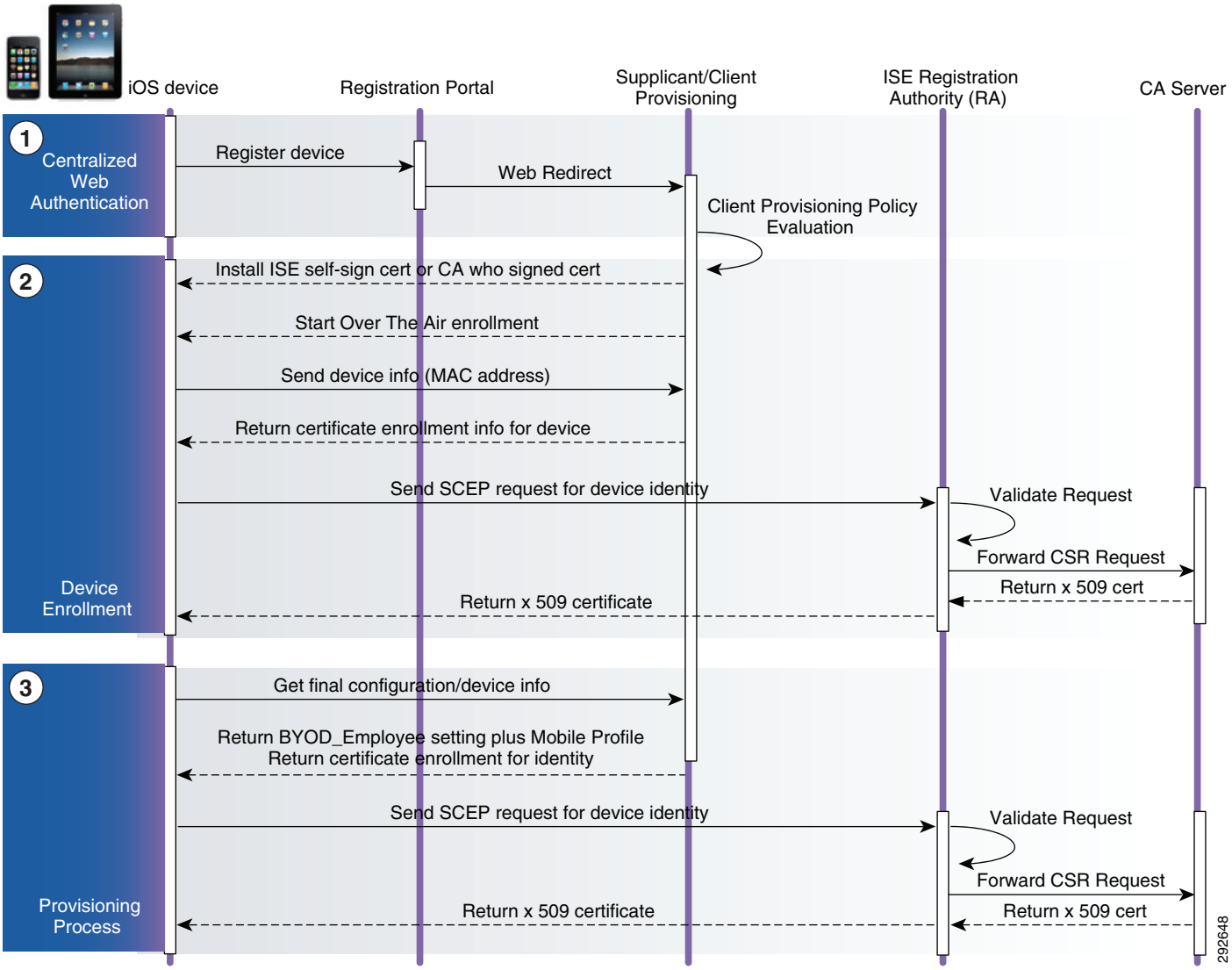
This section explains the interaction between the endpoints and the Guest Registration portal and the steps required to enroll the digital certificate and configuration profile. The way Windows and Mac devices are provisioned is similar.

Provisioning iPhone/iPads

The following steps take place while provisioning Apple iOS devices:

- The device is redirected to the Guest Registration Portal.
- After successful authentication, the Over-The-Air (OTA) enrollment begins.
- Device sends unique identifier (MAC address) and other information.
- Certificate enrollment information is sent to the device.
- A SCEP request is made to ISE, which returns a certificate.
- Wireless profile for BYOD_Employee is sent to the device.
- Once the enrollment is complete, the user manually connects to BYOD_Employee SSID.

Figure 107 Provisioning Flow for iOS Devices



For more details on Over-the-Air Enrollment and configuration for iOS devices, review the iPhone OS Enterprise Deployment Guide: http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf.

Provisioning Android Devices

The following steps take place while provisioning Android devices:

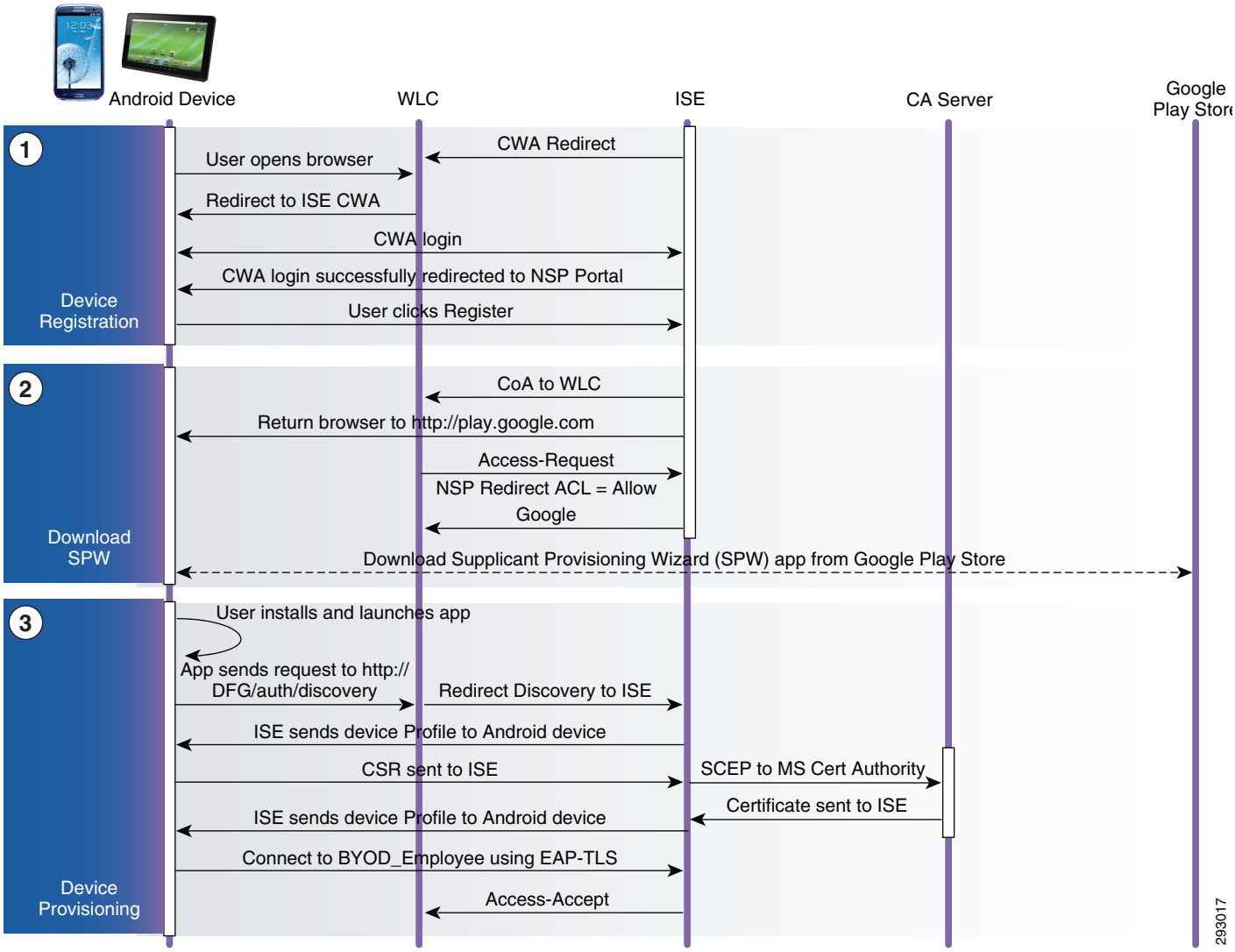
- The device is redirected to the Guest Registration portal.
- After successful authentication, the self-registration portal page redirects the user to the Google Play Store.
- The user installs the Supplicant Provisioning Wizard (SPW).
- The SPW is launched to perform provisioning of the supplicant. The SPW performs the following functions:

- Discovers the ISE and downloads the profile from the ISE.
- Creates a certificate/key pair for EAP TLS.
- Makes a SCEP proxy request to ISE and gets the certificate.
- Applies the wireless profile to allow connectivity to BYOD_Employee SSID.

- The SPW triggers re-authentication and connects to BYOD_Employee SSID automatically.

Note The Android agent must be downloaded from the Google Play Store and is not provisioned by the ISE.

Figure 108 Provisioning Flow for Android Devices



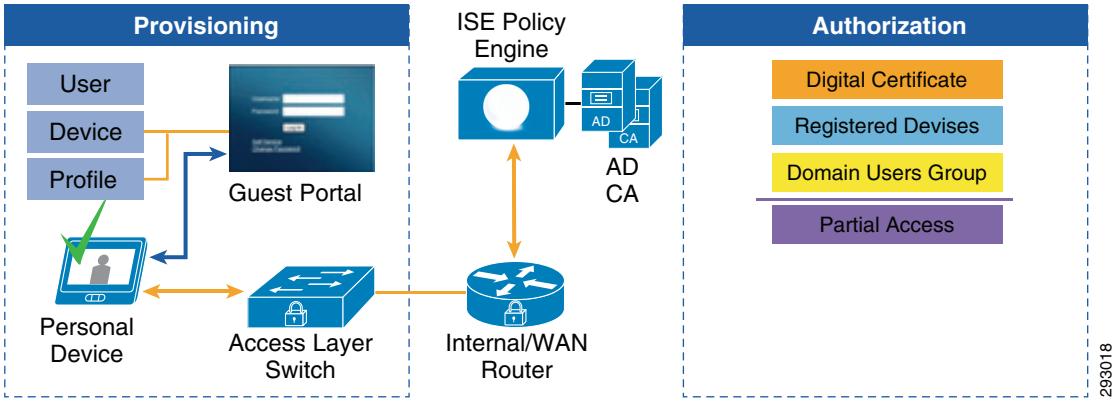
Provisioning Wired Devices

BYOD applies to both wired and wireless devices. Wired devices can be provisioned, registered, authenticated, and authorized in much the same way as wireless devices. The following are the many advantages of provisioning wired devices:

- Certificate provisioning can be done during the provisioning process, which alleviates the burden on IT to come up with another model to provision certificates on the devices.
- The native supplicants on the device can be configured with the right protocols during the provisioning process. If this is left to the user, it may often lead to incorrect configurations and management overhead for IT.
- Provides easier methods for IT to obtain visibility into who is accessing the network and also methods to remove network access for devices that are lost or stolen.

Figure 109 shows a high-level overview of the components used to deploy wired devices. ISE uses several building blocks, such as AD group membership, RegisteredDevices, and Digital Certificates to authenticate and authorize devices. Later in this guide several examples of how to construct these policies are shown (in Personal Wireless Devices—Full Access, Personal Wired Devices—Full Access, Personal Wireless Devices—Partial Access, etc.).

Figure 109 Wired Device Deployment



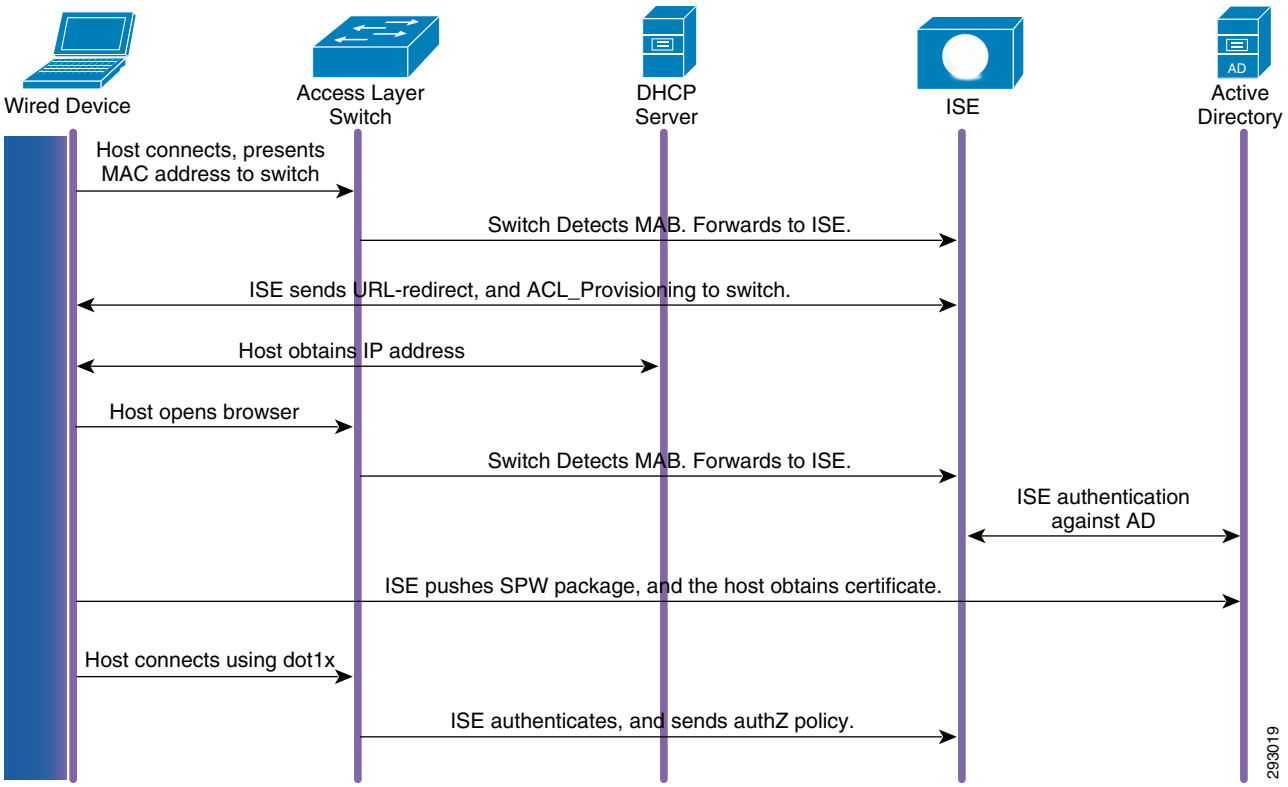
Provisioning Wired Devices

The following are high-level steps that occur when a wired device connects to the access layer switch:

1. The switch must detect that the wired endpoint is not configured for dot1x and should authenticate using MAB.
2. The ACL-WEBAUTH-REDIRECT URL redirect ACL is used to match Web traffic.
3. The URL redirect must point to the ISE Guest Registration portal.
4. The provisioning ACL must be downloaded on the port that restricts access in this state.
5. The user opens a browser and attempts to access any resource.
6. The switch redirects the user to an ISE self-registration portal.
7. ISE authenticates the user against AD and pushes the SPW package.
8. The SPW package helps the user register and obtain a digital certificate from ISE.
9. CoA occurs and the user reconnects to the network using the obtained digital certificate.

Figure 110 illustrates the flow for wired device provisioning.

Figure 110 Wired Device Provisioning Flow



Key and Certificate Storage

Being able to store digital certificates and their associated keys safely is critical for every device. Storage is implemented differently, depending on the operating system or media used. Table 11 shows the different platforms tested in this design guide and their certificate stores.

Table 11 Platform and Certificate Storage

Device	Certificate Store	How to Access
Microsoft Windows	Machine Certificate Store	Use the Certificates snap-in from the mmc.exe utility
Mac OS	Device Certificate Store	Use the Keychain Access application
Apple iPad	Device Certificate Store	Settings > General > Profile
Android	Credential Storage	May be deleted from Settings > Location & Security > Clear Storage

Once provisioned, the certificates have the following attributes, which can be used by ISE to enforce different permissions:

```
Common Name (CN) of the Subject:
    User identity used for authentication
```

```
Subject Alternative Name:
    MAC address(es) of the endpoint.
```

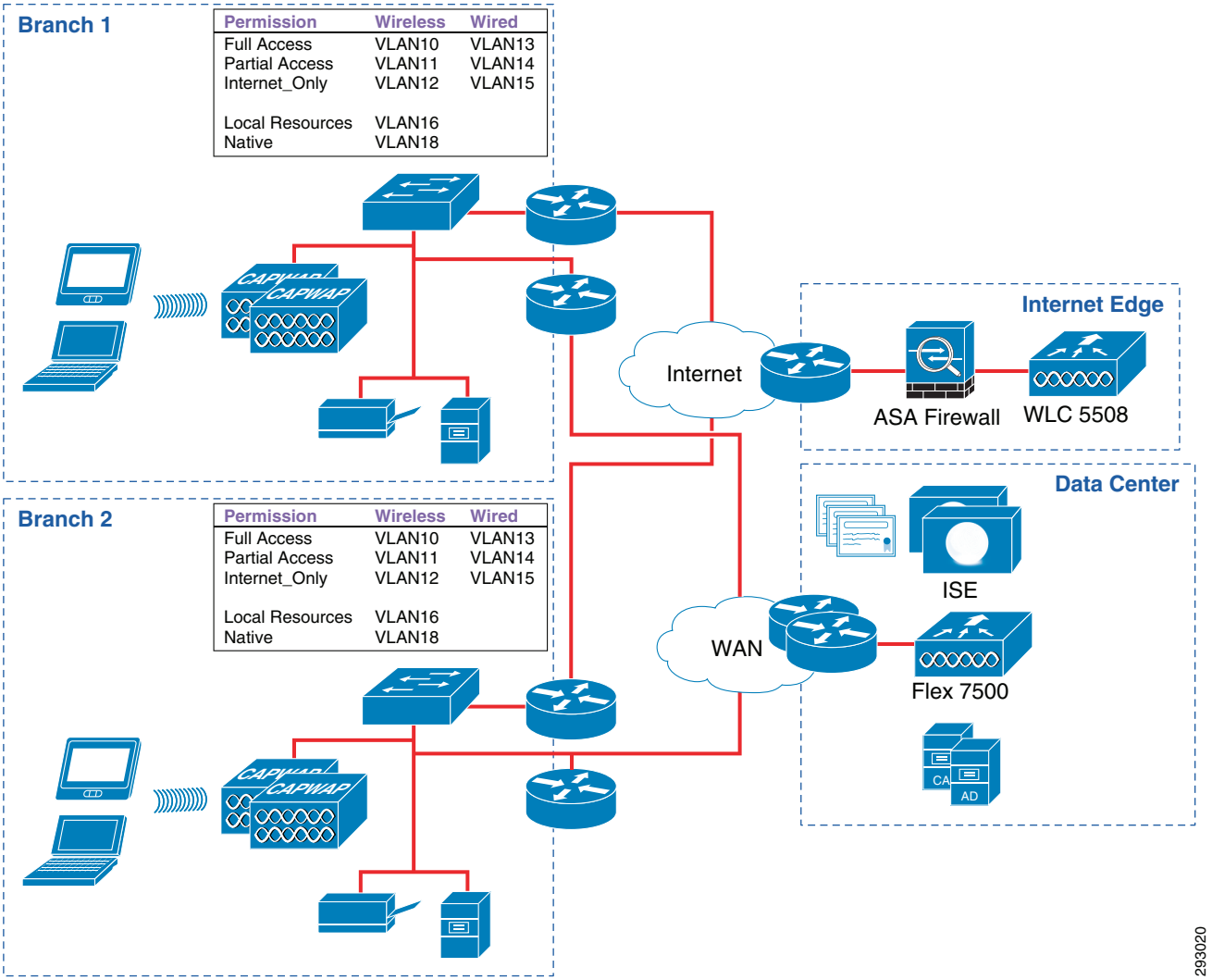
This solution provides guidance on how to achieve secure access to the corporate campus network via a wired, wireless, and remote connection using 802.1X authentication.

Personal Wireless Devices—Full Access

Figure 111 illustrates a high level network diagram depicting branches, how they connect to the campus location, and illustrates the following key points:

- At the branch the users are placed in different VLANs based on the level of access to which they are entitled.
- The same logic applies to wired, wireless, and MAB devices.

Figure 111 VLANs Used at the Branches

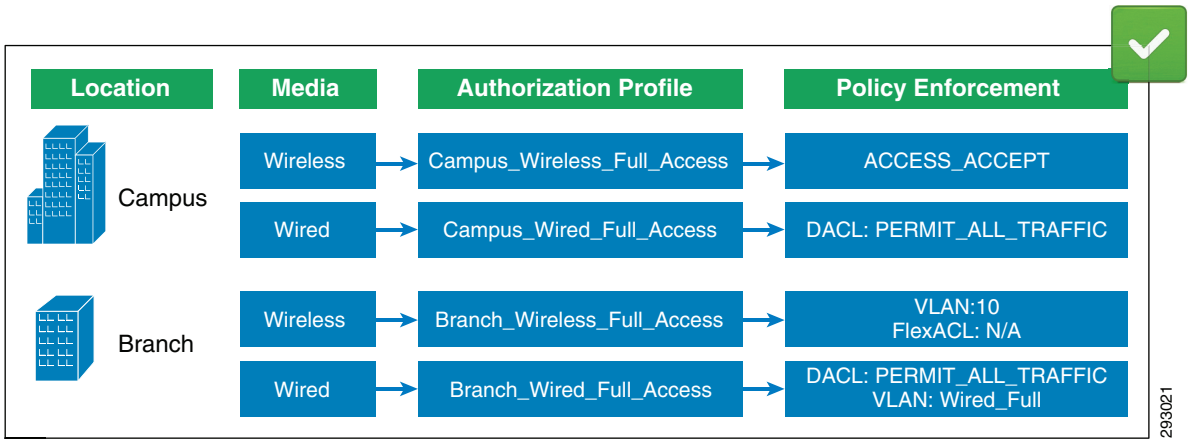


To provide full access to personal devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the Guest Registration portal and the device has been added to the RegisteredDevices identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate.
- The connection originated using EAP-TLS authentication.
- The user is member of the BYOD_Access Active Directory group.

Since the wireless design relies on two different clusters of WLCs, unique authorization rules are created for connections coming from the branch or the campus. At a high level, Figure 112 shows how different authorization profiles are selected for wired and wireless devices coming from different locations. Each authorization profile in turn enforces a unique permission using VLANs, dACLs, FlexACLs, etc.

Figure 112 Full Access Enforcement



To differentiate these connections, the ISE relies on Network Device Groups to group WLCs based on their location. This allows a single ISE to enforce policies across different groups of devices.

Figure 113 shows the different locations created for branch and campus devices.

Figure 113 Locations

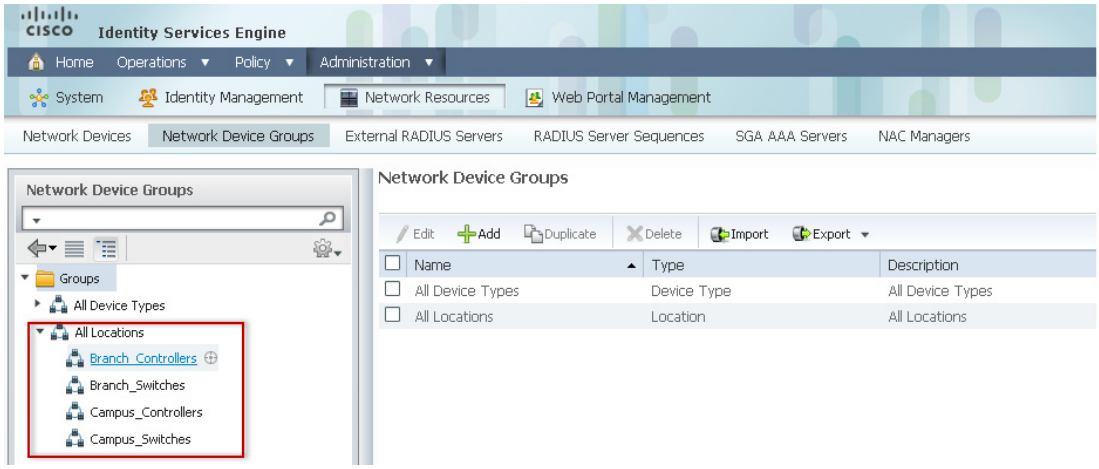
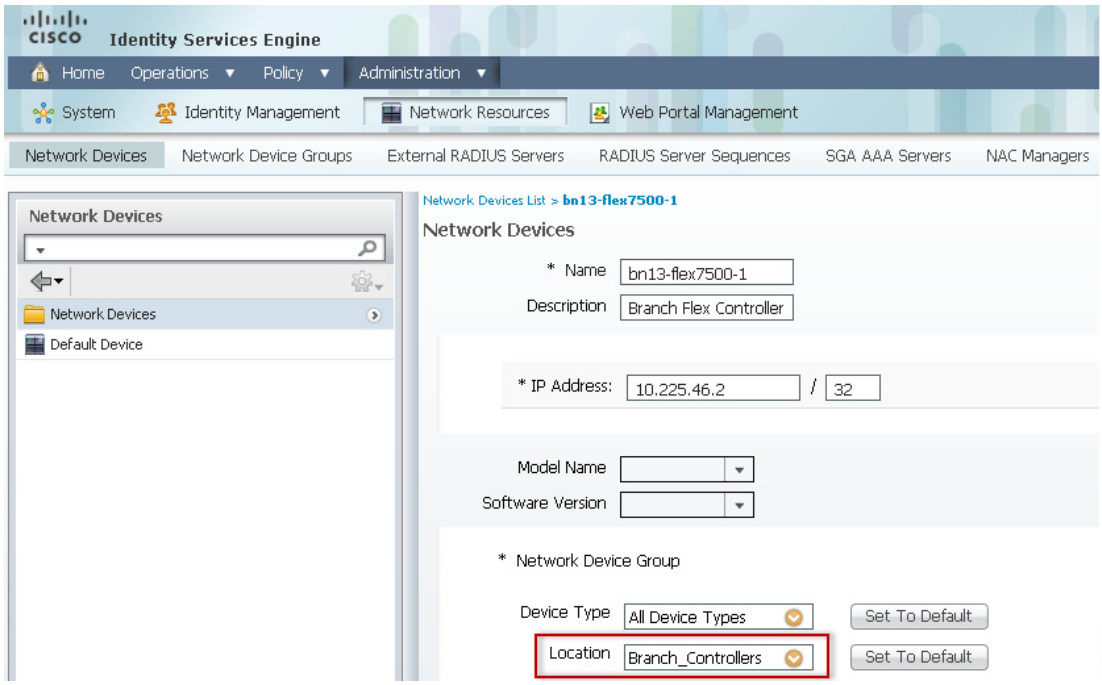


Figure 114 shows how the bn13-flex7500-1 controller belongs to the Branch_Controllers Network Device Group.

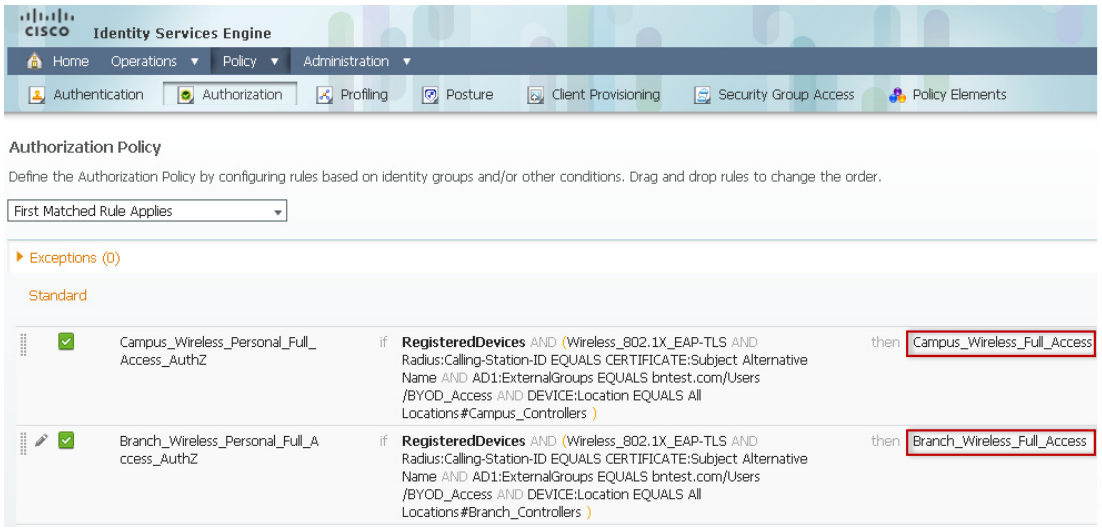
Figure 114 Branch Controller



Controllers managing wireless devices in the campus are assigned to the Campus_Controllers group.

To configure the authorization rules in ISE, click **Policy > Authorization**. Figure 115 highlights the authorization policy to grant full access to personal devices.

Figure 115 Authorization Policies for Full Access



Looking at the first rule in more detail, ISE evaluates the following conditions:

- RegisteredDevices—The endpoint has gone through the provisioning process.
- Wireless_802.X_EAP-TLS—A wireless endpoint using EAP-TLS (defined as a compound condition).

- Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name—The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name.
- AD1:ExternalGroups EQUAL Corp_Devices—The user belongs to the Corp_Devices Active Directory group.
- DEVICE:Location EQUALS Campus_Controllers—The connection originated from a WLC controller in the campus.

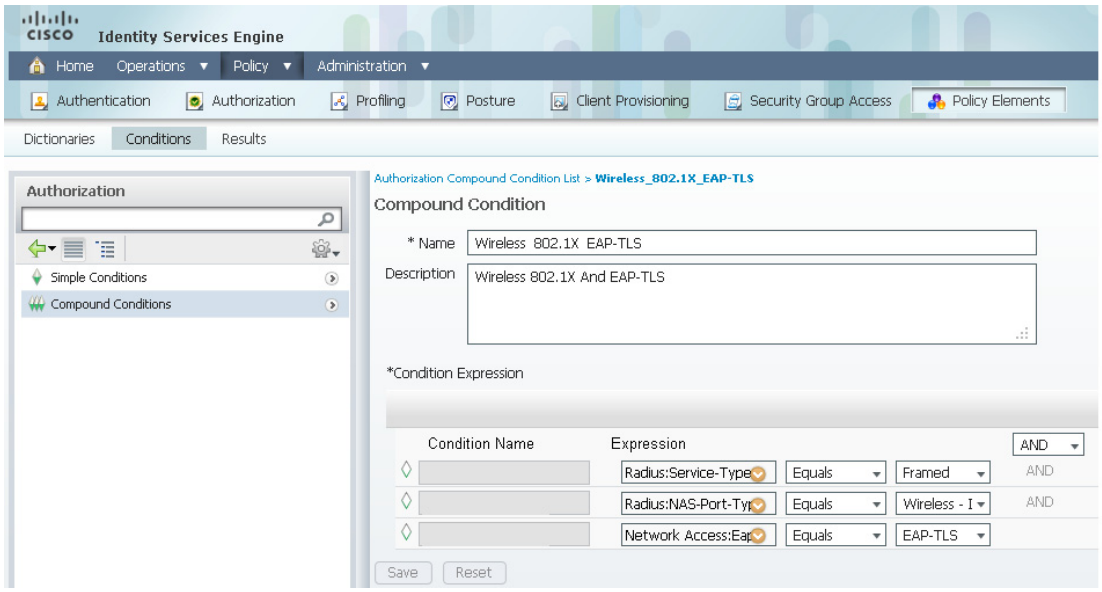
Separate rules are defined for campus and branch devices. These rules check the identity group membership (WhiteList or RegisteredDevices) and the Active Directory group membership to apply Full_Access permissions.

To reduce the number of conditions, compound authorization conditions can be used. A compound condition was defined to include Wireless 802.1X and EAP-TLS:

- Radius:Service-Type Equals Framed
- Radius:NAS-Port-Type Equals Wireless - IEEE 802.11
- Network Access:EapAuthentication Equals EAP-TLS

To define a compound condition, click **Policy > Conditions > Authorization > Compound Conditions**. Figure 116 shows how the three previous conditions may be combined into a single compound condition:

Figure 116 Compound Condition



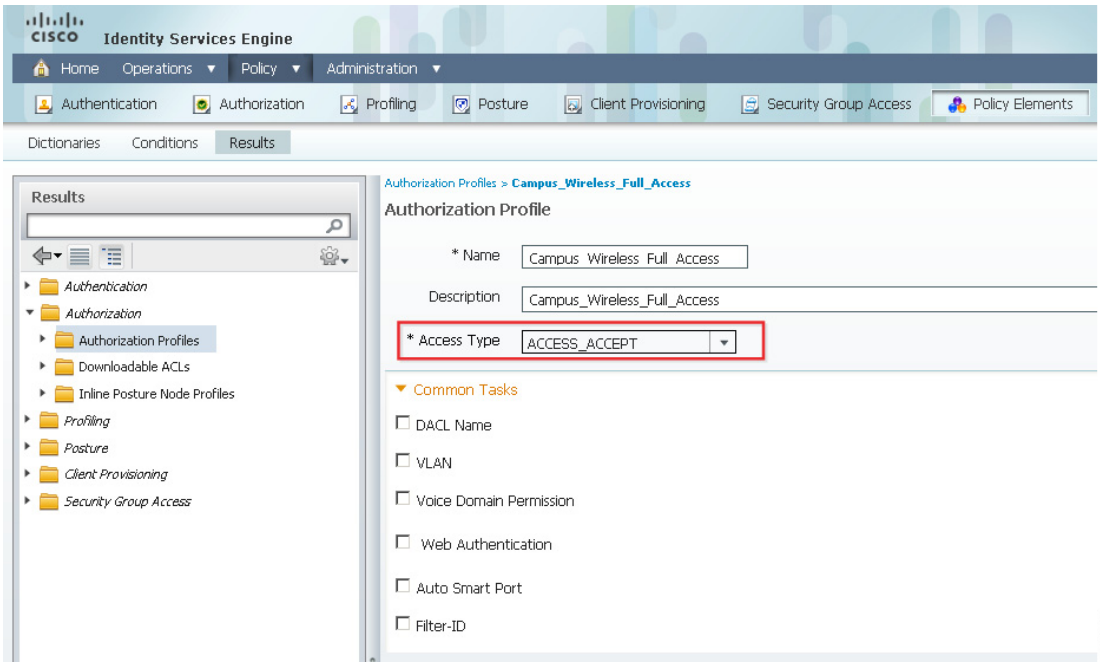
Authorization Profiles

When all conditions in the authorization policy rule match, the rule invokes the proper authorization profile:

- *Campus_Wireless_Full_Access* for 802.1X wireless devices connecting from the campus location.
- *Branch_Wireless_Full_Access* for 802.1X wireless devices connecting from a branch location.

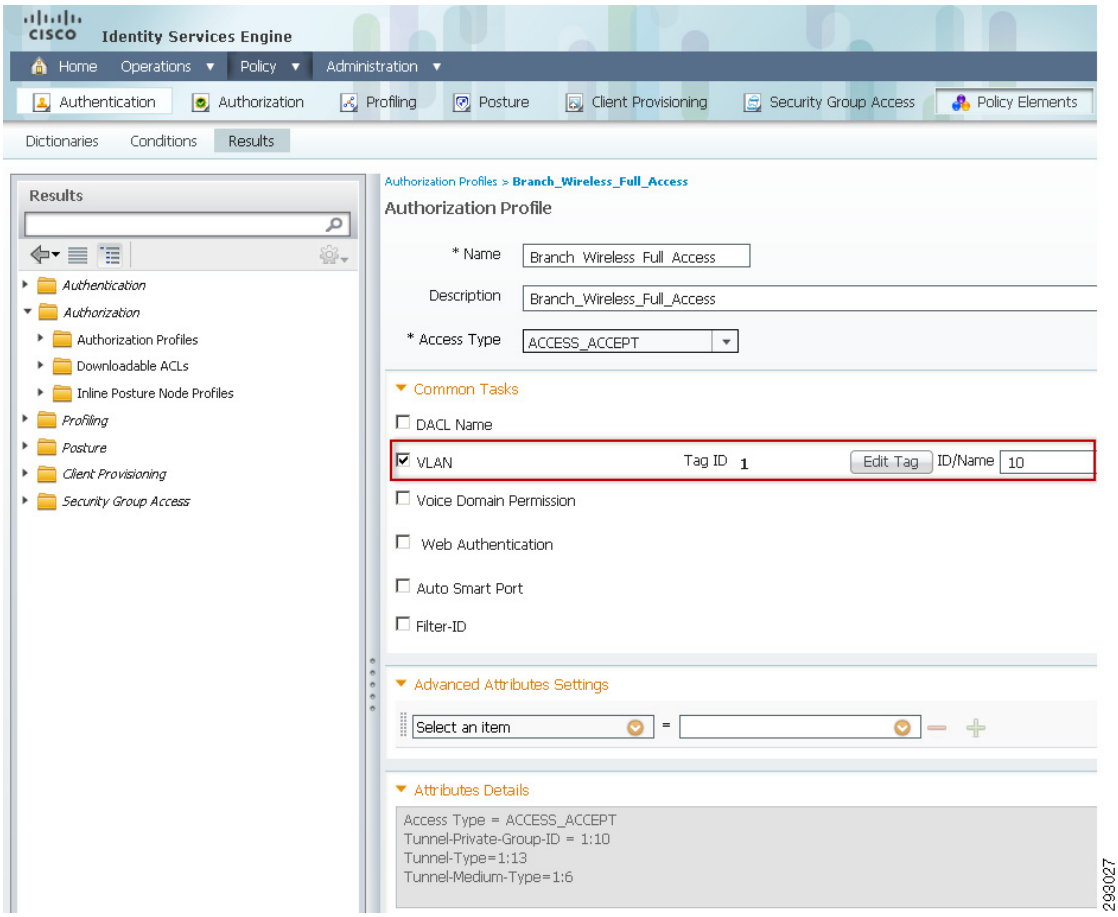
Figure 117 shows how the Campus_Wireless_Full_Access authorization profile is using the ACCESS_ACCEPT Access Type to allow full access.

Figure 117 Campus_Wireless_Full_Access



Endpoints connecting from a branch location dynamically get assigned to VLAN 10, which has been configured to provide full access.

Figure 118 Branch_Wireless_Full_Access



Personal Wired Devices—Full Access

When a connection initiates from a branch or campus location, the basic objective is to enforce partial policy on the device. The primary method by which policy is enforced is using ACLs. In a campus location the dACLs are enforced on every device, whereas at the branch there are different methods in which ACLs can be enforced, including:

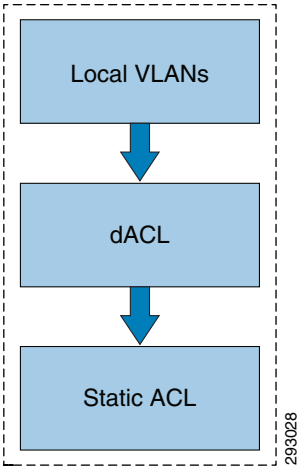
- Configuring static ACLs at every branch router in the network.
- Configuring the ISE to push downloadable ACLs to access layer switches at every branch location.

Table 12 gives the advantages and disadvantages of each approach.

Each of the above methods has advantages and disadvantages. This design guide focuses on a combination that includes both methods. The static ACLs are the primary method by which access is restricted. However, the static ACLs are applied at the router only, and to override the ACL called "DEFAULT-ACL" which is present on every port, a dACL is downloaded from ISE.

Figure 119 shows how the authorization policy pushes the VLAN information and the dACL (permit all traffic) to the port. This allows the traffic to reach up to the router where the traffic will be filtered.

Figure 119 Enforcing Permissions

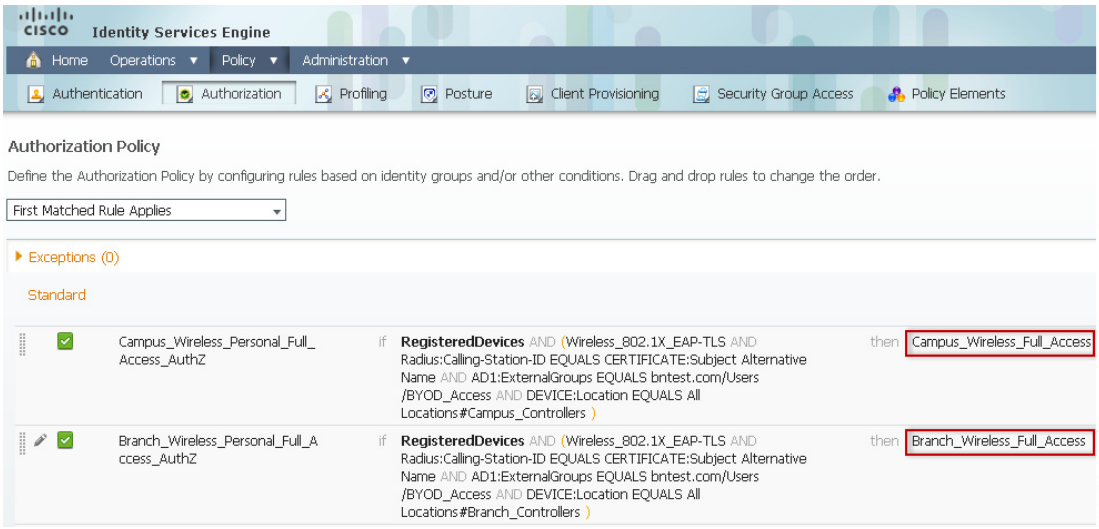


To provide full access to personal wired devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the Guest Registration portal and the device has been added to the RegisteredDevices identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the BYOD Access Active Directory group.

Figure 120 shows the details of authorization profile configured in ISE for wired devices.

Figure 120 Authorization Policies for Wired Full Access



Authorization Profiles

When all conditions in the authorization policy rule match, the rule invokes the proper authorization profile:

- Campus_Wired_Full_Access for 802.1X wired devices connecting from the campus location.
- Branch_Wired_Full_Access for 802.1X wired devices connecting from a branch location.

Figure 121 shows how the Campus_Wired_Full_Access authorization profile is defined in ISE.

Figure 121 Campus_Wired_Full_Access Authorization Profile

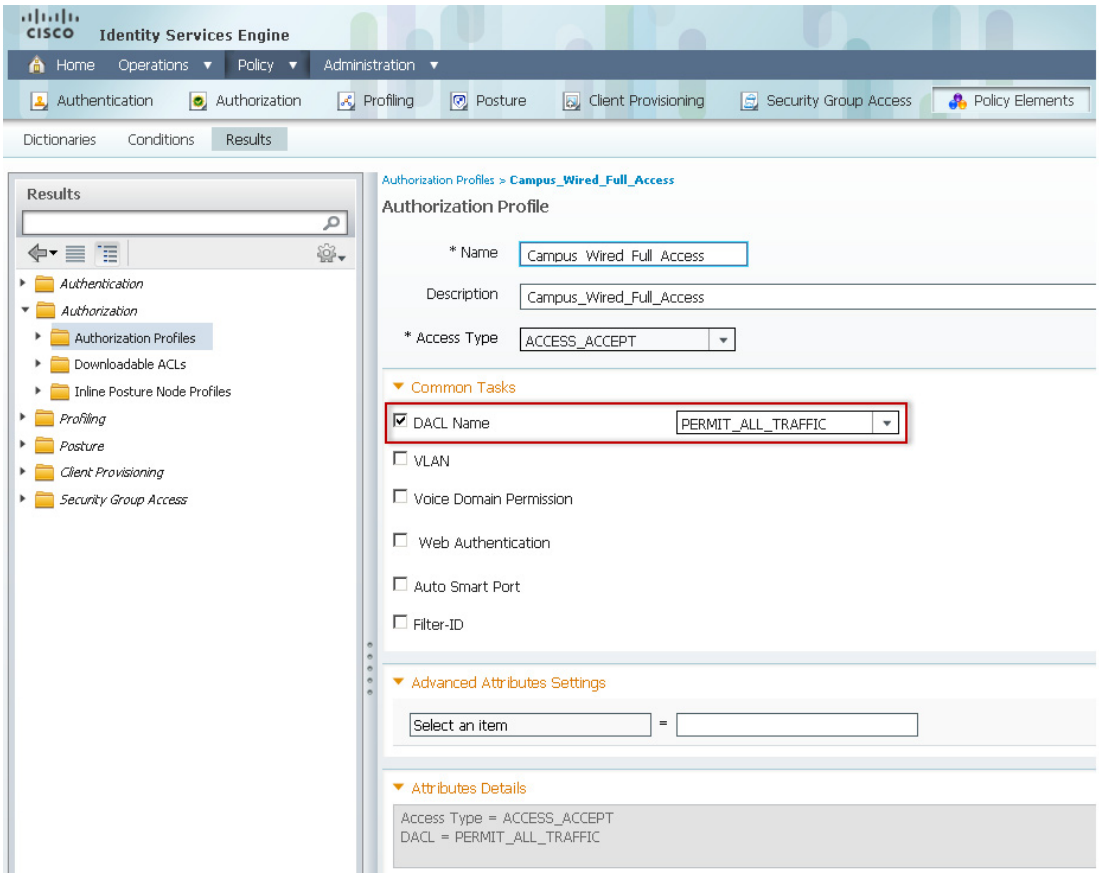
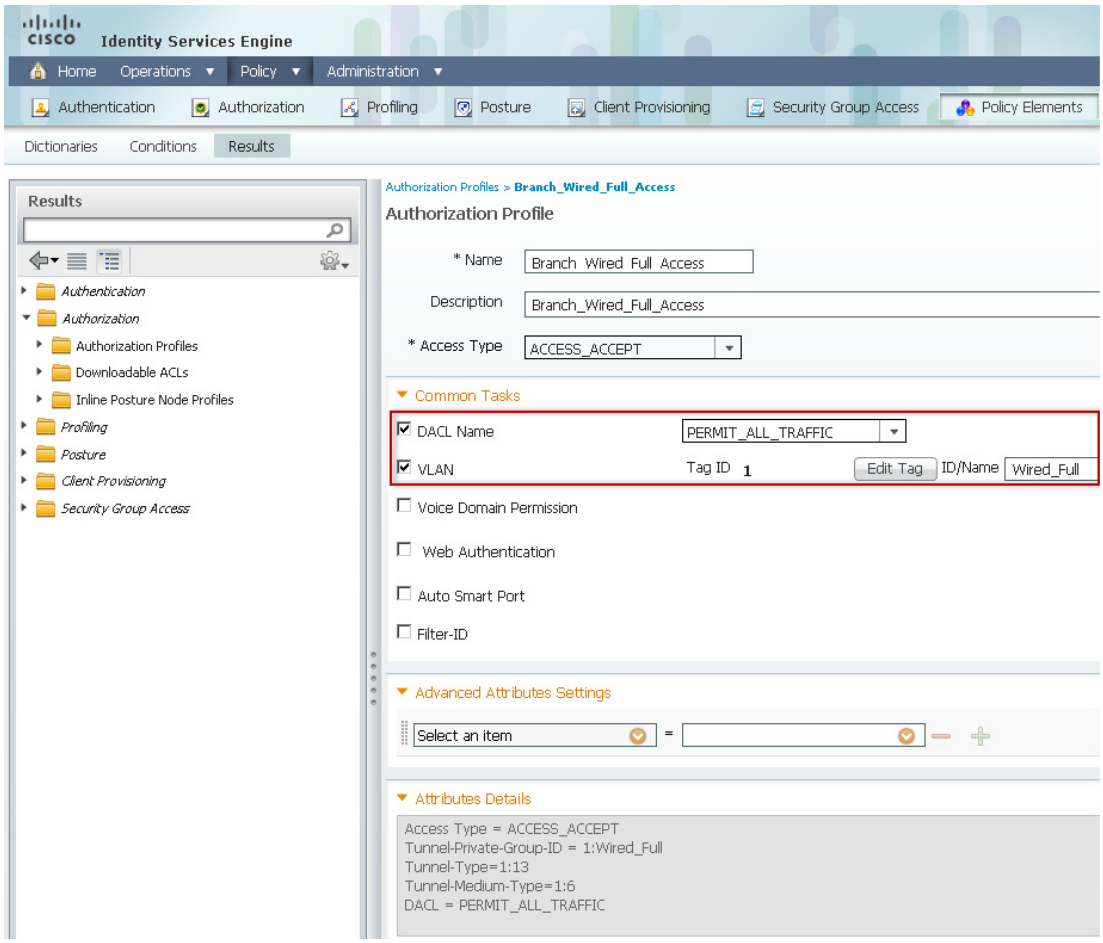


Figure 122 shows how a similar authZ profile is constructed for devices located in the branch and accessing the network using wired medium.

Figure 122 Branch_Wired_Full_Access Authorization Profile



It is important to note that the authorization profile also pushes VLAN information along with the ACL information.

Once this profile is downloaded to the Catalyst switch, the endpoint gets full access to the network. Figure 123 shows an example of the state of the port when this profile is downloaded by using the switch command **show authentication session interface Gi0/23**.

Figure 123 Catalyst Switch Port

```
----------------------------------------
          Interface:  GigabitEthernet0/23
        MAC Address:  0050.568f.0020
         IP Address:  10.11.31.14
          User-Name:  user1
             Status:  Authz Success
             Domain:  DATA
    Security Policy:  Should Secure
    Security Status:  Unsecure
     Oper host mode:  multi-auth
  Oper control dir:  both
     Authorized By:  Authentication Server
        Vlan Group:  N/A
           ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f6095bc
    Session timeout:  N/A
       Idle timeout:  N/A
Common Session ID:  960101010000002B001555A3
  Acct Session ID:  0x0000002F
            Handle:  0x9E00002C
```

293654

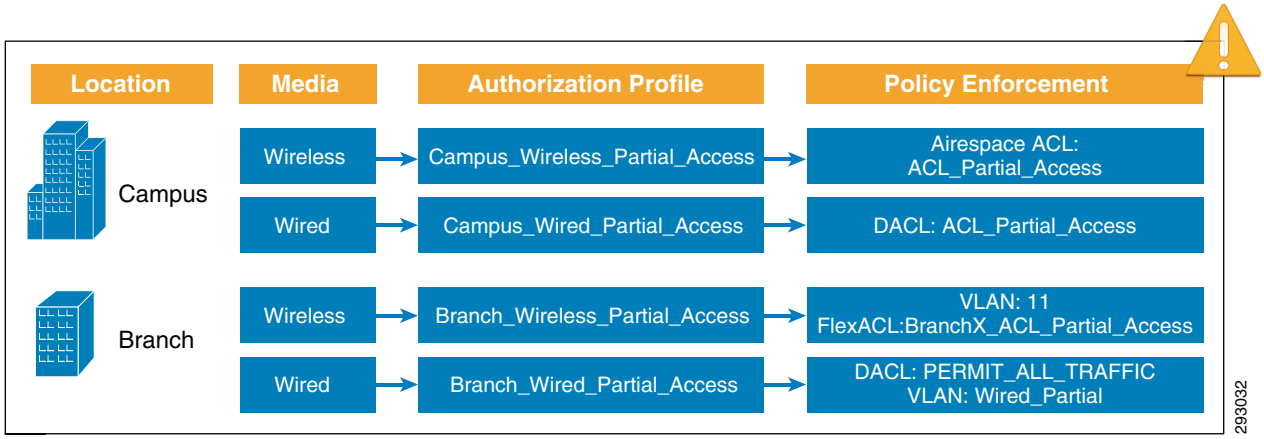
Personal Wireless Devices—Partial Access

To provide partial access to personal devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the Guest Registration portal and the device has been added to the RegisteredDevices identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is member of the Domain Users Active Directory group.

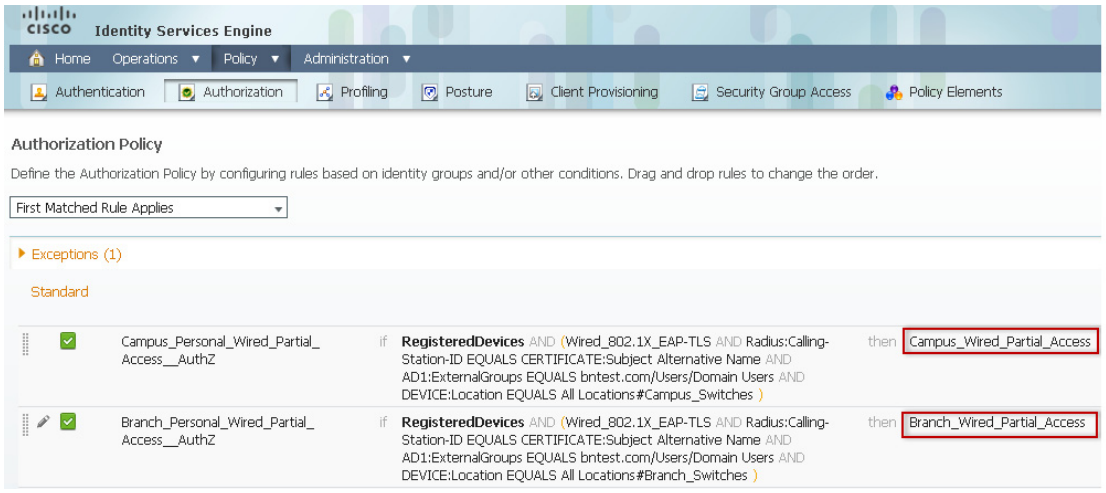
At a high level, Figure 124 shows how different authorization profiles are selected for wired and wireless devices coming from different locations. Each authorization profile in turn enforces a unique permission using VLANs, dACLs, FlexACLs, etc.

Figure 124 Partial_Access Enforcement



To configure the authorization rules in ISE, click **Policy** > **Authorization**. Figure 125 highlights the authorization policy to grant partial access to personal devices.

Figure 125 Authorization Policies for Partial Access



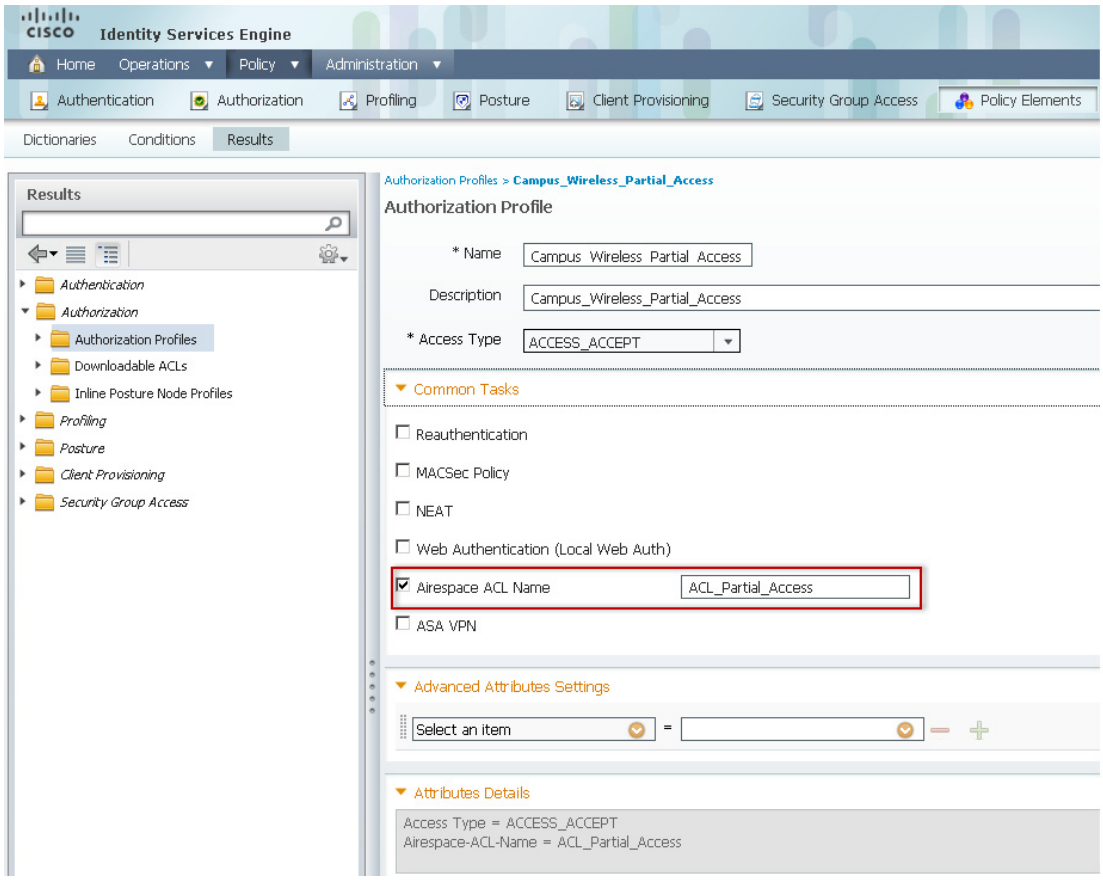
Authorization Profiles for Wireless Devices

When all conditions in the authorization policy rules match, the rule invokes the proper authorization profile:

- Campus_Wireless_Partial_Access for 802.1X wireless devices connecting from the campus location.
- Branch_Wireless_Partial_Access for 802.1X wireless devices connecting from a branch location.

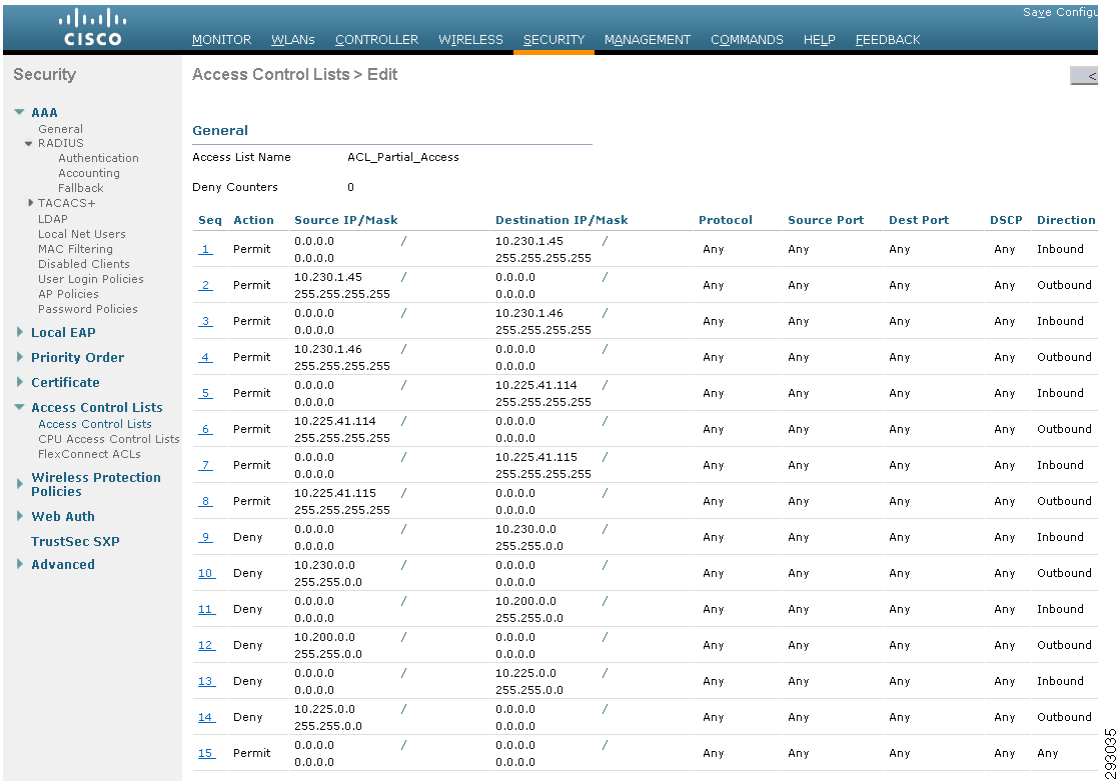
For devices connecting from the campus location, the Campus_Wireless_Partial_Access authorization profile relies on the ACL_Partial_Access access list, enforced by the WLC, as shown in Figure 126.

Figure 126 Campus_Wireless_Partial_Access



Cisco Wireless LAN Controllers support named ACLs, meaning that the ACL must be previously configured on the controller rather than being downloaded from ISE. Using the RADIUS Airespace-ACL Name attribute-value pair, ISE instructs the WLC to apply the ACL_Partial_Access ACL. Figure 127 shows the contents of this ACL, as defined in the 5508 WLC campus controller.

Figure 127 ACL_Partial_Access



The access-list shown in Figure 127 has the following characteristics:

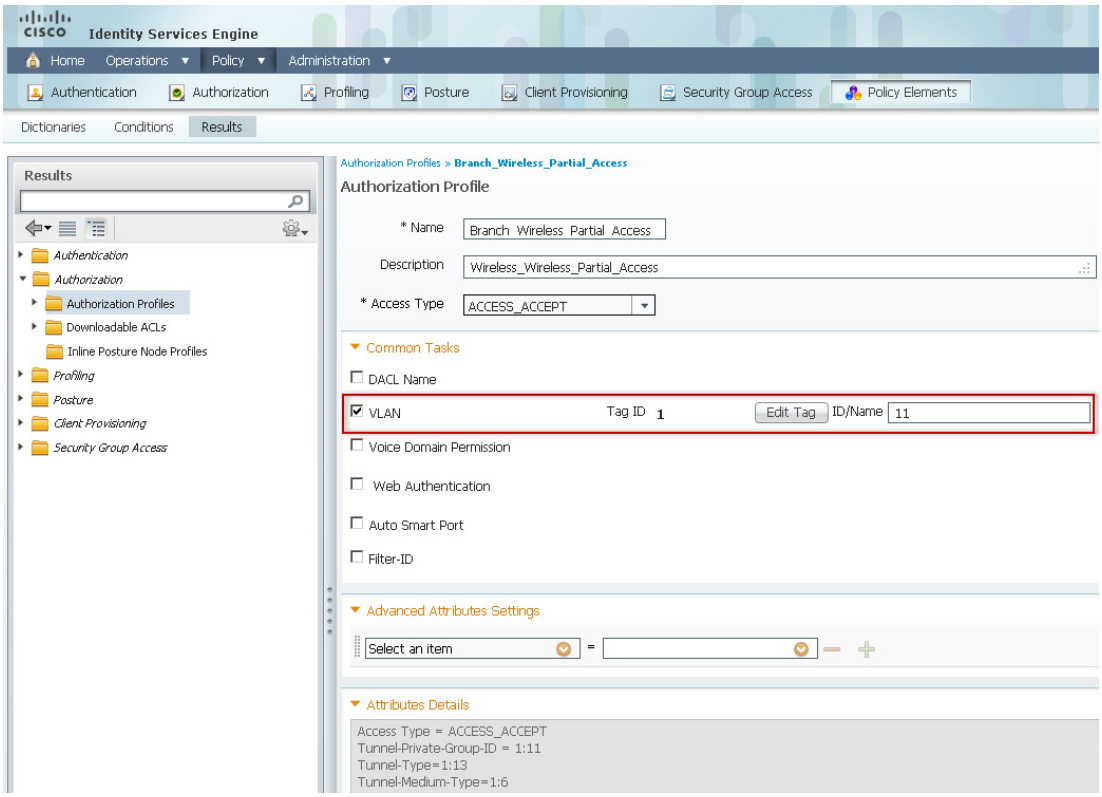
- Allow access to DNS servers (10.230.1.45, 10.230.1.46) and ISE Servers (10.225.41.114, 10.225.41.115).
- Deny Access to Data Center subnets (10.230.0.0).
- Deny access to router links 10.225.0.0.
- Allow access to all other internal subnets and Internet access.

The access list is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

Note The WLC supports a maximum of 64 ACLs with a maximum of 64 lines per ACL.

For devices connecting from a branch location, the Branch_Wireless_Partial_Access authorization profile dynamically assigns the device to VLAN11, which is dedicated for devices obtaining Partial_Access. Figure 128 shows this authorization profile.

Figure 128 Branch_Wireless_Partial_Access



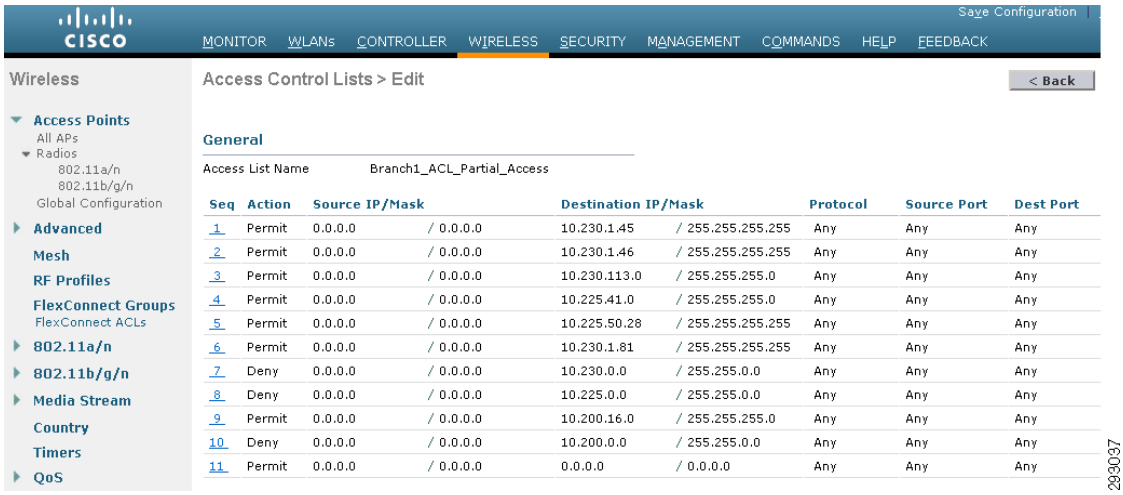
Deploying ACLs on the branch is slightly different than using ACLs with a centralized WLC. For branch locations, the Cisco 7500 Flex Wireless Controller relies on FlexConnect ACLs to enforce policy permissions. FlexConnect ACLs are created on the WLC and configured with the VLAN defined on the AP or the FlexConnect Group using the VLAN-ACL mapping for dynamic or AAA override VLANs. These FlexConnect ACLs are pushed to the APs when the authorization policy matches. This design guide relies on FlexConnect groups to enforce Flex ACLs for each VLAN.

1. Create a FlexConnect ACL for each branch.
2. Apply the FlexConnect ACL on the FlexConnect group for each branch.
3. Define the VLAN-ACL mapping for each VLAN.

On the FlexConnect 7500 Controller, click **Security > Access Control Lists > FlexConnect ACLs** and define the ACL rules for Partial Access. Figure 129 shows the Branch1_ACL_Partial_Access ACL, which allows access to the Internet and some internal resources

Note A unique ACL may be needed for each branch since each branch location may have its own local resources.

Figure 129 Branch1_ACL_Partial_Access



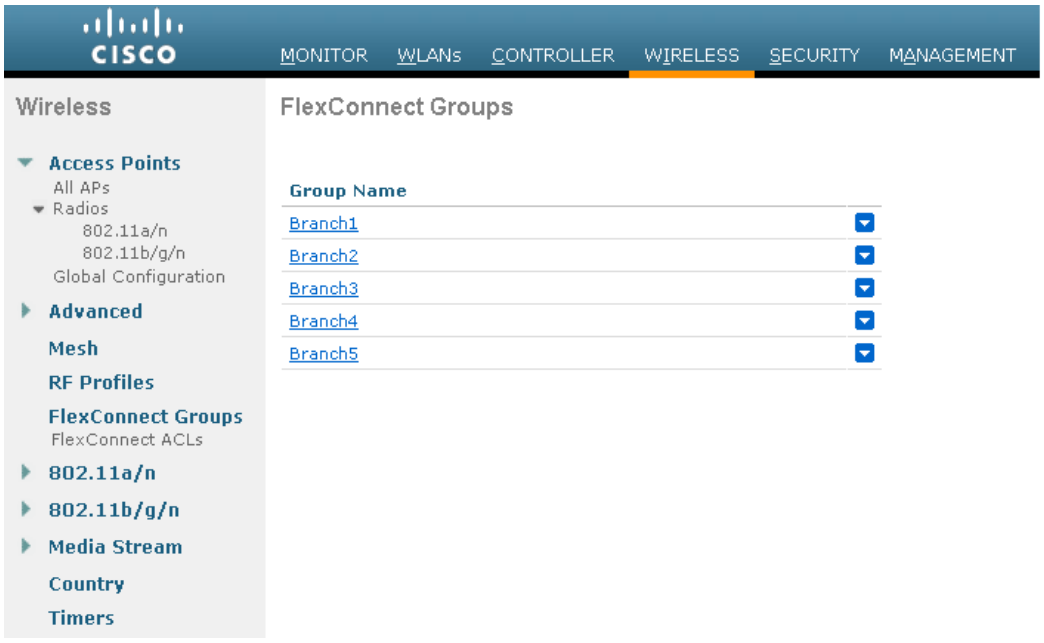
The above ACL has the following characteristics:

- Allow access to DNS servers (10.230.1.45, 10.230.1.46) and ISE Servers (10.225.41.114, 10.225.41.115).
- Deny Access to Data Center subnets (10.230.0.0).
- Allow access to router links 10.225.0.0.
- Allow access to Branch Servers (10.200.16.0).
- Deny access to all other internal subnets.
- Allow access to Internet.

For the purposes of this design guide, a FlexConnect group is defined for each branch, which allows for multiple FlexConnect access points in the branch to share configuration parameters.

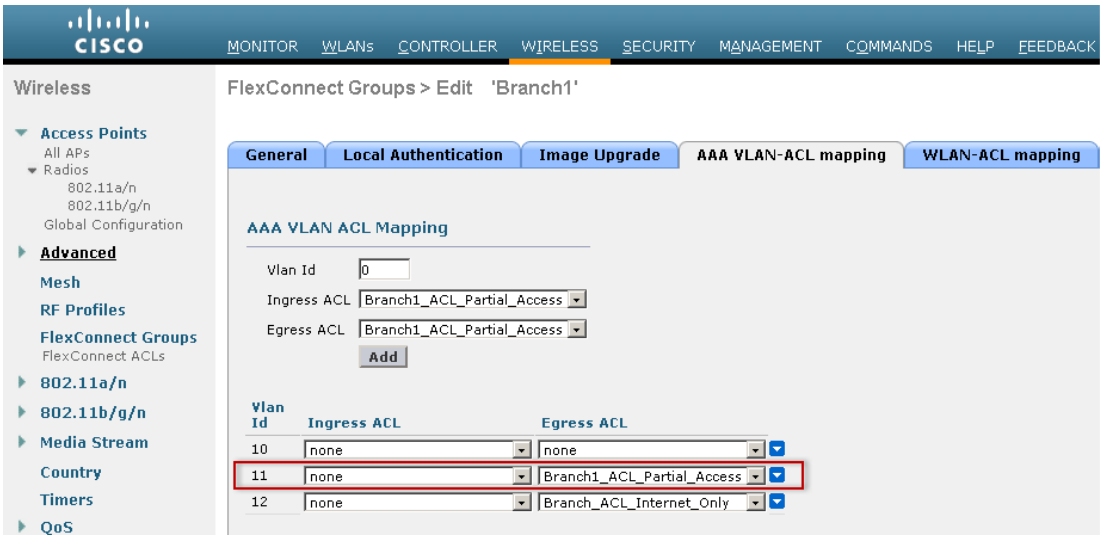
On the FlexConnect 7500 controller, click **Wireless > FlexConnect Groups** and select the FlexConnect group for a particular branch location, as shown in Figure 130.

Figure 130 FlexConnect Groups



In Figure 131 , the FlexConnect group for Branch1 is applying the Branch1_ACL_Partial_Access ACL to endpoints connecting to VLAN 11.

Figure 131 FlexConnect Group for Branch1

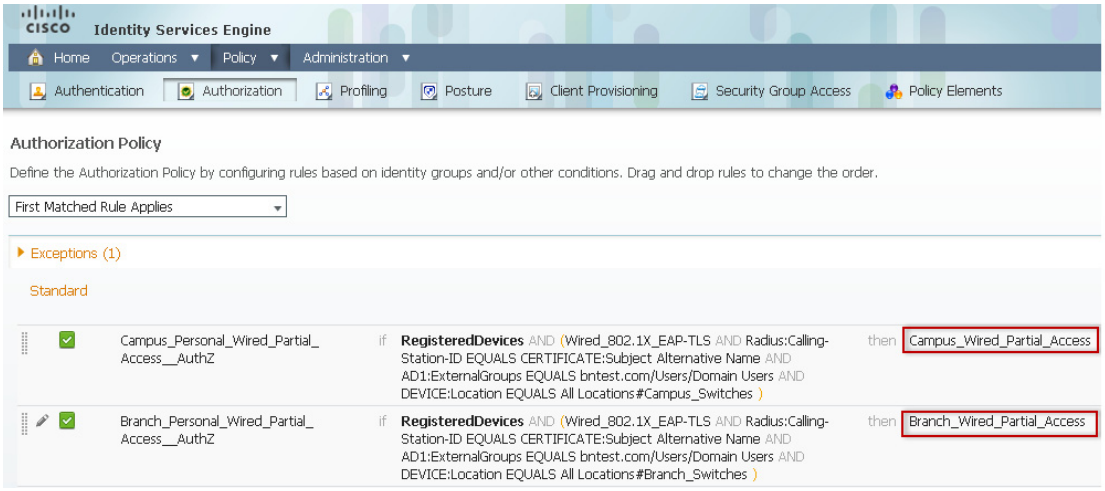


Personal Wired Devices—Partial Access

In addition to Internet access, partial access allows access to some internal resources. As mentioned in Personal Wireless Devices—Partial Access, for a user/device to obtain partial access, the user must authenticate to ISE, present its credentials which are verified by ISE, and the end result is an

authorization profile which is applied to the access layer switch. The first step is to define an authorization policy for devices originating at the campus or branch location. Figure 132 highlights the authorization policy to grant partial access to personal devices:

Figure 132 Authorization Policies for Wired Partial Access



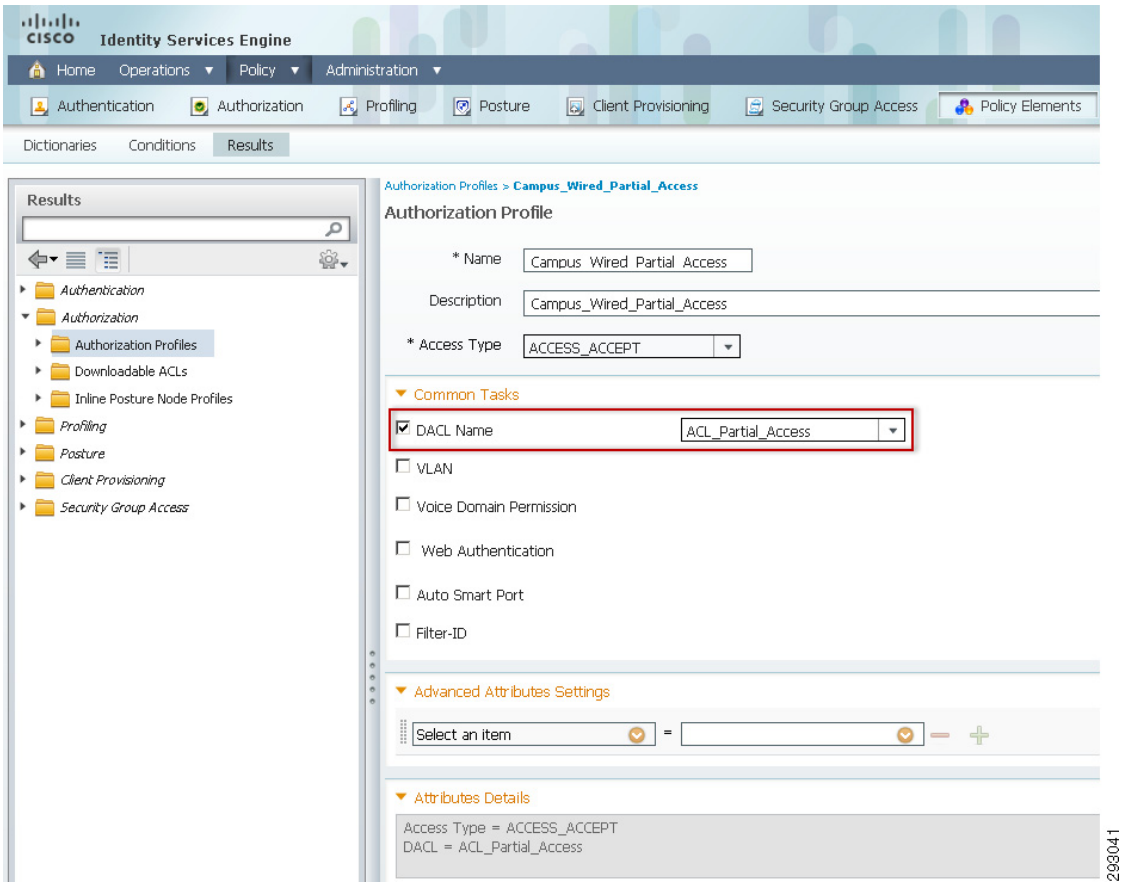
Authorization Profiles for Wired Devices

The following are two authorization profiles defined on ISE for devices originating from campus or branch location:

- Campus_Wired_Partial_Access for 802.1X wired devices connecting from the campus location.
- Branch_Wired_Partial_Access for 802.1X wired devices connecting from a branch location.

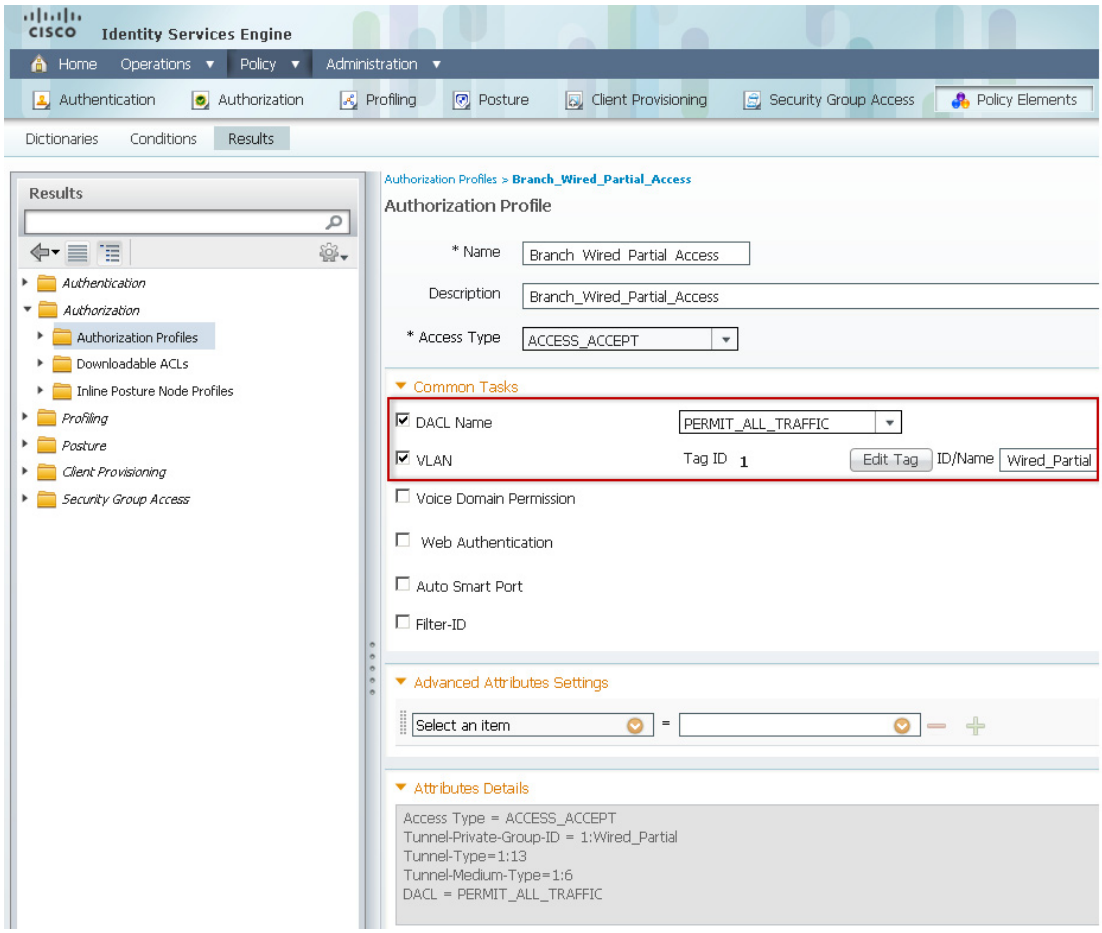
For devices connecting from the campus location, the Campus_Wired_Partial_Access authorization uses a dACL named ACL_Partial_Access, enforced by the access layer switch, as shown in Figure 133.

Figure 133 Campus_Wired_Partial_Access



Cisco Access Layer Switches support downloadable ACLs (dACL) rather than named ACLs (used in WLC). This ACL over-rides the default-ACL configured on the switch. Figure 134 provides an example of how this ACL can be implemented. The dACL allows all traffic, so that the traffic initiated by the host reaches the branch router where the router-ACL is applied.

Figure 134 Branch_Wired_Partial_Access Authorization Profile



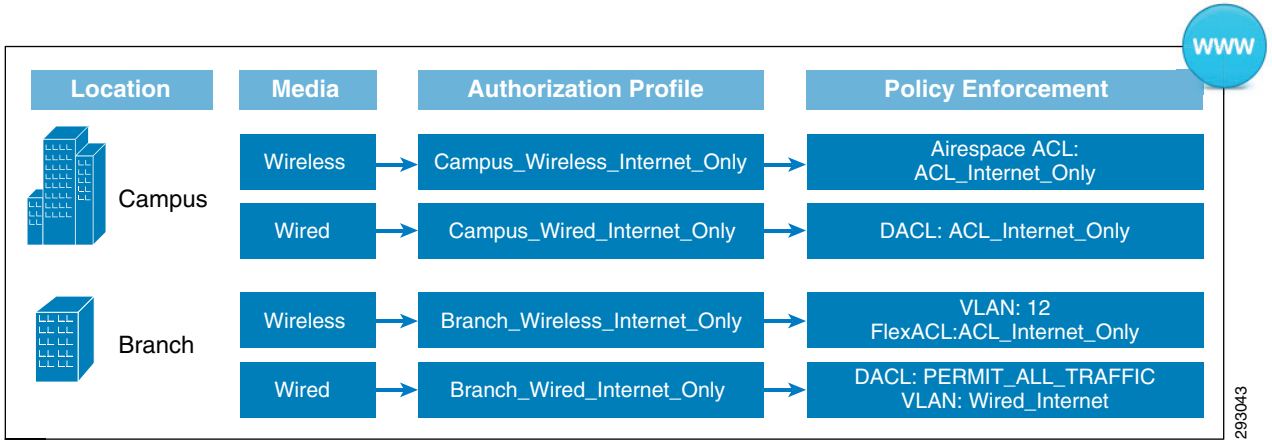
Personal Devices—Internet Only Access

To provide Internet Only access to personal devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the self-registration portal and the device has been added to the RegisteredDevices identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the Internet_Access Active Directory group.

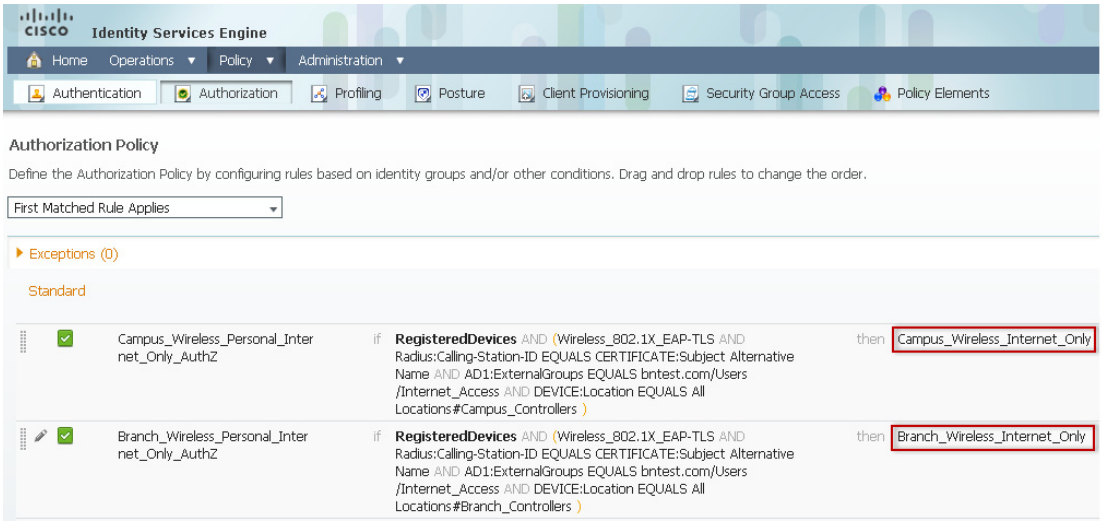
At a high level, Figure 135 shows how different authorization profiles are selected for wired and wireless devices coming from different locations. Each authorization profile in turn enforces a unique permission using VLANs, dACLs, FlexACLs, etc.

Figure 135 Internet_Only Enforcement



To configure the authorization rules in ISE, click **Policy** > **Authorization**. Figure 136 highlights the authorization policy to grant Internet_Only access to personal devices.

Figure 136 Authorization Policies for Internet Only Access

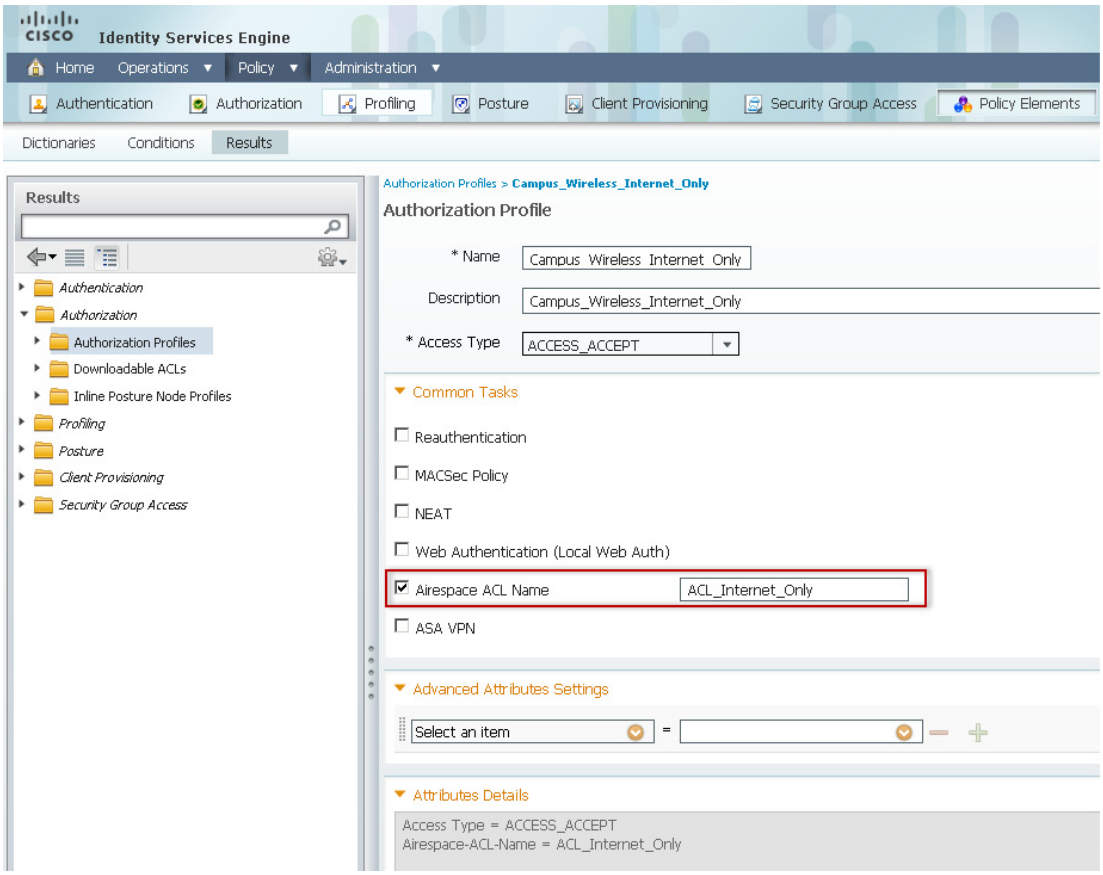


When all conditions in the authorization policy rules match, the rule invokes the proper authorization profile:

- *Campus_Wireless_Internet_Only* for 802.1X wireless devices.
- *Branch_Wireless_Internet_Only* for 802.1X wired devices.

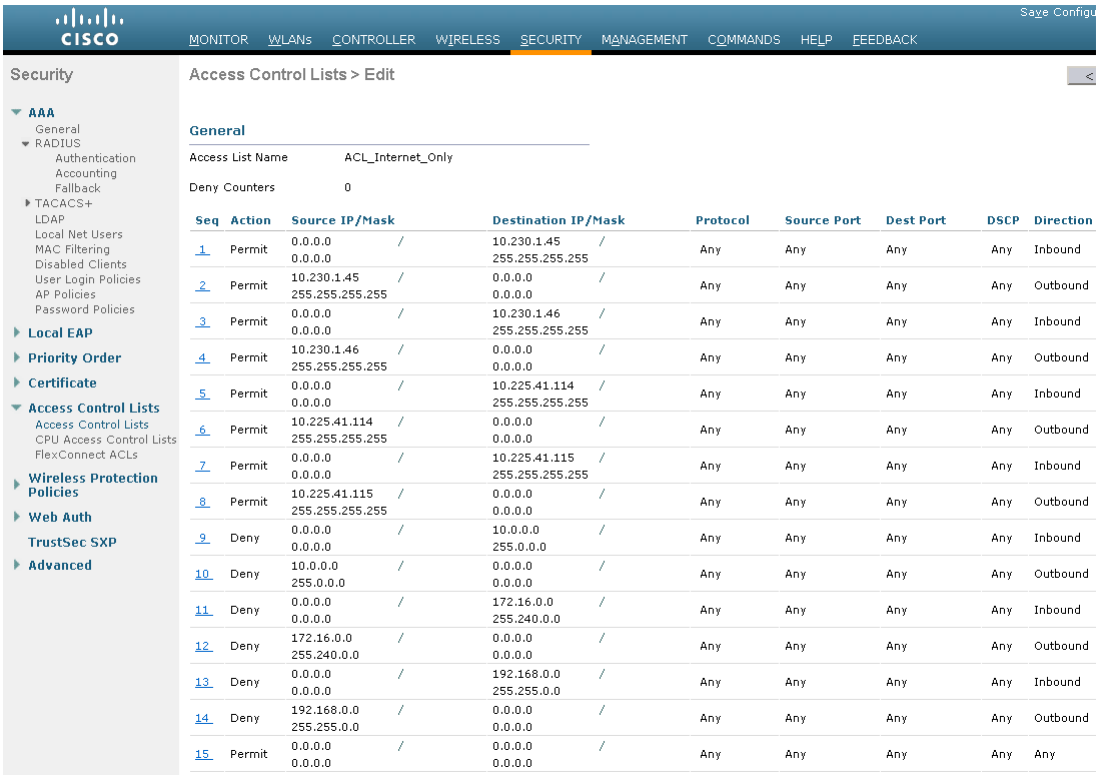
For devices connecting from the campus location, the Campus_Wireless_Internet_Only authorization profile relies on the ACL_Internet_Only access list, enforced by the WLC, as shown in Figure 137.

Figure 137 Campus_Wireless_Internet_Only



Cisco Wireless LAN Controllers support named ACLs, meaning the ACL must be previously configured on the controller, rather than being downloaded from ISE. Using the RADIUS Airespace-ACL Name attribute-value pair, ISE instructs the WLC to apply the ACL_Internet_Only ACL. Figure 138 shows the contents of this ACL, as defined in the 5508 WLC campus controller.

Figure 138 ACL_Internet_Only



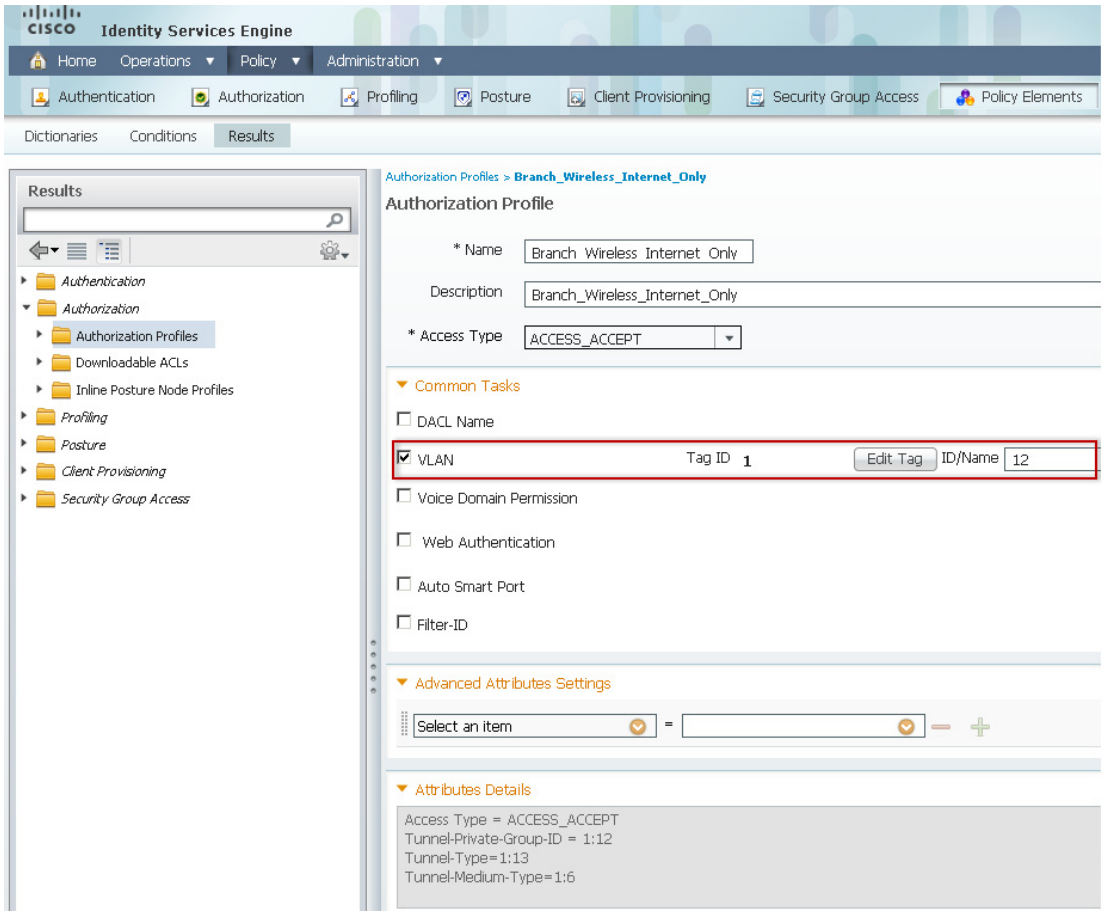
The access list allows access to DNS and DHCP servers, denies the RFC 1918 private addresses, and allows access to all other addresses.

Once again, the access list is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

Figure 139 shows how the Internet_Only_Wireless authorization profile instructs the WLC to apply the ACL.

For devices connecting from a branch location, the Branch_Wireless_Internet_Only authorization profile dynamically assigns the device to VLAN12, which is dedicated for devices obtaining Internet_Only access. Figure 128 and Figure 139 show this authorization profile.

Figure 139 Branch_Wireless_Internet_Only

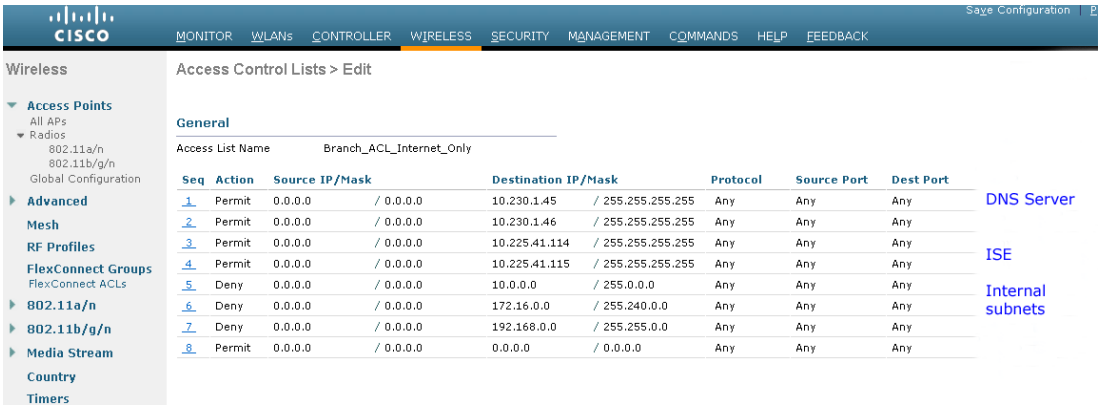


For branch locations, the Cisco 7500 Flex Wireless Controller relies on FlexConnect ACLs to enforce policy permissions. FlexConnect ACLs are created on the WLC and configured with the VLAN defined on the AP or the FlexConnect Group using the VLAN-ACL mapping for dynamic or AAA override VLANs. These FlexConnect ACLs are pushed to the APs when the authorization policy matches.

1. Create a FlexConnect ACL for each branch.
2. Apply the FlexConnect ACL on the FlexConnect group for each branch.
3. Define the VLAN-ACL mapping for each VLAN.

On the FlexConnect 7500 Controller, click **Security > Access Control Lists > FlexConnect ACLs** and define the ACL rules for Internet_Only access. Figure 140 shows the Branch_ACL_Internet_Only ACL, which only allows access to the Internet. This ACL is the same for all branches.

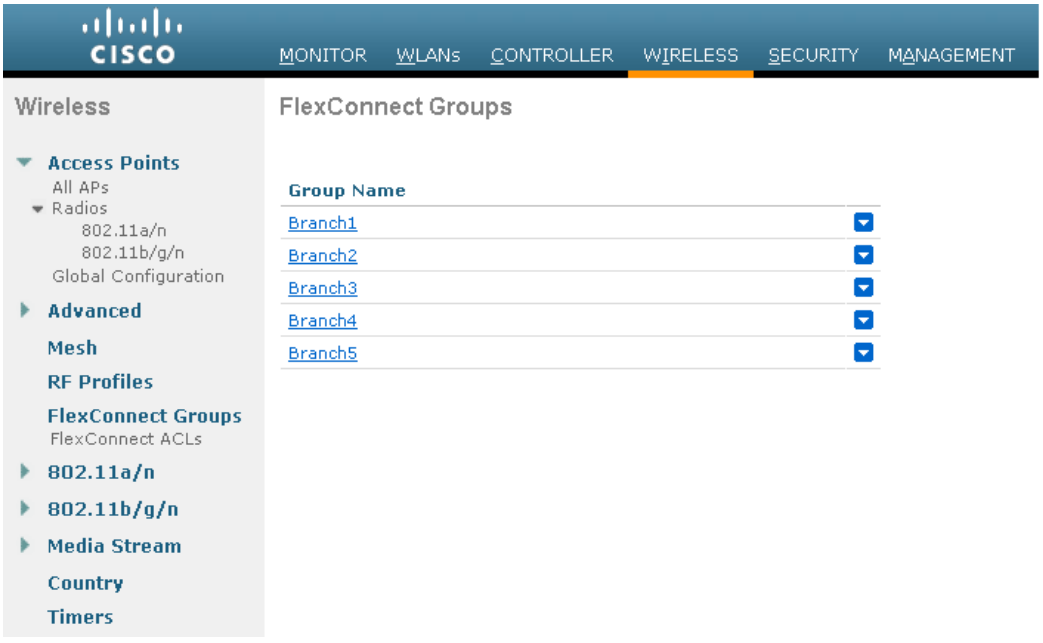
Figure 140 Branch_ACL_Internet_Only



For the purposes of this design guide, a FlexConnect group is defined for each branch, which allows for multiple FlexConnect access points in the branch to share configuration parameters.

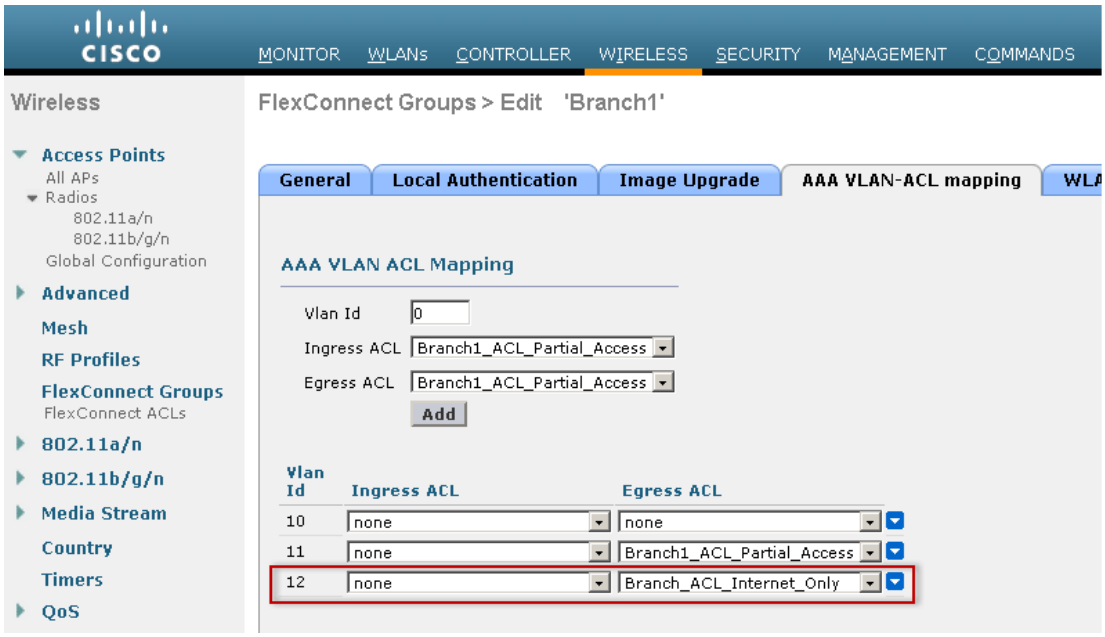
On the FlexConnect 7500 controller, click **Wireless > FlexConnect Groups** and select the FlexConnect group for a particular branch location, as shown in Figure 141.

Figure 141 FlexConnect Groups



In Figure 142, the FlexConnect group for Branch1 is applying the Branch_ACL_Internet_Only ACL to endpoints connecting to VLAN 12.

Figure 142 FlexConnect Group for Branch1



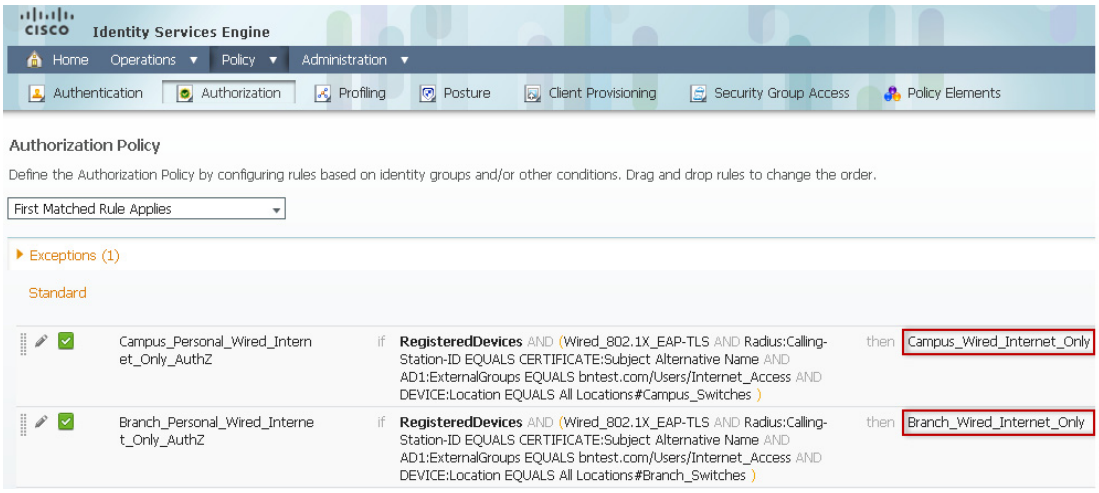
Personal Wired Devices—Internet Only Access

To provide Internet Only access to personal devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the self-registration portal and the device has been added to the RegisteredDevices identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the Internet_Access Active Directory group.

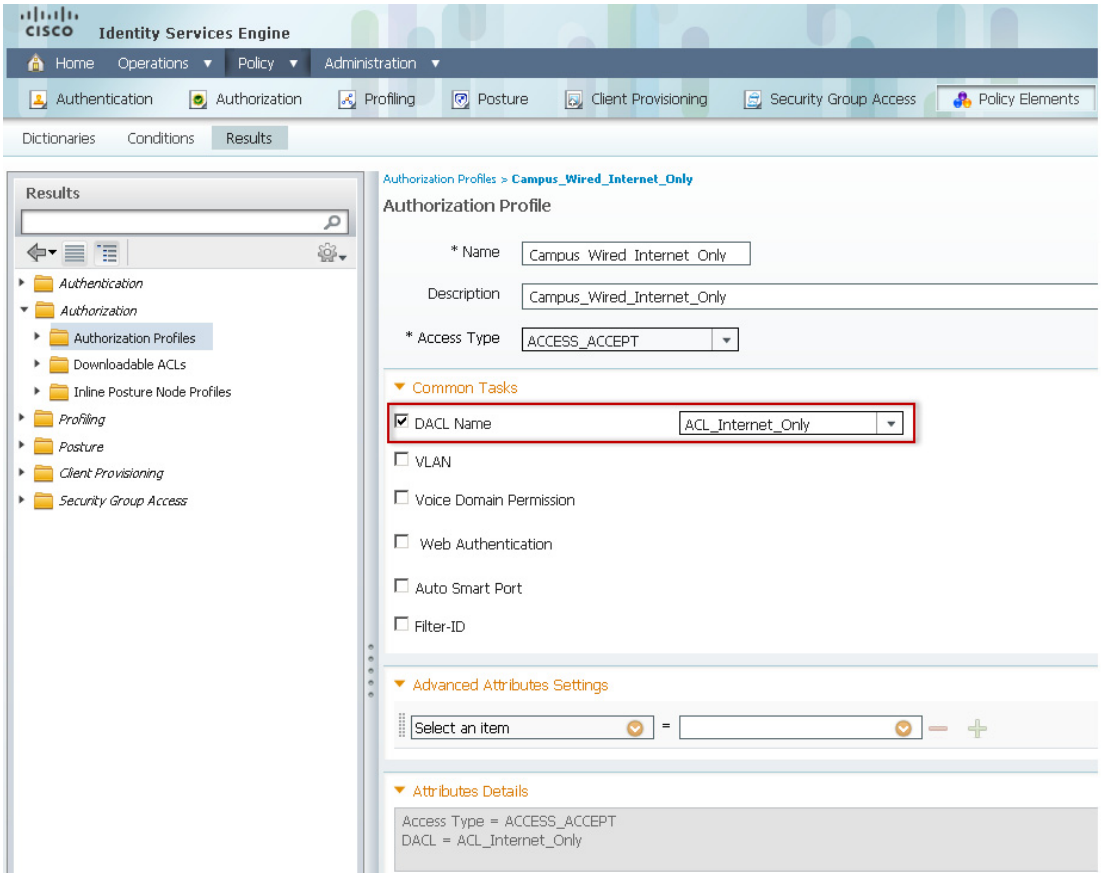
To configure the authorization rules in ISE, click **Policy** > **Authorization**. Figure 143 highlights the authorization policy to grant Internet_Only access to personal devices.

Figure 143 Authorization Policies for Wired Internet Only Access



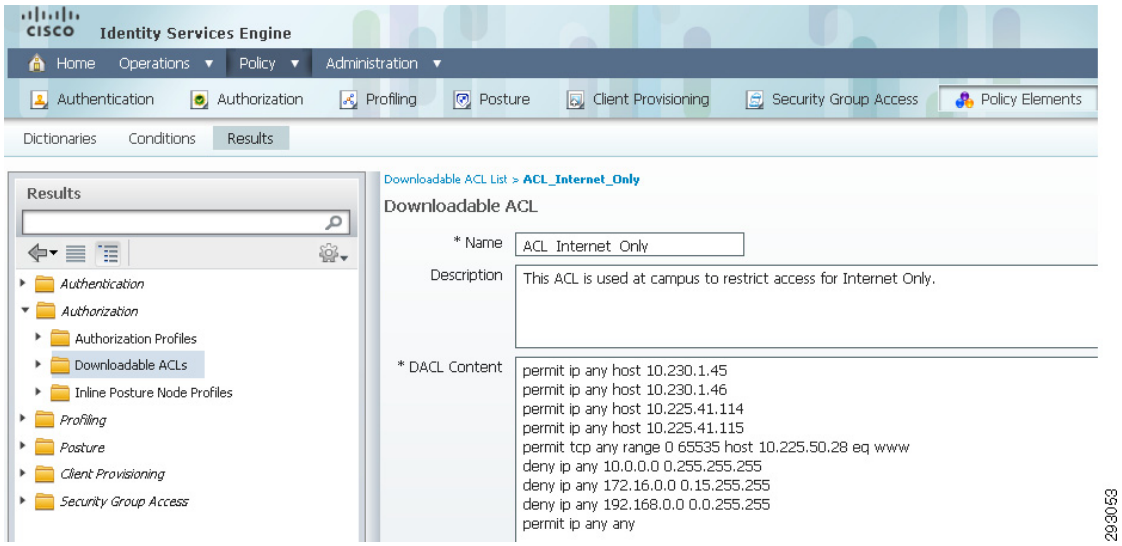
For devices connecting from the campus location, the Campus_Wired_Internet_Only authorization profile uses the dACL named ACL_Internet_Only, which is pushed to the access layer port. Figure 144 shows the Authorization profile.

Figure 144 Campus_Wired_Internet_Only



The details of this dACL are shown in Figure 145.

Figure 145 ACL_Internet_Only



The above ACL provides access to ISE and DNS servers, denies access to all internal networks, and provides access to Internet.

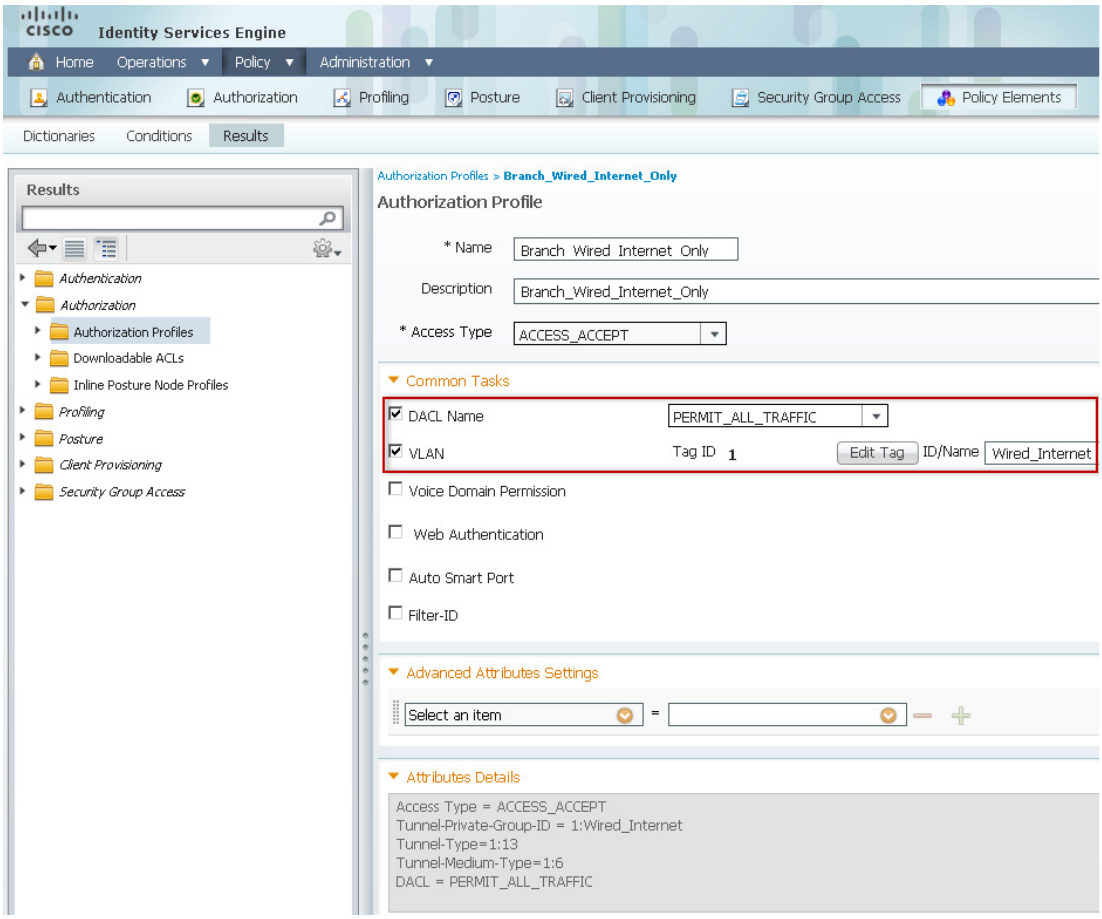
When a device initiates the connection from the branch, then to provide Internet Only access to personal devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the self-registration portal and the device has been added to the RegisteredDevices identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the Internet_Access Active Directory group.

If all of the above conditions match, then the ISE pushes a profile that consists of the VLAN number in which the user is entitled to be and the access-list. Figure 146 illustrates an authorization profile called Branch_Wired_Internet_Only.

To configure the authorization profile in ISE, click **Policy > Policy Elements > Authorization > Authorization Profiles**. Figure 146 illustrates the authorization profile to grant Internet_Only access to personal devices.

Figure 146 Branch_Wired_Internet_Only Authorization Profile



The dACL that is pushed to the access layer switch is PERMIT_ALL_TRAFFIC, which over-rides the default-acl on the port and lets the traffic flow up to the Branch router. In the Branch router there is a static ACL that is applied to every Layer 3 interface that restricts the traffic. The following is an example of the configuration of the Branch router which is configured to restrict traffic initiated by the user to Internet_Only:

```
ip access-list extended ACL_Internet_Only
 permit ip any host 10.230.1.45
 permit ip any host 10.230.1.46
 permit ip any host 10.225.41.114
 permit ip any host 10.225.41.115
 deny  ip any 10.0.0.0 0.255.255.255
 deny  ip any 172.16.0.0 0.15.255.255
 deny  ip any 192.168.0.0 0.0.255.255
 permit ip any any
```

The above ACL is applied to the sub-interface that is associated with VLAN 15. The following is an example of the configuration of the sub-interface:

```
interface GigabitEthernet0/1.15
 encapsulation dot1Q 15
 ip address 10.200.15.2 255.255.255.0
 ip access-group ACL_Internet_Only in
 ip helper-address 10.230.1.61
 standby 15 ip 10.200.15.1
 standby 15 priority 110
```

```
 standby 15 preempt
!
```

Android Devices—Deny Access

The deny access permission is unique in that it focuses on not allowing BYOD devices access to the network. Some organizations may decide to have a more restrictive BYOD environment and grant access only to a specific type of device (e.g., Android, Apple iOS, etc.).

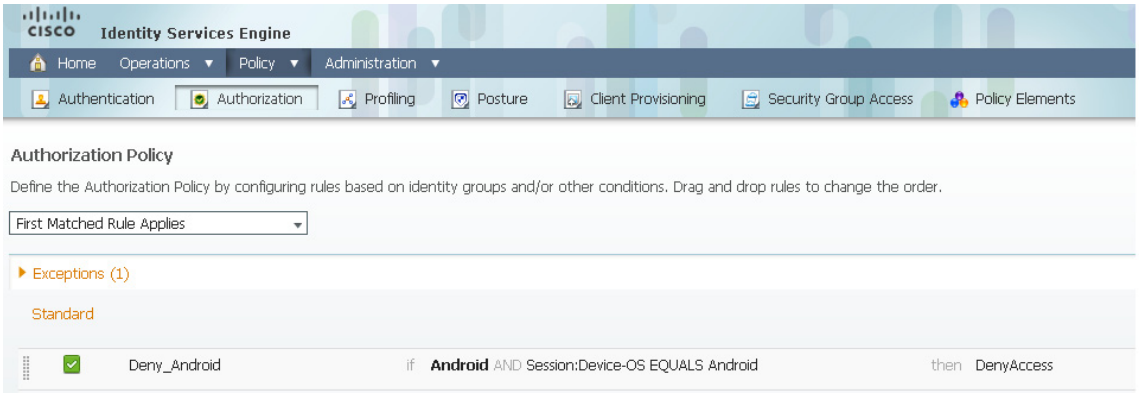
This example focuses on denying access to Android devices, relying on the profiling capabilities of ISE.

To deny access to Android devices, the Cisco ISE verifies the following:

- The employee attempts to connect to the network.
- The ISE profiler identifies the device type.
- If the device type matches the Android identity group, deny access.

To configure the authorization rules in ISE, click **Policy > Authorization**. Figure 147 highlights the authorization policy to deny access to Android devices.

Figure 147 Authorization Policy to Deny Access



The DenyAccess authorization profile is used to enforce the permissions and deny access to Android devices. The DenyAccess profile is a standard ISE profile and cannot be edited. This profile may be found under **Policy > Results> Authorization Profiles**, as shown in Figure 148.

Figure 148 DenyAcces Authorization Profile

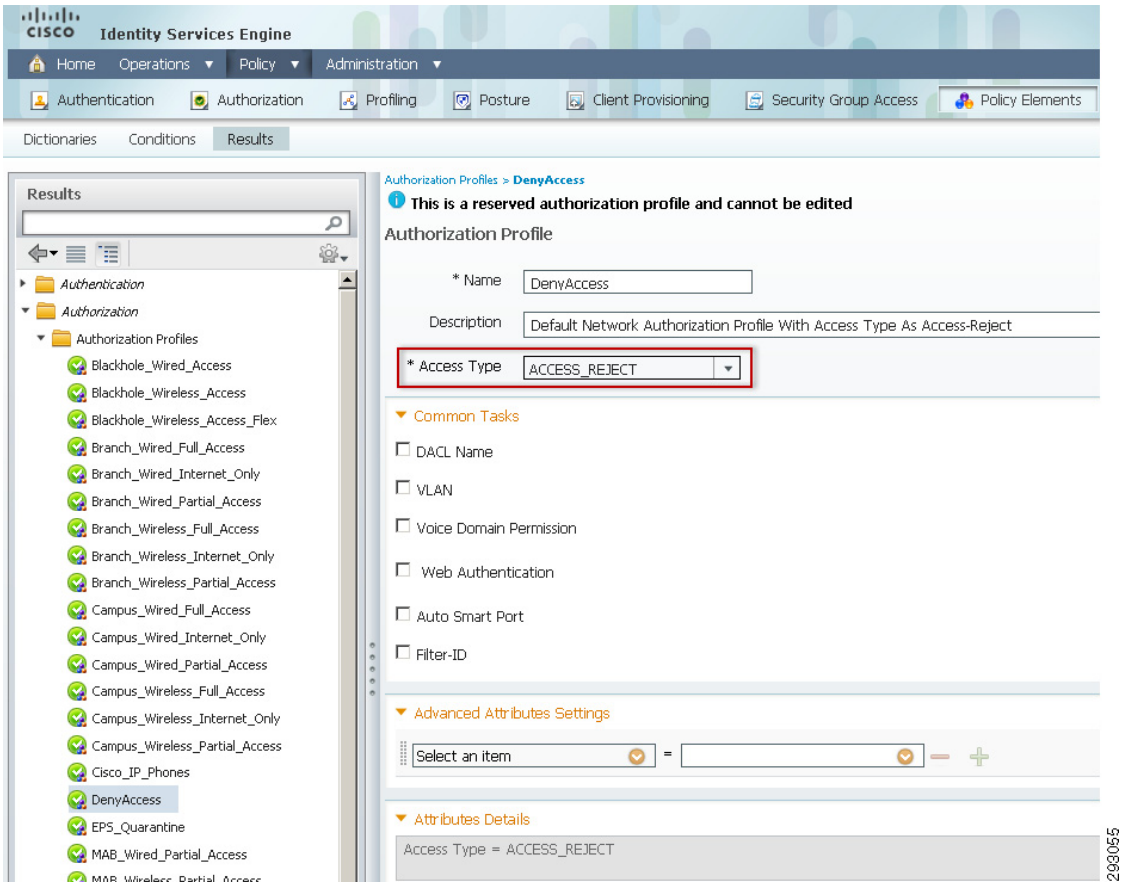


Figure 149 shows an entry from ISE's log, highlighting the fact that the device has been profiled as an Android device and the DenyAccess authorization rule has been enforced.

Figure 149 Deny_Access

For reference purposes, the complete authorization policy used during testing is shown in Figure 150 and Figure 151.

Figure 150 Complete Authorization Policy (1 of 2)

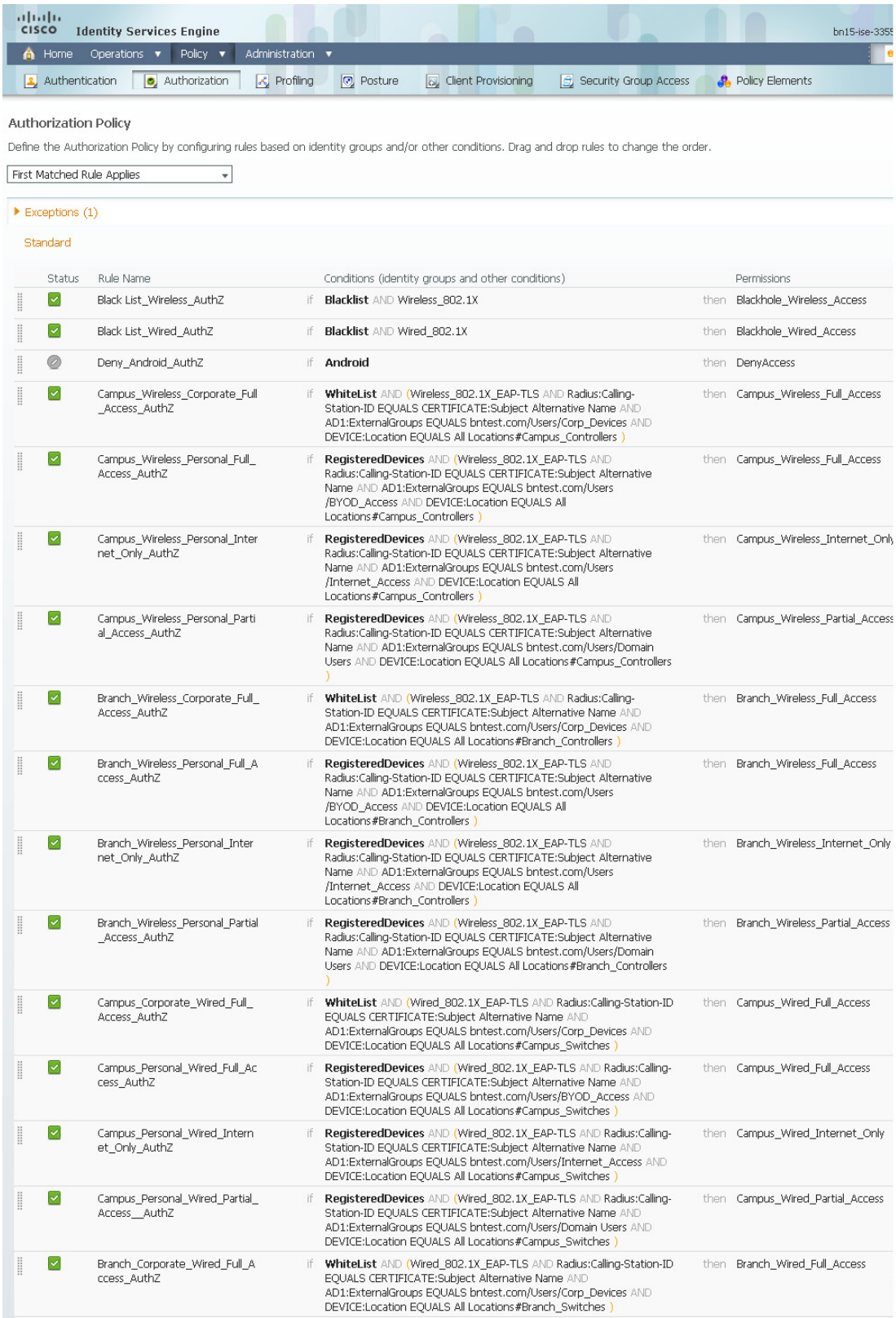
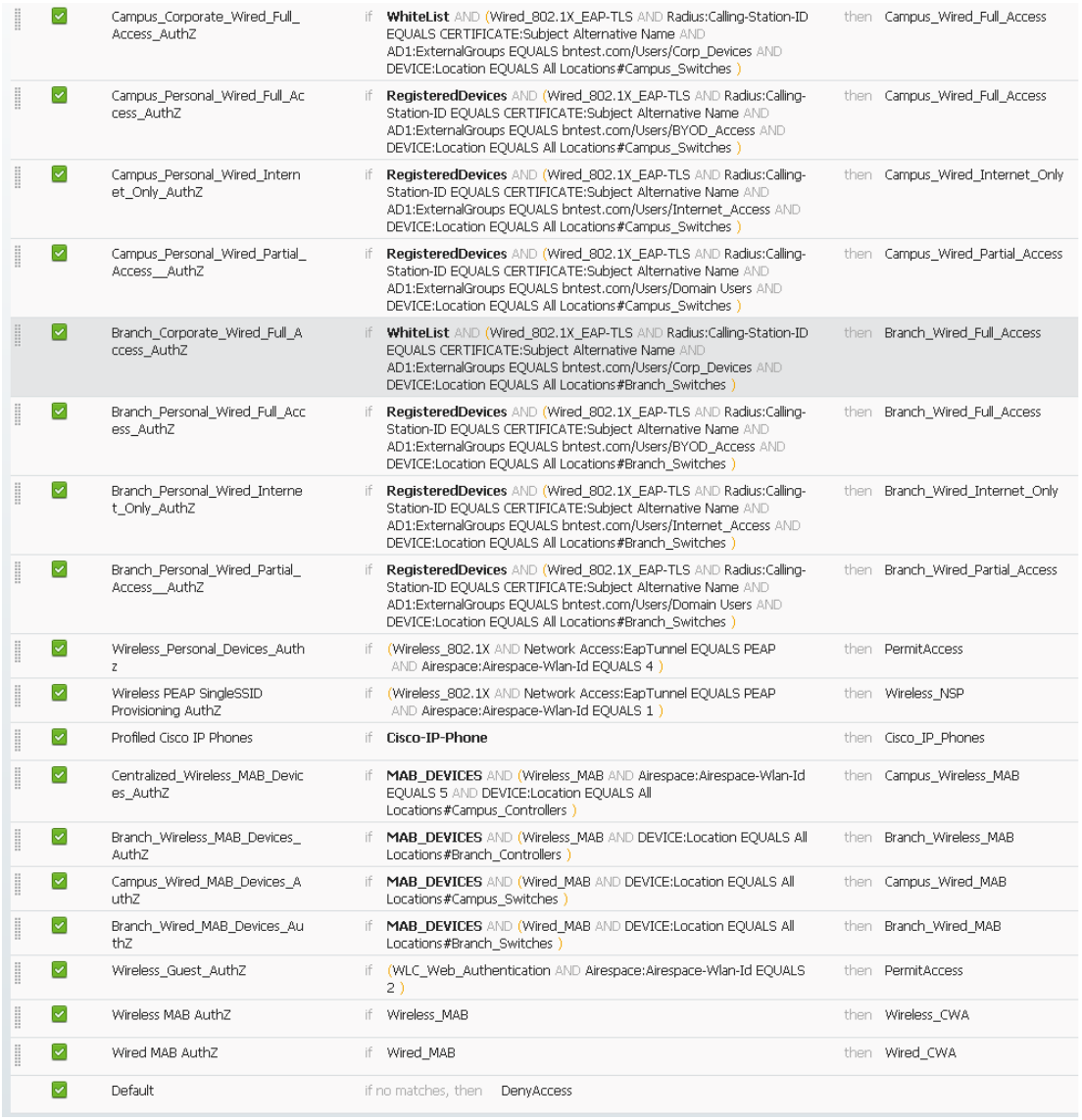


Figure 151 Complete Authorization Policy (2 of 2)



Campus_Corporate_Wired_Full_Access_AuthZ	if	**WhiteList** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Corp_Devices AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Full_Access
Campus_Personal_Wired_Full_Access_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/BYOD_Access AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Full_Access
Campus_Personal_Wired_Internet_Only_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Internet_Access AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Internet_Only
Campus_Personal_Wired_Partial_Access__AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Domain Users AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Partial_Access
Branch_Corporate_Wired_Full_Access_AuthZ	if	**WhiteList** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Corp_Devices AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Full_Access
Branch_Personal_Wired_Full_Access_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/BYOD_Access AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Full_Access
Branch_Personal_Wired_Internet_Only_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Internet_Access AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Internet_Only
Branch_Personal_Wired_Partial_Access__AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Domain Users AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Partial_Access
Wireless_Personal_Devices_Authz	if	(Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND Airespace:Airespace-Wlan-Id EQUALS 4)	then PermitAccess
Wireless PEAP SingleSSID Provisioning AuthZ	if	(Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND Airespace:Airespace-Wlan-Id EQUALS 1)	then Wireless_NSP
Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then Cisco_IP_Phones
Centralized_Wireless_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wireless_MAB AND Airespace:Airespace-Wlan-Id EQUALS 5 AND DEVICE:Location EQUALS All Locations#Campus_Controllers)	then Campus_Wireless_MAB
Branch_Wireless_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wireless_MAB AND DEVICE:Location EQUALS All Locations#Branch_Controllers)	then Branch_Wireless_MAB
Campus_Wired_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wired_MAB AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_MAB
Branch_Wired_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wired_MAB AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_MAB
Wireless_Guest_AuthZ	if	(WLC_Web_Authentication AND Airespace:Airespace-Wlan-Id EQUALS 2)	then PermitAccess
Wireless MAB AuthZ	if	Wireless_MAB	then Wireless_CWA
Wired MAB AuthZ	if	Wired_MAB	then Wired_CWA
Default	if no matches, then	DenyAccess	

293057

User Experience

The Cisco ISE allows employees to be in charge of on-boarding their own devices through a self-registration workflow and simplifies the automatic provisioning of supplicants as well as certificate enrollment for the most common BYOD devices. The workflow supports iOS, Android, Windows, and Mac OS devices and moves the devices from an open environment to a secure network with the proper access based on device and user credentials.

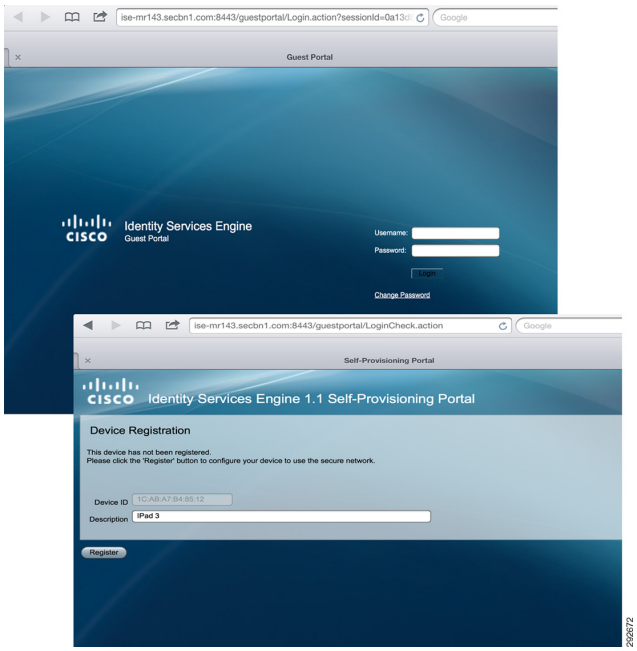
The simple workflow should provide a positive experience to employees provisioning their own device and should allow IT to enforce the appropriate access policies.

Apple iOS Devices

The employee connects to the provisioning SSID and is redirected to the Guest Registration portal for registration after opening a browser. The employee logs in using their Active Directory credentials.

If the device is not yet registered, the session is redirected to the self-registration portal, where the user is aksed enter a description for the new device. The employee is not allowed to change the Device ID (MAC address), which is automatically discovered by ISE.

Figure 152 Guest Portal and Self-Registration Portal

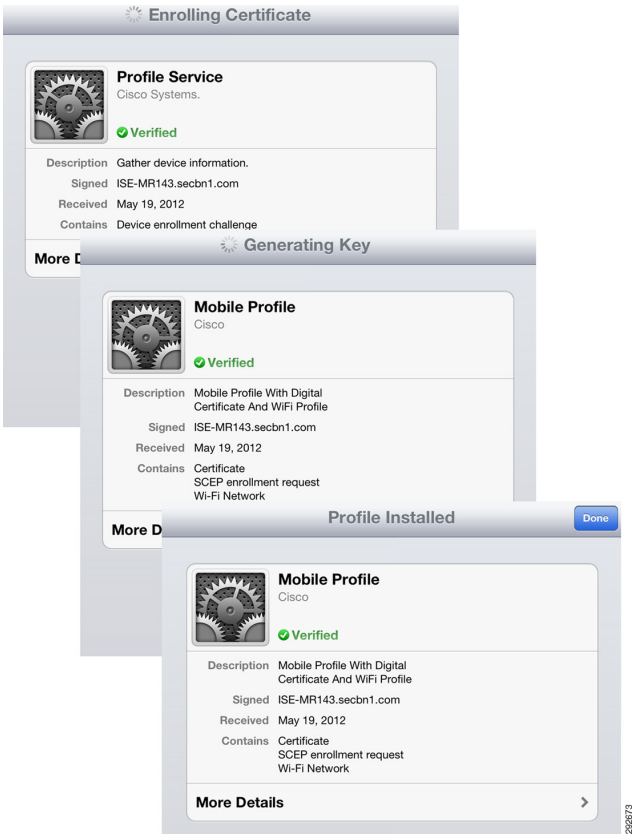


The supplicant profile is downloaded and installed on the endpoint.

Keys are generated and the certificate is enrolled.

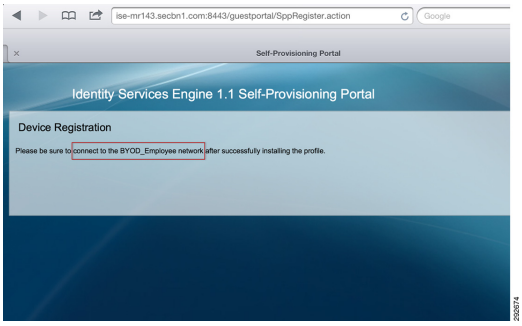
The Wi-Fi profile required to connect to the BYOD_Employee is installed.

Figure 153 Enrollment and Profile Installation



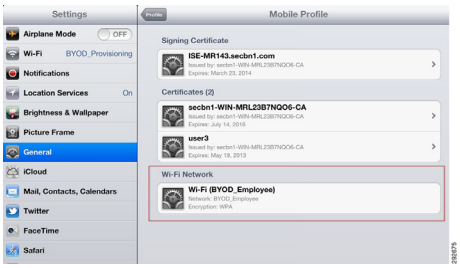
The employee is notified that registration is complete and is reminded to connect manually to the BYOD_Employee SSID.

Figure 154 Device Registration Complete



The certificates and profile can be viewed by clicking **Settings > General > Profiles** and selecting **Mobile Profile**. Figure 155 highlights the Wi-Fi profile to connect to the BYOD_Employee SSID.

Figure 155 Mobile Profile Details



Note For iOS devices, the employee is required to connect manually to the BYOD_Employee SSID.

As shown in Figure 156, the ISE maintains a detailed log of the authentications as they take place:

- The first log shows how the device connects, the MAC address is used for authentication, and the Wireless_CWA profile is used for authorization, enabling the redirection to the Guest Registration portal.
- Once the enrollment and provisioning take place, the user connects to the secure BYOD_Employee SSID. ISE grants Partial Access to the device.

Figure 156 ISE Authentications Log

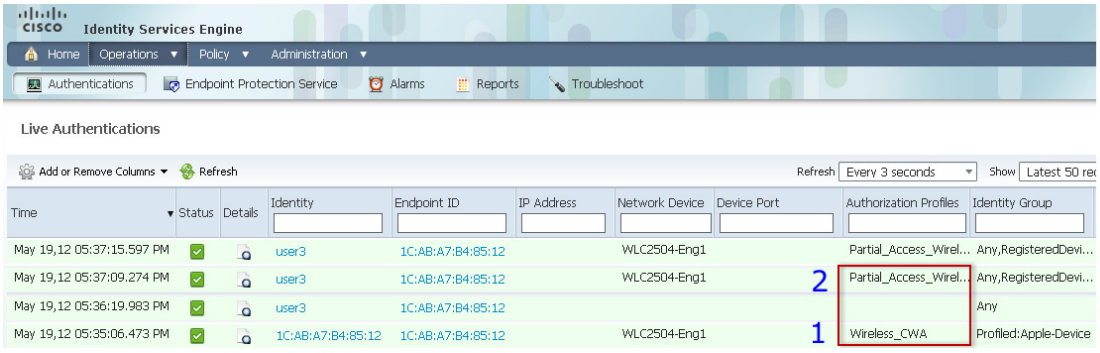


Figure 157 shows in more detail the steps that took place and how the rule was evaluated to grant Partial Access.

- Authentication is dot1x and EAP-TLS.
- Username is user3. The Active Directory (AD1) identity store was used.
- MAC Address is discovered.
- The Wireless_Dot1X_AuthC authentication rule was used.
- The Personal_Partial_Access_Wireless_AuthZ authorization rule matched. This rule enforces the ACL_Partial_Access in the Wireless LAN Controller.

Figure 157 ISE Authentication Details

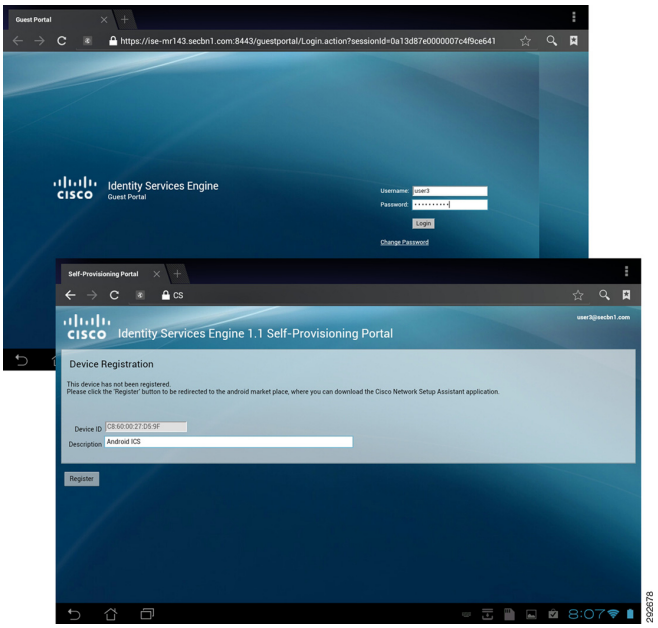
Server:	ISE-MR143
Authentication Method:	dot1x
EAP Authentication Method :	EAP-TLS
EAP Tunnel Method :	
Username:	user3
RADIUS Username :	user3
Calling Station ID:	1C:AB:A7:B4:85:12
Framed IP Address:	
Use Case:	Guest Flow
Network Device:	WLC2504-Eng1
Network Device Groups:	Location#All Locations#Englewood,Device Type#All Device Types
NAS IP Address:	10.19.216.126
NAS Identifier:	WLC2504-1
NAS Port:	1
NAS Port ID:	
NAS Port Type:	Wireless - IEEE 802.11
Allowed Protocol:	Default Network Access
Service Type:	Framed
Identity Store:	AD1
Authorization Profiles:	Partial_Access_Wireless
Active Directory Domain:	
Identity Group:	Any,RegisteredDevices
Allowed Protocol Selection Matched Rule:	Wireless_Dot1X_AuthC
Identity Policy Matched Rule:	Wireless_Certificate
Selected Identity Stores:	
Authorization Policy Matched Rule:	Personal_Partial Access_Wireless_AuthZ
SGA Security Group:	
AAA Session ID:	ISE-MR143/126489141/682
Audit Session ID:	0a13d87e000003364fb774e6
Tunnel Details:	
Cisco-AVPairs:	audit-session-id=0a13d87e000003364fb774e6
	ConfigVersionId=4,DestinationPort=1812,Protocol=Radius,Framed-M

296577

Android Devices

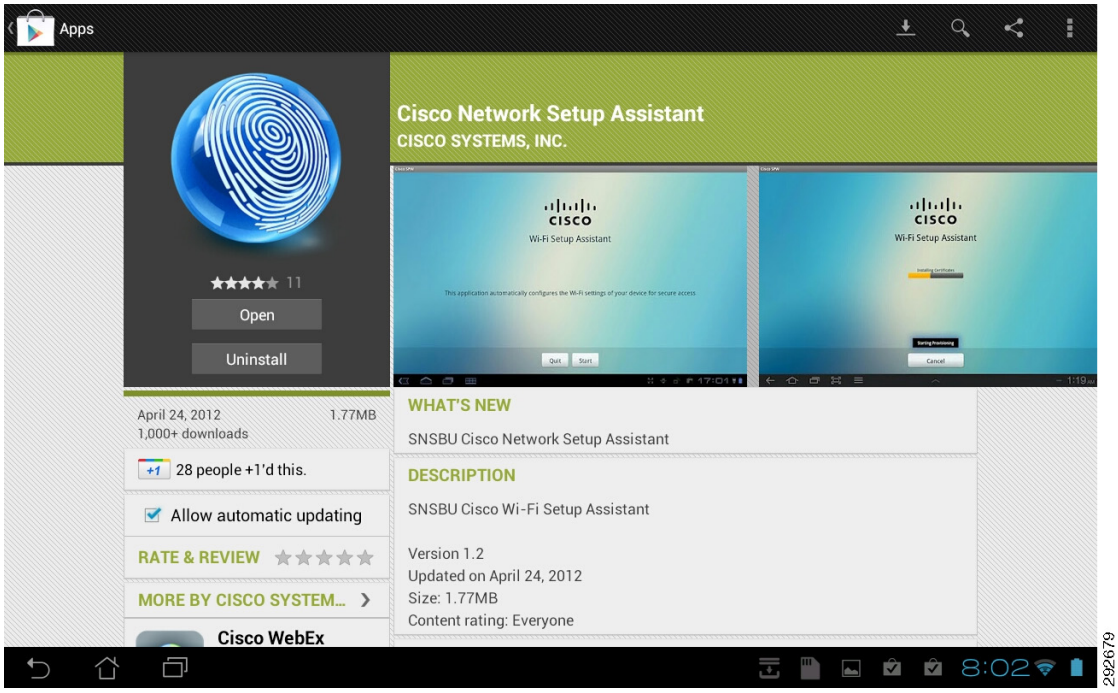
The user experience is very similar when provisioning Android devices. The employee is redirected to the Guest Registration portal and is allowed to enter a description for the new device.

Figure 158 Guest Portal and Self-Registration Portal



The employee is then redirected to the Google Play Store (Android Marketplace) where the Cisco SPW for Android may be downloaded.

Figure 159 Supplicant Provisioning Wizard from Google Play



The SPW is launched and the provisioning process begins. The SPW discovers the ISE and begins downloading the profile and installing the certificates.

Figure 160 Provisioning Process

The employee is allowed to name the certificate and provides a password for the certificate storage for their device. The Wi-Fi profile to connect to BYOD_Employee is applied.

Figure 161 Certificate and Profile

Without employee intervention, the provisioning process automatically connects the Android device to the BYOD_Employee SSID, as shown in Figure 162.

Figure 162 Automatic Connection to BYOD_Employee

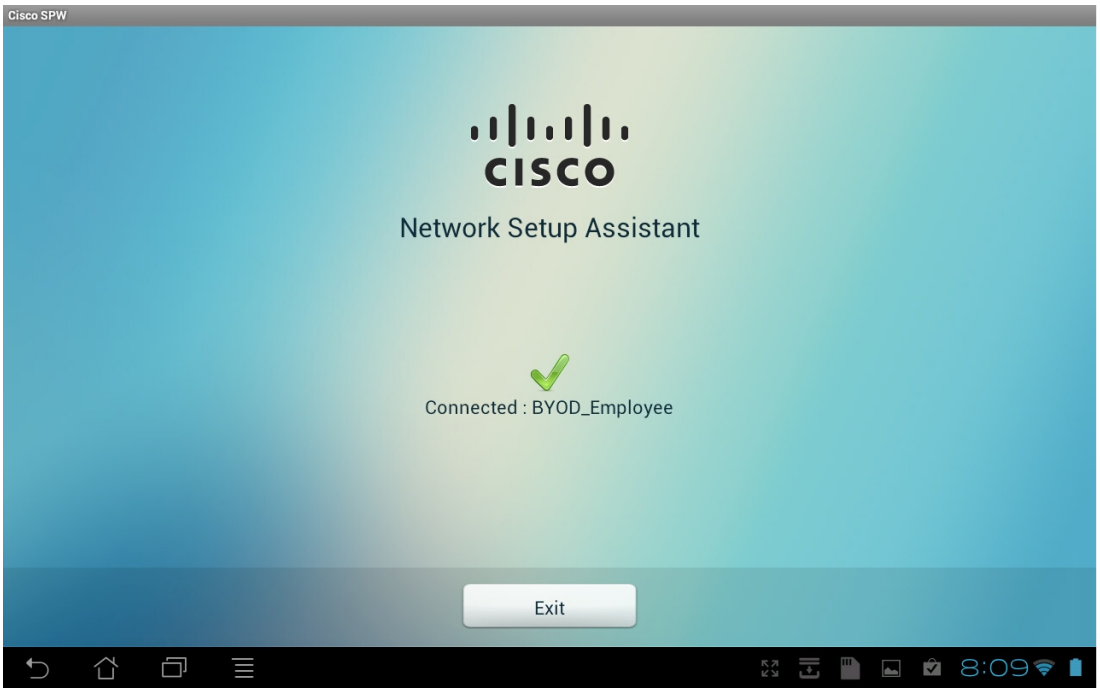
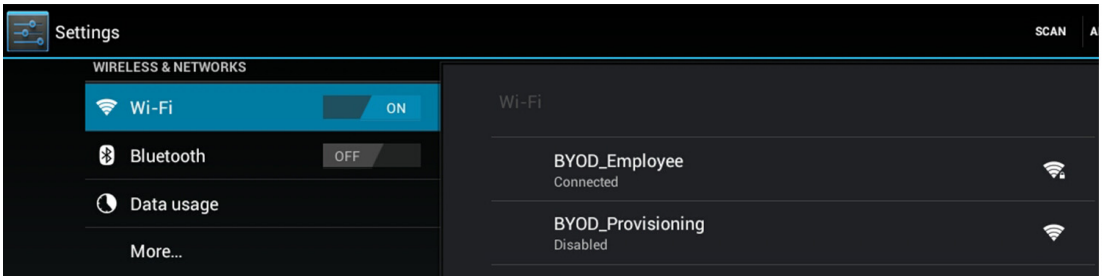


Figure 163 shows how the device is automatically connected to the secure BYOD_Employee SSID.

Figure 163 BYOD_Employee Secure SSID



Windows Devices

The user experience while provisioning a Windows device is very similar, redirecting the session to the Guest Registration portal and asking the employee for authentication.

Some Windows devices have multiple network adapters, for example, a laptop with both wired and wireless adapter. The network security policy checks that the device mac-address (sent using calling-station-id attribute) matches the SAN field of the device digital certificate before allowing access. This is done to prevent spoofing. Since each adapter has a unique mac-address, the anti-spoofing policy check can cause difficulties for devices with multiple adapters. If a device registers with a wired adapter, it will obtain a digital certificate with the mac-address of the wired adapter. If the same device attempts to later authenticate to the secure wireless network, most operating systems will attempt to the use the wired adapter certificate for authentication and will fail because the mac-address of the wireless adapter will not match the SAN field of the digital certificate. To avoid this problem, a device with multiple adapters must register both the wired and wireless adapter.

There are two methods for provisioning wireless devices:

- Dual SSID model, which supports MAB on the provisioning SSID and dot1X on the employee SSID.
- Single SSID model, which supports only the dot1X protocol.

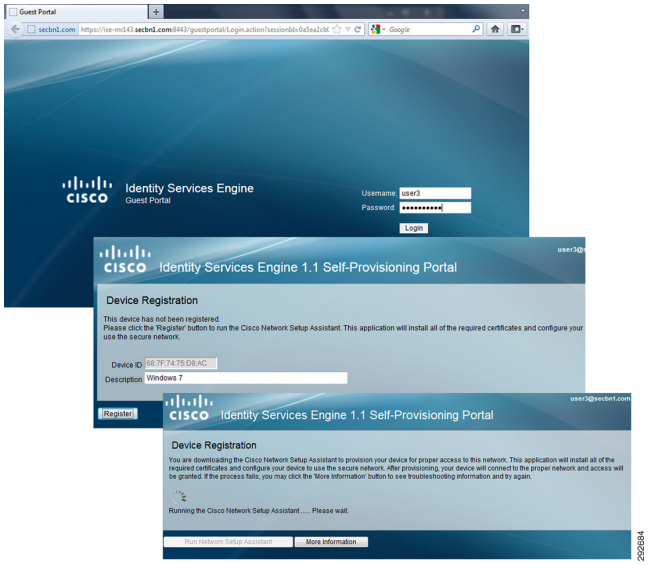
For the Dual SSID method, the wired and wireless adapters may be provisioned in any order. For example, if the device associates with the provisioning SSID (which supports MAB) and is successfully provisioned, then subsequently connects with the wired adapter, dot1x will fail because of the anti-spoofing check in the policy and provisioning will complete using MAB. Thereafter, the device can access the network with either adapter.

For the Single SSID method, the order in which the wired and wireless adapters are provisioned matters. For example, if the device connects using the wired adapter first and is successfully provisioned, then subsequently connects using the wireless adapter, some operating systems attempt to establish a EAP-TLS connection using the wired digital certificate instead of undergoing the provisioning process. This connection attempt will fail because of the anti-spoofing check in the policy. To prevent this from happening, the user must provision the wireless adapter before connecting with the wired adapter for the single SSID method.

Windows Wireless Devices

After authenticating at the portal and entering a description for the new Windows device, the SPW is downloaded.

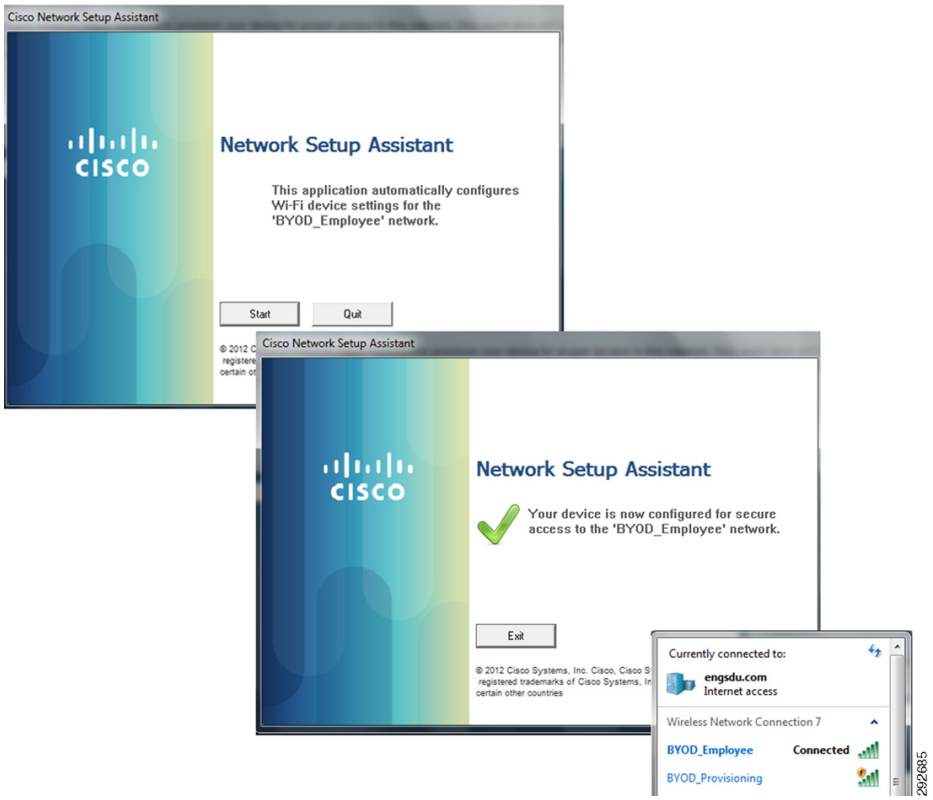
Figure 164 Guest Registration Portal



The SPW is launched to install the profile, the keys are generated, and the certificate enrollment takes place.

The SPW installs the BYOD_Employee configuration to connect to the secure SSID. The connection is switched automatically to the BYOD_Employee SSID.

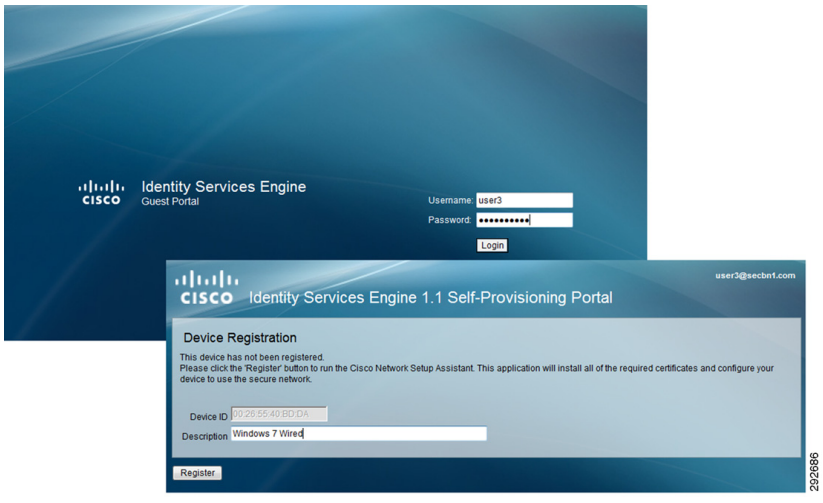
Figure 165 SPW and Connection to Secure SSID



Windows Wired Devices

The user experience is very similar, but instead of configuring access to a secure SSID, the SPW configures the devices to connect via a wired connection.

Figure 166 Guest Registration Portal



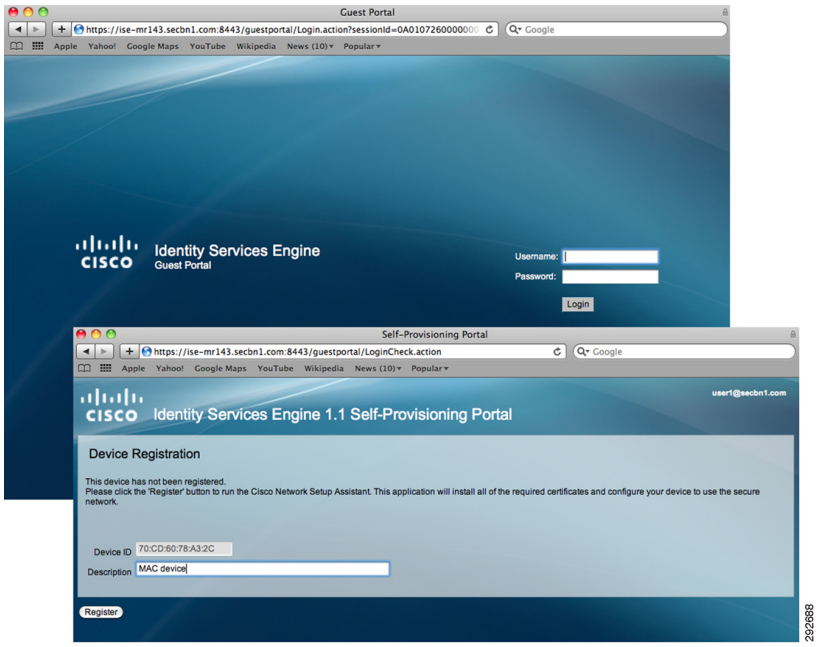
The SPW is downloaded and the proper configurations are applied to the device.

Figure 167 SPW and Secure Access

Mac OS/X Devices

The user experience while provisioning a Mac OS X wired device is also very similar, redirecting the session to the Guest Registration portal and asking the employee for authentication.

Figure 168 Guest Registration and Self-Registration Portals

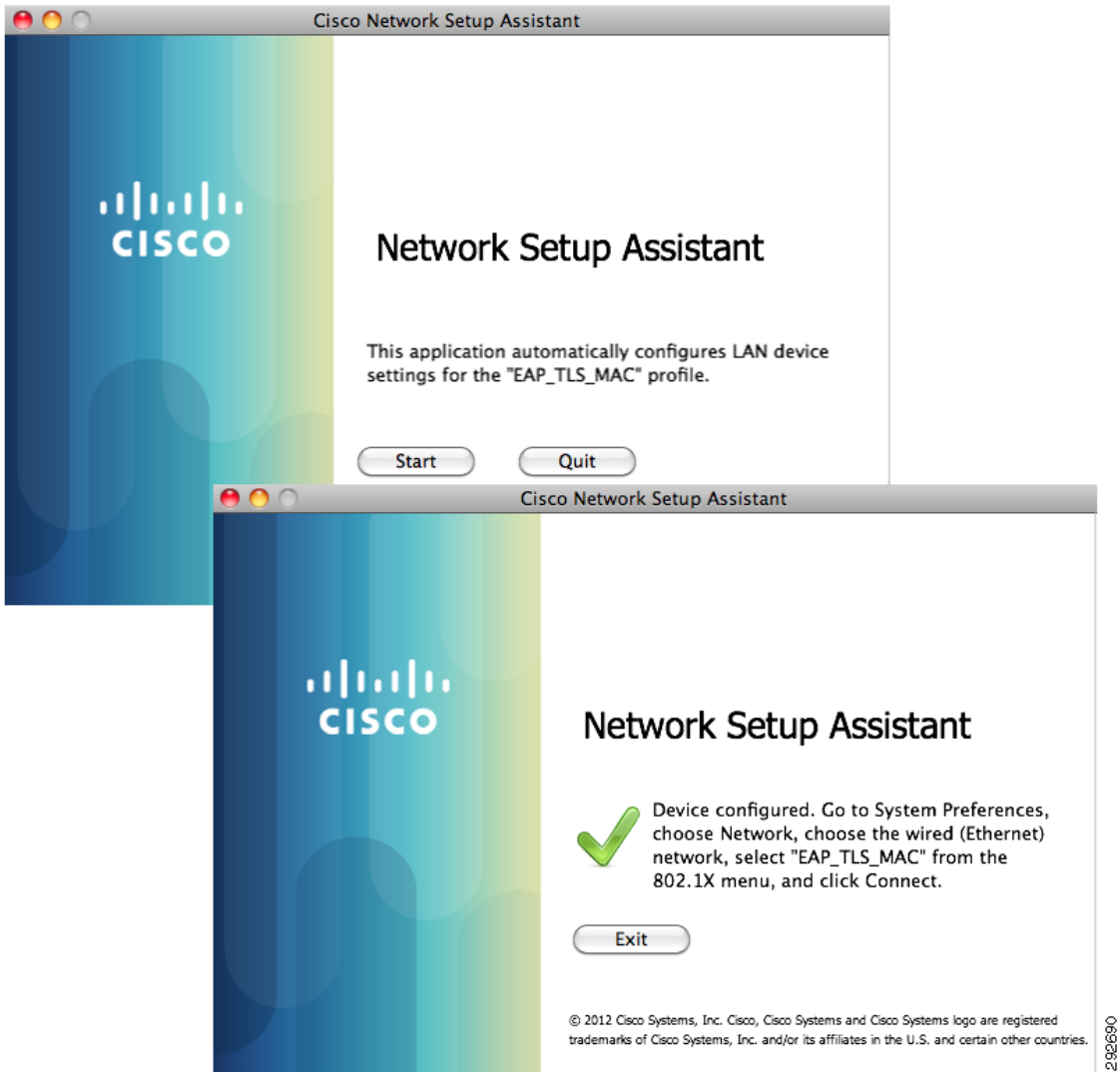


The SPW is downloaded and installed.

Figure 169 SPW and Secure Access

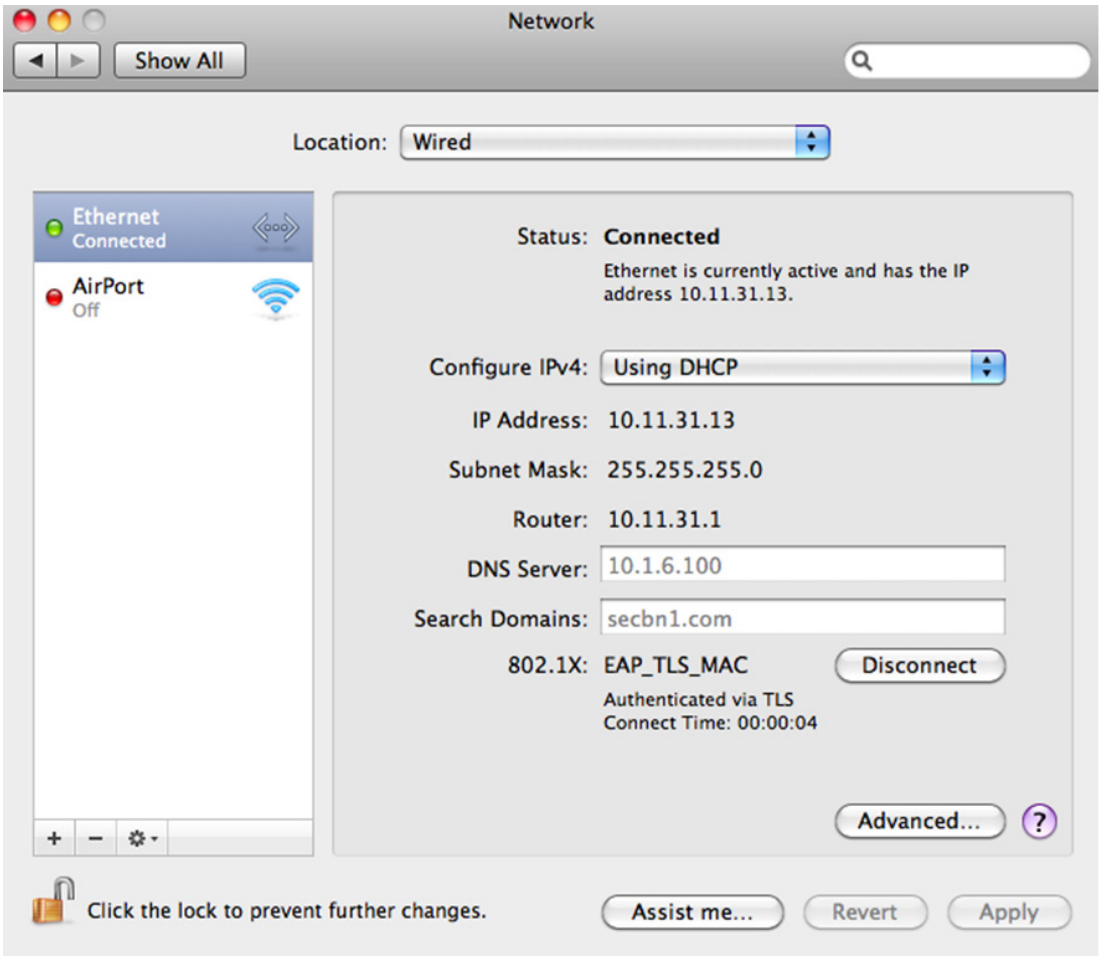
The Network Setup Assistant configures the EAP-TLS_MAC profile for secure access.

Figure 170 Network Setup Assistant



The network settings in Figure 171 show the new EAP_TLS_MAC configuration.

Figure 171 Network Settings



Cisco Jabber Clients and the Cisco BYOD Infrastructure

Cisco Jabber, a Cisco mobile client application, provides core Unified Communications and collaboration capabilities, including voice, video, and instant messaging to users of mobile devices such as Android and Apple iOS smartphones and tablets. When a Cisco Jabber client device is attached to the corporate wireless LAN, the client can be deployed within the Cisco Bring Your Own Device (BYOD) infrastructure.

Because Cisco Jabber clients rely on enterprise wireless LAN connectivity or remote secure attachment through VPN, they can be deployed within the Cisco Unified Access network and can utilize the identification, security, and policy features and functions delivered by the BYOD infrastructure.

The Cisco BYOD infrastructure provides a range of access use cases or scenarios to address various device ownership and access requirements. The following high-level access use case models should be considered:

- Enhanced Access—This comprehensive use case provides network access for corporate, personal, and contractor/partner devices. It allows a business to build a policy that enables granular role-based application access and extends the security framework on and off-premises.
- Limited Access—Enables access exclusively to corporate issued devices.

- Basic Access—This use case is an extension of traditional wireless guest access. It represents an alternative where the business policy is to not on-board/register employee wireless personal devices, but still provides Internet-only or partial access to the network.

Use Case Impact on Jabber

The Enhanced use case allows the simplest path for implementing a Cisco Jabber solution. Cisco Jabber clients, whether running on corporate or personal devices, require access to numerous back-end on-premises enterprise application components for full functionality. The Enhanced Access use case will allow access from corporate devices with the option of allowing access from personal devices for Jabber back-end applications.

The Limited Access use case will allow Jabber use only from corporate devices.

Basic Access adds a significant layer of complexity for personal devices, requiring them to have access to back-end on-premise Jabber applications from the DMZ. Various signal, control, and media paths must be allowed through the firewall for full functionality.

In the case of cloud-based collaboration services, Cisco mobile clients and devices connect directly to the cloud through the Internet without the need for VPN or full enterprise network attachment. In these scenarios, user and mobile devices can be deployed using the Basic Access model because these use cases require only Internet access.

Other Jabber Design Considerations

When deploying Cisco Jabber clients within the Cisco BYOD infrastructure, consider the following high-level design and deployment guidelines:

- The network administrator should strongly consider allowing voice- and video-capable clients to attach to the enterprise network in the background (after initial provisioning), without user intervention, to ensure maximum use of the enterprises telephony infrastructure. Specifically, use of certificate-based identity and authentication helps facilitate an excellent user experience by minimizing network connection and authentication delay.
- In scenarios where Cisco Jabber clients are able to connect remotely to the enterprise network through a secure VPN:
  - The network administrator should weigh the corporate security policy against the need for seamless secure connectivity without user intervention to maximize utilization of the enterprise telephony infrastructure. The use of certificate-based authentication and enforcement of a device pin-lock policy provides seamless attachment without user intervention and functionality similar to two-factor authentication because the end user must possess the device and know the pin-lock to access the network. If two-factor authentication is mandated, then user intervention will be required in order for the device to attach remotely to the enterprise.
  - It is important for the infrastructure firewall configuration to allow all required client application network traffic to access the enterprise network. Failure to open access to appropriate ports and protocols at the corporate firewall could result in an inability of Cisco Jabber clients to register to on-premises Cisco call control for voice and video telephony services and/or the loss of other client features such as enterprise directory access or enterprise visual voicemail.
- When enterprise collaboration applications such as Cisco Jabber are installed on employee-owned mobile devices, if the enterprise security policy requires the device to be wiped or reset to factory default settings under certain conditions, device owners should be made aware of the policy and encouraged to backup personal data from their device regularly.

- When deploying Cisco Jabber, it is important for the underlying network infrastructure to support, end-to-end , the necessary QoS classes of service, including priority queuing for voice media and dedicated video and signaling bandwidth, to ensure the quality of client application voice and video calls and appropriate behavior of all features.

For further information regarding Cisco Jabber clients, see the product collateral and documentation at: http://www.cisco.com/go/jabber.

For further information regarding Cisco Mobile Unified Communications, see the Cisco Unified Communications System 9.X SRND at: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/9x/mobilapp.html.

Limited BYOD Access

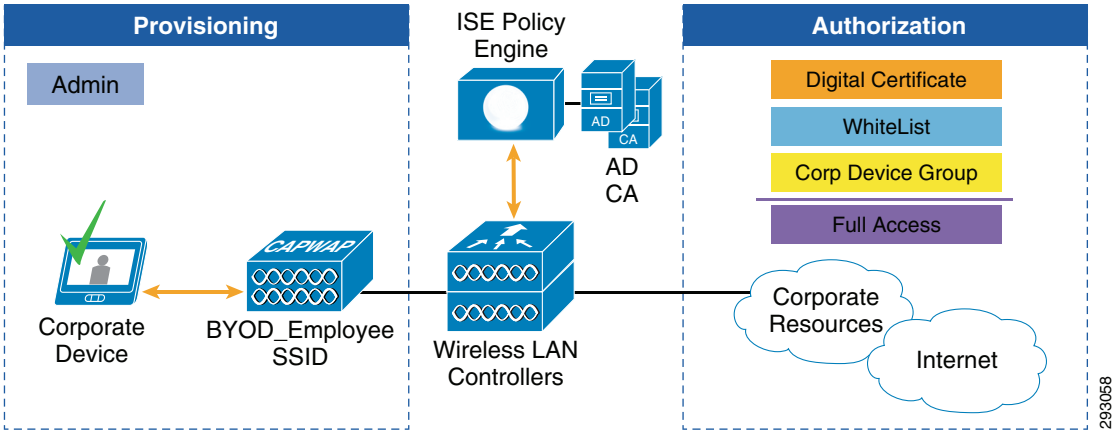
This chapter discusses design considerations and the construction of policy rules for providing access to corporate devices and the security policy being enforced by the Cisco ISE. A corporate device is a corporate asset that is provided by the organization and has been provisioned with the right configuration profiles and has a digital certificate which is enrolled by IT. Since the device has already been on-boarded and configured by an IT administrator, the employee is not required to go through the registration steps.

Cisco ISE provides many ways to enforce security policies and determines what network resources each device is allowed to access. This section focuses on allowing full access to provisioned corporate devices.

The ISE feature set is extremely flexible to meet diverse business requirements and this section focuses on different ways to enforce those policies. The goal of this section is to highlight this flexibility and explain the steps to restrict access for BYOD devices.

Figure 172 shows how a corporate mobile device connects to the network and the different authorization rules checked by ISE to grant full access. Different network components play a role in this process, including the wireless infrastructure, Active Directory, a CA server, etc.

Figure 172 Provisioning Corporate Devices



Identity Groups, Active Directory, and WhiteList

An identity group is a logical list used to group endpoints according to their profiles and is an efficient way for ISE to enforce different permissions to different types of devices. Devices that have gone through the provisioning process get added to the RegisteredDevices identity group in ISE. It is assumed that corporate devices have been provisioned by an IT administrator and have the digital certificates and permissions necessary to get full access to corporate resources.

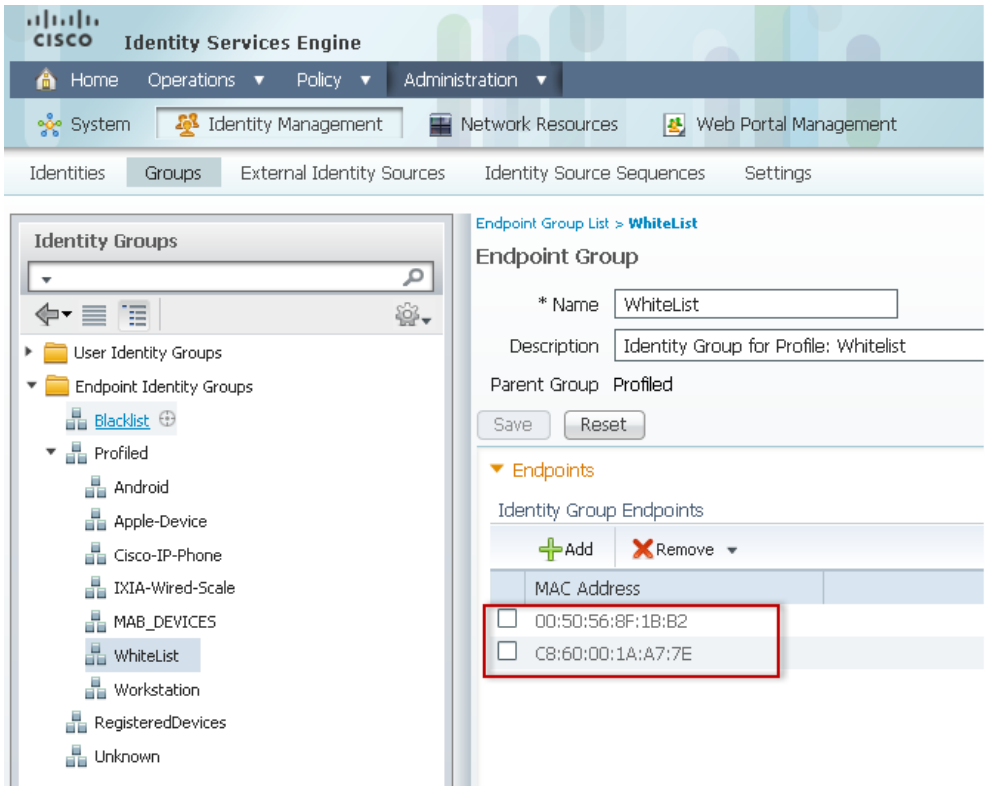
For this design guide, an additional identity group was defined for the purpose of uniquely identifying corporate devices. This identity group, named WhiteList, maintains a list of devices owned by the corporation. The WhiteList is manually updated by the IT administrator and contains the MAC addresses that are granted full access. The assumption is that IT has decided to grant corporate devices full access to the network and has added the devices to the WhiteList.

Endpoints may be moved to other identity groups, such as the WhiteList identity group or the Blacklist identity group, used when a device is lost or stolen. Managing a Lost or Stolen Device has more details on the Blacklist identity group.

Note Endpoints can only be members of one identity group at a time.

To update an endpoint's identity group, click **Administration > Groups > Endpoint Identity Groups**. Figure 173 shows endpoints as members of the WhiteList identity group.

Figure 173 WhiteList Identity Group



For this use case an Active Directory group is used as an additional way to grant access to different users. This section relies on the following AD group:

- Corp_Devices—Members of this group are allowed full access. This group is maintained by an IT administrator.

This model could easily be expanded to include other user groups with similar access requirements.

ISE Integration with Active Directory explains the steps to synchronize AD groups to ISE.

Figure 174 highlights the policy tested in this section, along with the different requirements and permissions. These policies, along with detailed configurations, are explained in this section.

Figure 174 Access Policies and Permissions

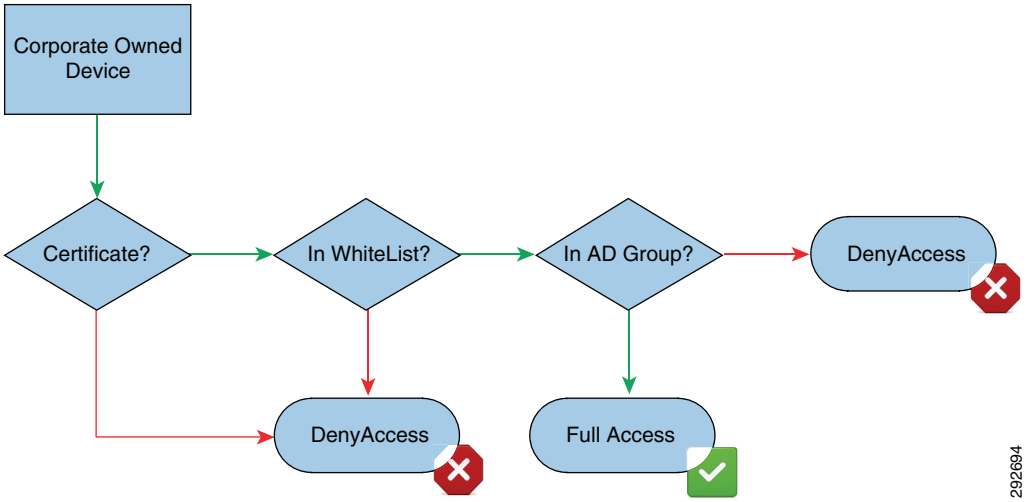
Policy	Identity Group	AD Group	Profile	Permission
Corporate Owned	WhiteList	Corp_Devices		Full

293060

This section assumes that to obtain Full Access the device has been provisioned by IT and the employee is a member of the Corp_Devices Active Directory group.

Figure 175 highlights the connectivity flow to allow full access to corporate devices. If the device belongs to the WhiteList Identity group, has a digital certificate, and the user is a member of the Corp_Devices AD group, then the user is granted full access.

Figure 175 Corporate Device BYOD Access



Corporate Devices—Full Access

To provide full access to corporate devices, the Cisco ISE verifies the following:

- The device has been provisioned by IT.
- The device has been added to the WhiteList identity group.
- The Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is member of the Corp_Devices Active Directory group.

Since the wireless design relies on two different clusters of WLCs, unique authorization rules are created for connections coming from the branch or the campus. To differentiate these connections, the ISE relies on Network Device Groups to group WLCs based on their location. This allows a single ISE to enforce policies across different groups of devices.

Figure 176 shows the different locations created for branch and campus devices.

Figure 176 Locations

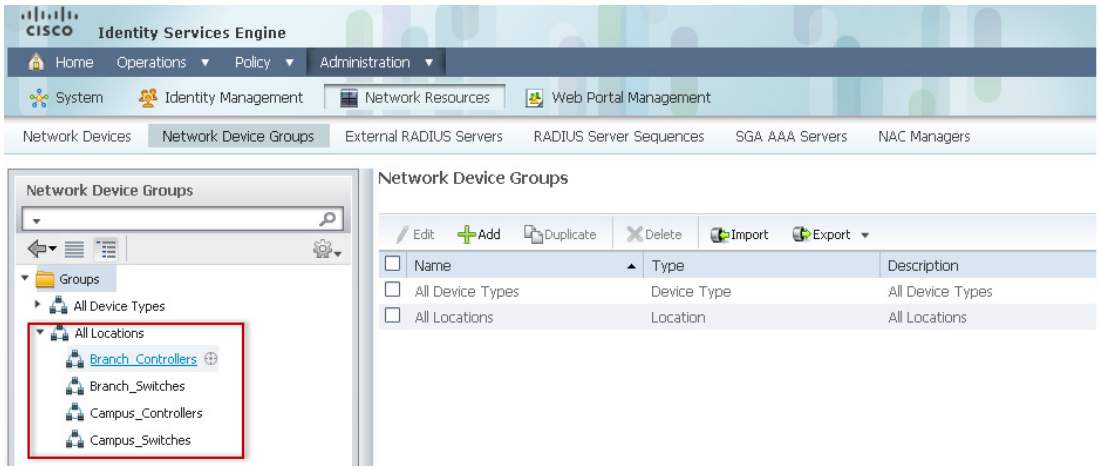
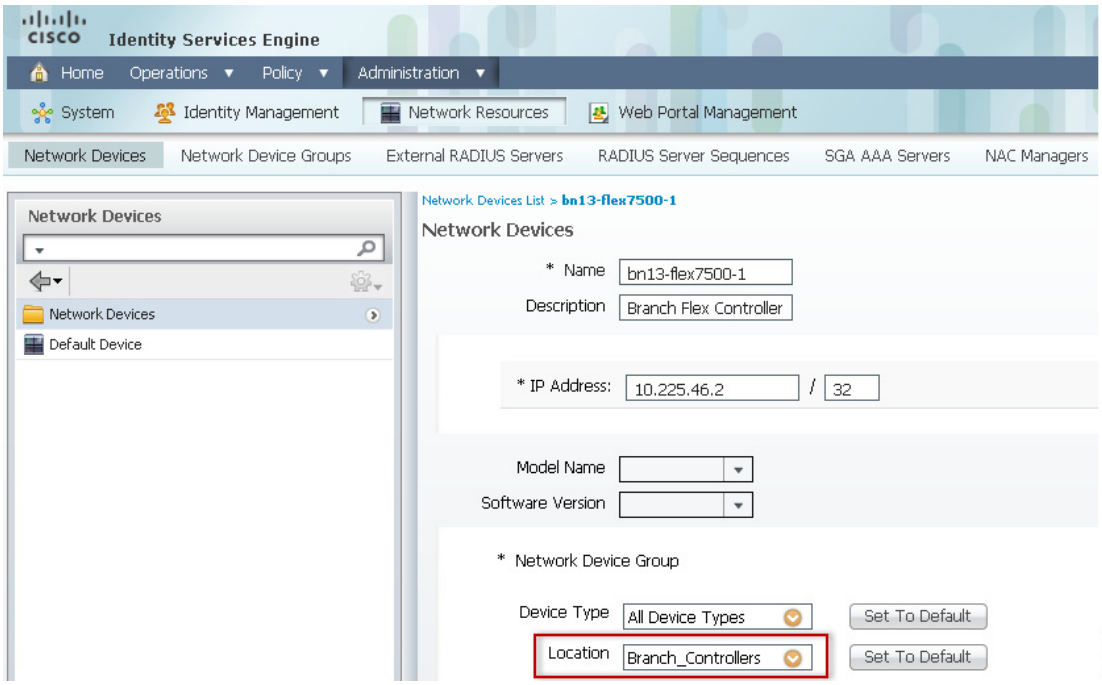


Figure 177 shows how the bn13-flex7500-1 controller belongs to the Branch_Controllers Network Device Group.

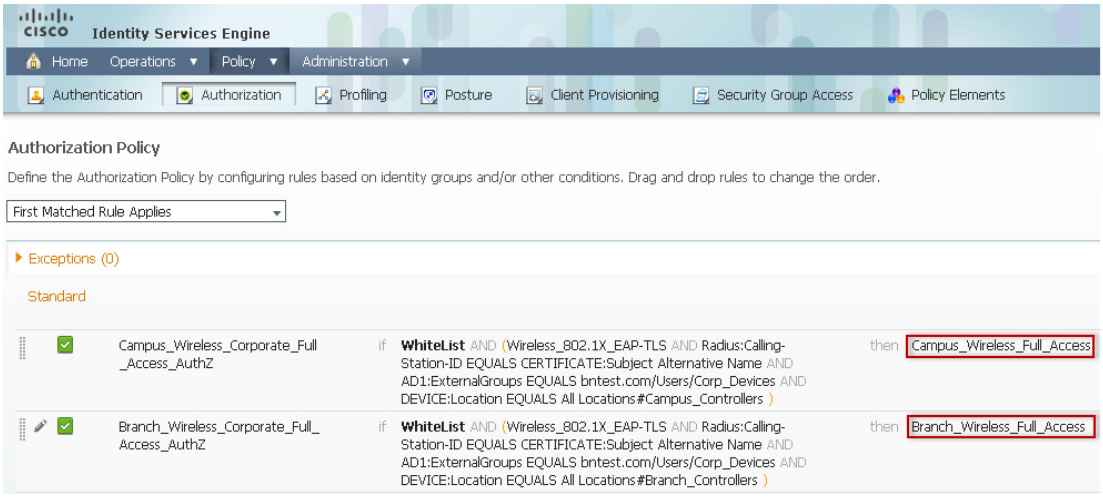
Figure 177 Branch Controller



Controllers managing wireless devices in the campus are assigned to the Campus_Controllers group.

To configure the authorization rules in ISE, click **Policy > Authorization**. Figure 178 highlights the authorization policy to grant full access to personal devices.

Figure 178 Authorization Policies for Full Access

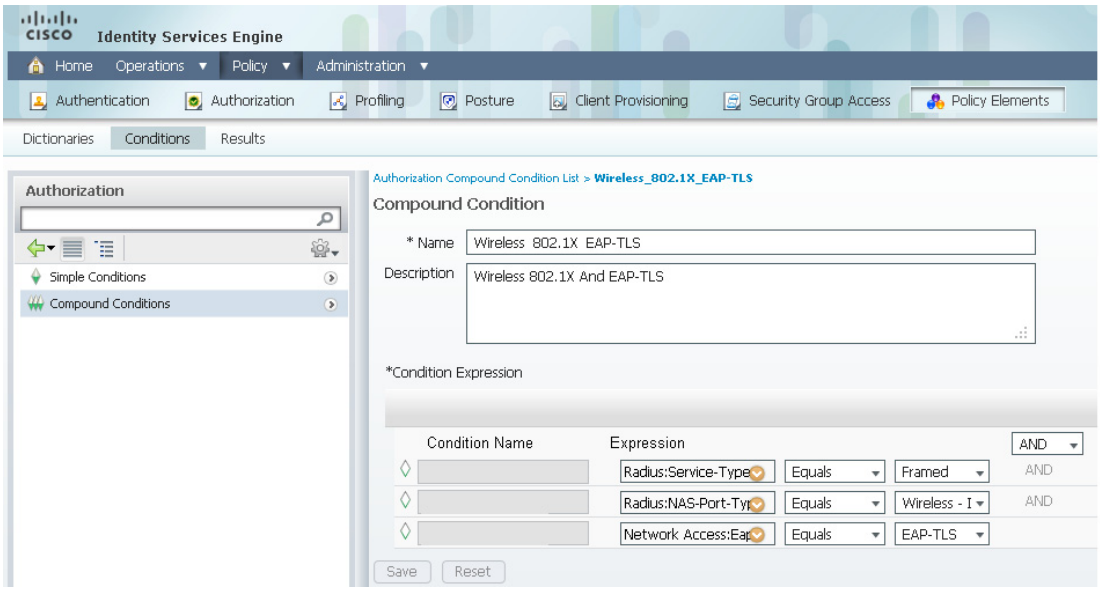


Looking at the first rule in more detail, ISE evaluates these conditions:

- WhiteList—The endpoint has been added by an IT Administrator to the WhiteList identity group.
- Wireless_802.X_EAP-TLS—A wireless endpoint using EAP-TLS (defined as a compound condition).
- Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name—The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name.
- AD1:ExternalGroups EQUAL Corp_Devices—The user belongs to the Corp_Devices Active Directory group.
- DEVICE:Location EQUALS Campus_Controllers—The connection originated from a WLC controller in the campus.

As shown in Figure 178, a compound condition was used to combine three conditions, such as Radius:Service-Type, Radius:NAS-Port-Type, and EAP authentication, into a single rule. Compound conditions allow combining multiple conditions into a single one, which improves the readability of policy rules. To define a compound condition, click **Policy > Conditions > Authorization > Compound Conditions**. Figure 179 shows how the three previous conditions may be combined into a single compound condition.

Figure 179 Compound Condition



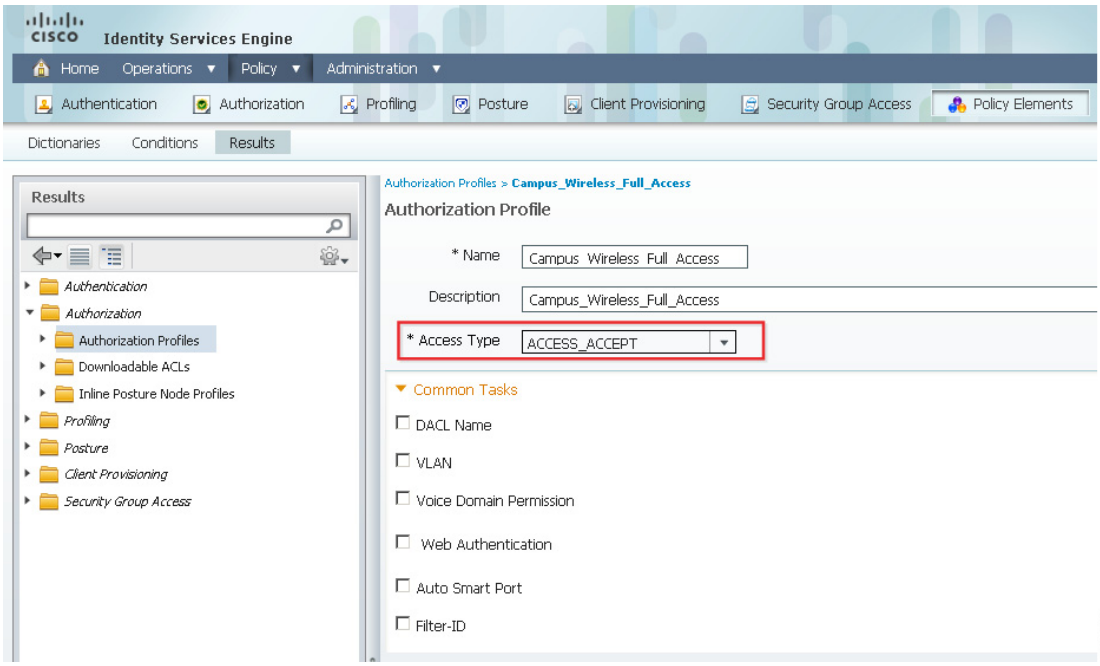
Authorization Profiles for Wireless Users

When all conditions in the authorization policy rules match, the rule invokes the proper authorization profile:

- *Campus_Wireless_Full_Access* for 802.1X wireless devices.
- *Branch_Wireless_Full_Access* for 802.1X wired devices.

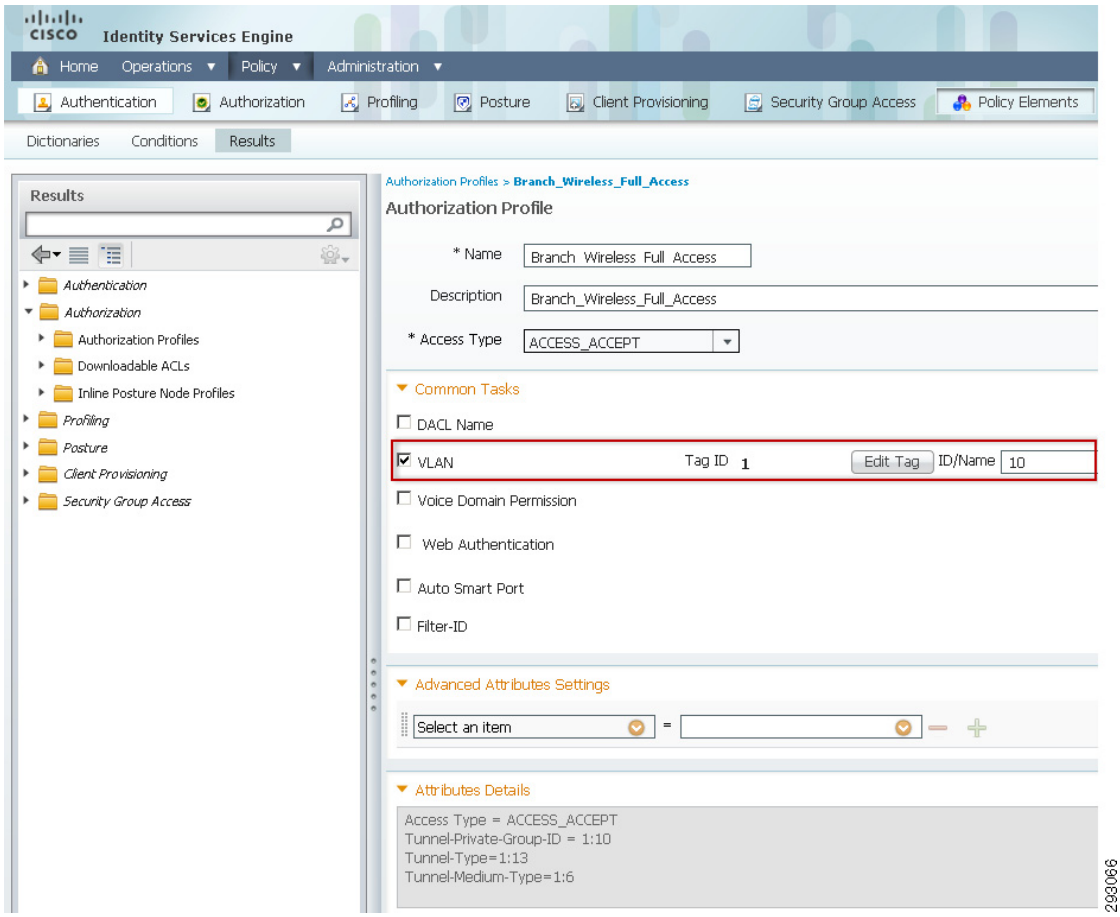
Figure 180 shows how the Campus_Wireless_Full_Access authorization profile is using the ACCESS_ACCEPT Access Type to allow full access.

Figure 180 Campus_Wireless_Full_Access



Endpoints connecting from a branch location dynamically get assigned to VLAN 10, which has been configured to provide full access.

Figure 181 Branch_Wireless_Full_Access



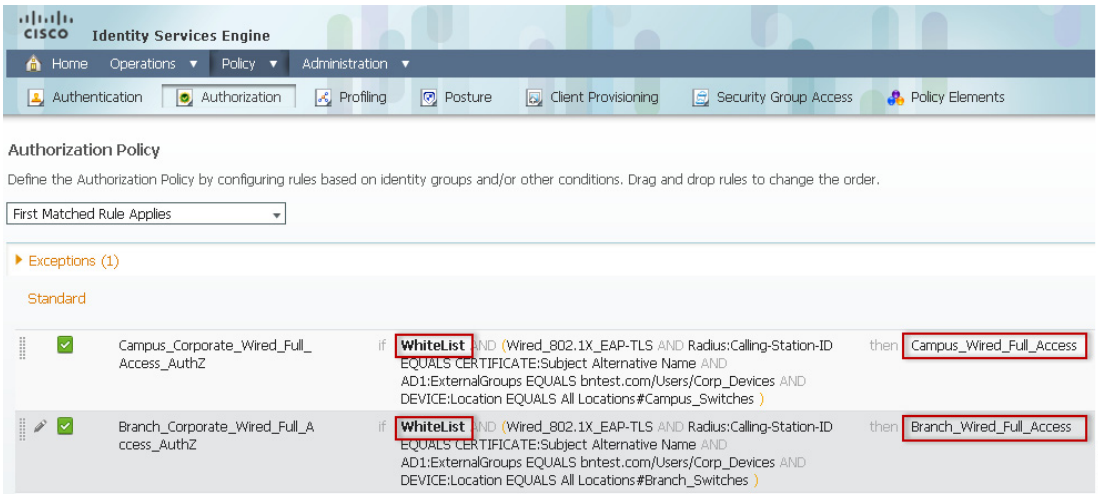
Authorization Profiles for Wired Users

The Authorization policy rules for wired devices follows the same logic as wireless devices. Corporate approved wired devices are assumed to be pre-configured with the correct configuration profiles and are also pre-enrolled with a digital certificate by the IT organization. When the device accesses the network, ISE verifies the following:

- The device has been provisioned by IT.
- The device has been added to the WhiteList identity group.
- The Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is member of the Corp_Devices Active Directory group.

Figure 182 shows the ISE policy rules for Corporate approved wired devices.

Figure 182 Authorization Policies for Wired Full Access



Looking at the common part of the two highlighted rules in more detail, it can be inferred that ISE evaluates these conditions:

- WhiteList—The endpoint has been added by an IT Administrator to the WhiteList identity group.
- Wired_802.X_EAP-TLS—A wired endpoint using EAP-TLS (defined as a compound condition).
- Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name—The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name.
- AD1:ExternalGroups EQUAL Corp_Devices—The user belongs to the Corp_Devices Active Directory group.

The condition that differs for connections initiated by branch or by campus is the device location group which is created under Network Devices. If a switch initiates a connection from the branch, then that switch is part of Branch_Switches and similarily, if a switch initiates the connection from a campus location, the switch is under the group Campus_Switches. Based on the last condition ISE enforces one of two authorization profiles:

- Campus_Wired_Full Access
- Branch_Wired_Full_Access

Authorization Profiles for Wired Users

When all conditions in the authorization policy rules match, the rule invokes the proper authorization profile:

- *Campus_Wired_Full_Access* for 802.1X wired devices.
- *Branch_Wired_Full_Access* for 802.1X wired devices.

Figure 183 shows the configuration details for the Campus_Wired_Full_Access authorization profile. For corporate approved devices a dACL permit_all_traffic is applied to the access layer switch.

Figure 183 Campus_Wired_Full_Access Authorization Profile

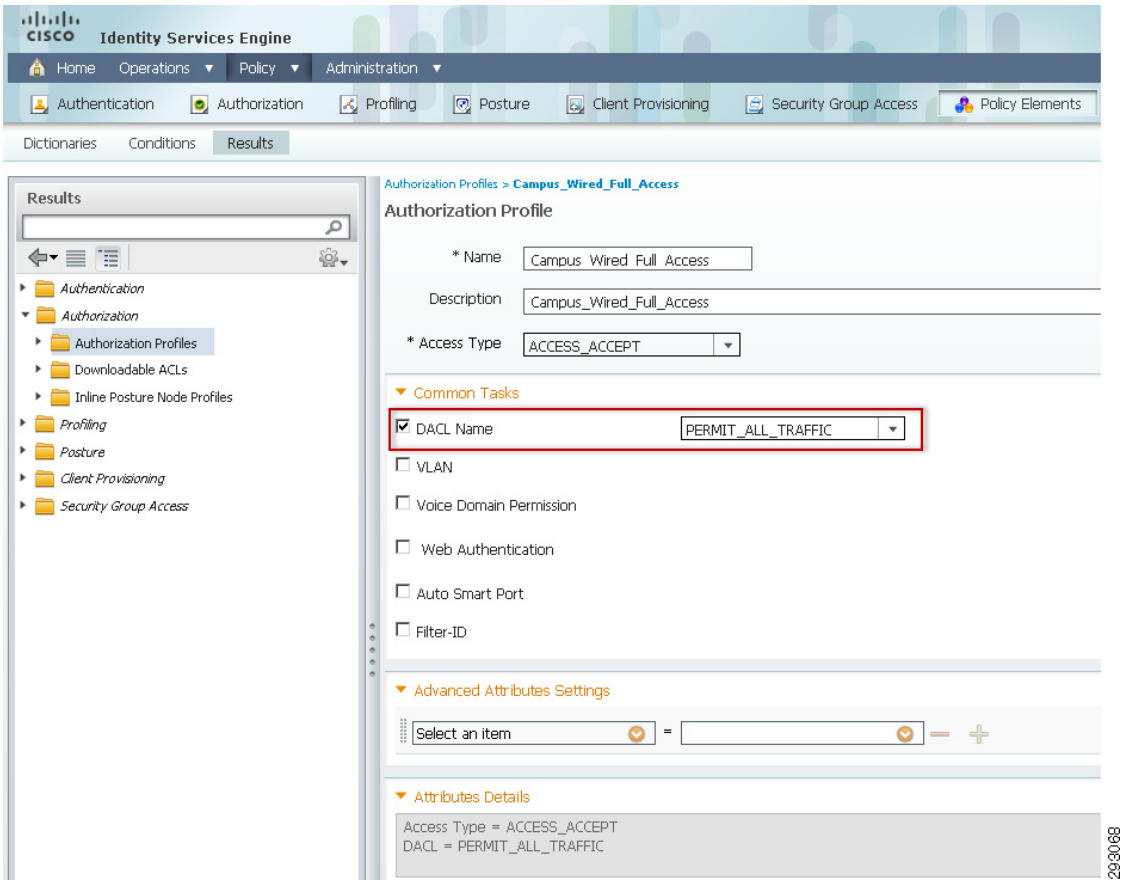
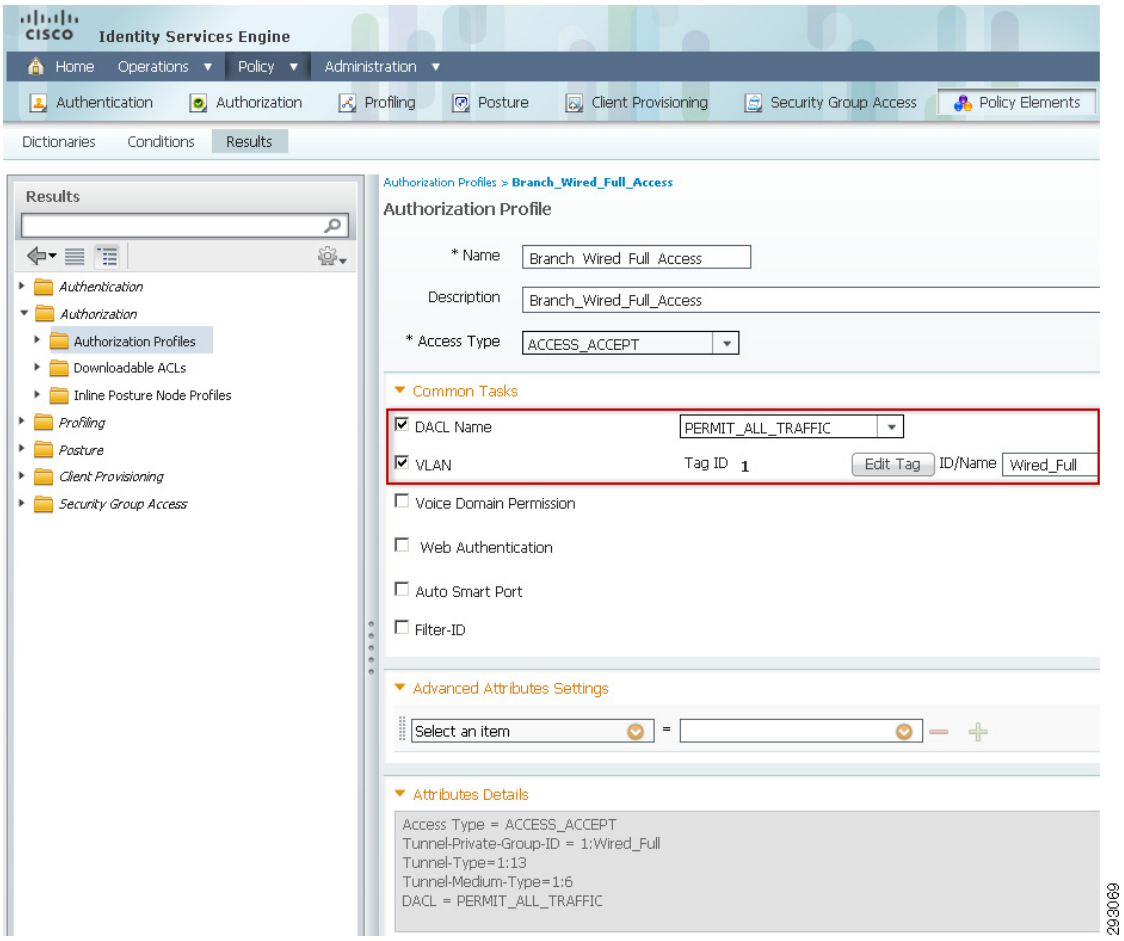


Figure 184 shows the Branch_Wired_Full_Access Authorization Profile for 802.1X wired devices. This authorization profile puts the users in a different VLAN, which is configured to grant full access.

For branch users, as mentioned in Enhanced BYOD Access, the strategy to provide differentiated access is to place the users in different VLANs.

Figure 184 Branch_Wired_Full_Access Authorization Profile



For reference purposes, the complete authorization policy used during testing is shown in Figure 185 and Figure 186.

Figure 185 Complete Authorization Policy (1 of 2)

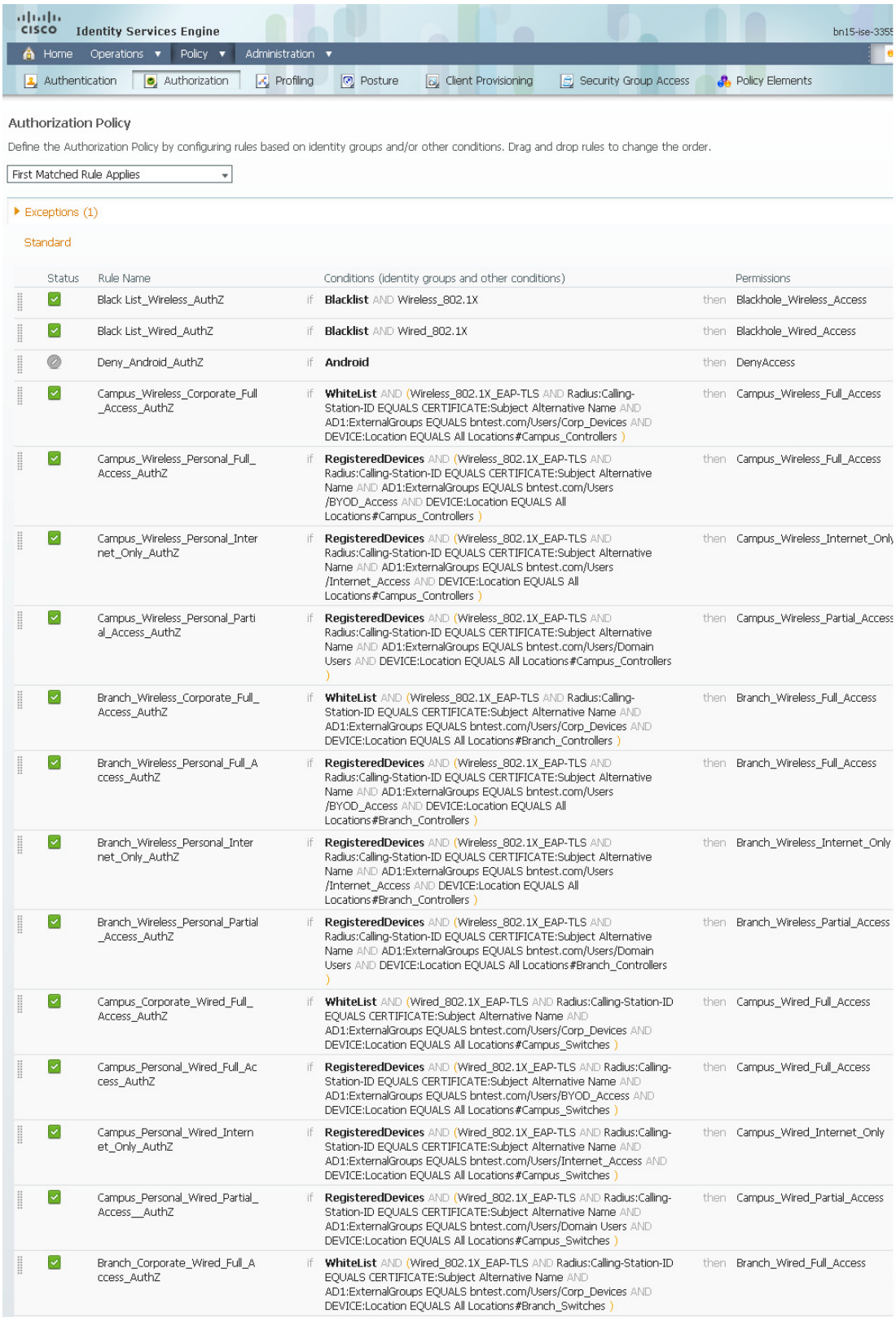


Figure 186 Complete Authorization Policy (2 of 2)

Campus_Corporate_Wired_Full_Access_AuthZ	if	**WhiteList** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Corp_Devices AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Full_Access
Campus_Personal_Wired_Full_Access_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/BYOD_Access AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Full_Access
Campus_Personal_Wired_Internet_Only_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Internet_Access AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Internet_Only
Campus_Personal_Wired_Partial_Access__AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Domain Users AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_Partial_Access
Branch_Corporate_Wired_Full_Access_AuthZ	if	**WhiteList** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Corp_Devices AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Full_Access
Branch_Personal_Wired_Full_Access_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/BYOD_Access AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Full_Access
Branch_Personal_Wired_Internet_Only_AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Internet_Access AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Internet_Only
Branch_Personal_Wired_Partial_Access__AuthZ	if	**RegisteredDevices** AND (Wired_802.1X_EAP-TLS AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name AND AD1:ExternalGroups EQUALS bntest.com/Users/Domain Users AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_Partial_Access
Wireless_Personal_Devices_Authz	if	(Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND Airespace:Airespace-Wlan-Id EQUALS 4)	then PermitAccess
Wireless PEAP SingleSSID Provisioning AuthZ	if	(Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND Airespace:Airespace-Wlan-Id EQUALS 1)	then Wireless_NSP
Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then Cisco_IP_Phones
Centralized_Wireless_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wireless_MAB AND Airespace:Airespace-Wlan-Id EQUALS 5 AND DEVICE:Location EQUALS All Locations#Campus_Controllers)	then Campus_Wireless_MAB
Branch_Wireless_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wireless_MAB AND DEVICE:Location EQUALS All Locations#Branch_Controllers)	then Branch_Wireless_MAB
Campus_Wired_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wired_MAB AND DEVICE:Location EQUALS All Locations#Campus_Switches)	then Campus_Wired_MAB
Branch_Wired_MAB_Devices_AuthZ	if	**MAB_DEVICES** AND (Wired_MAB AND DEVICE:Location EQUALS All Locations#Branch_Switches)	then Branch_Wired_MAB
Wireless_Guest_AuthZ	if	(WLC_Web_Authentication AND Airespace:Airespace-Wlan-Id EQUALS 2)	then PermitAccess
Wireless MAB AuthZ	if	Wireless_MAB	then Wireless_CWA
Wired MAB AuthZ	if	Wired_MAB	then Wired_CWA
Default	if no matches, then	DenyAccess	

293071

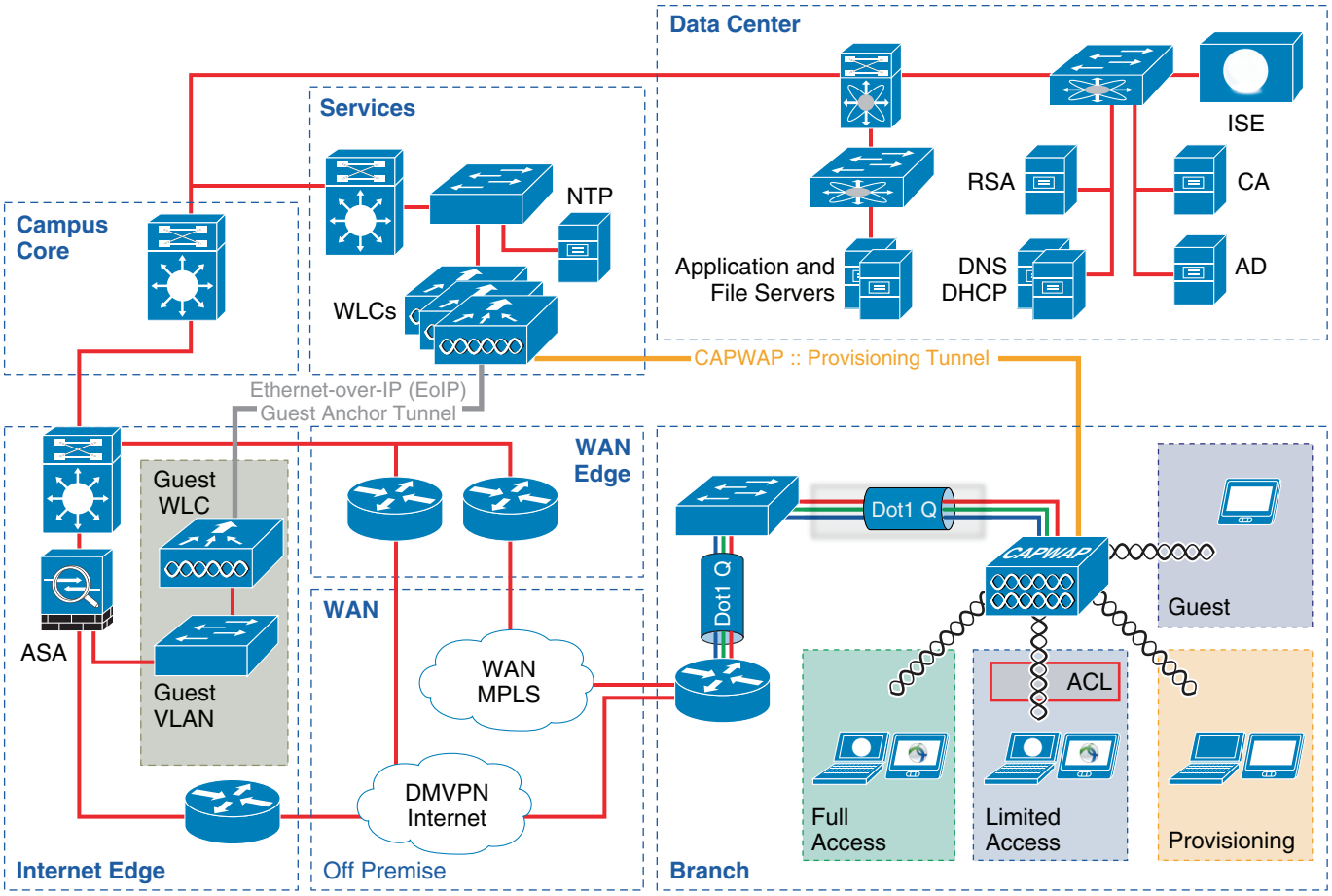
BYOD Guest Wireless Access

This section discusses traditional network access for wireless guest devices to present various options around how guest wireless devices can be accommodated within an overall BYOD implementation. It also provides background information for a later section which discusses how guest wireless access can be extended to support wireless employee personal devices. Note that within this design guide, guest access refers to temporary Internet access provided for visitors who are sponsored by a representative of the organization being visited.

Overview

For guest wireless access, a Cisco recommended best practice has been to deploy a separate, dedicated wireless controller off of a DMZ segment of a Cisco ASA firewall located within the Internet edge module. An example of this design is shown in Figure 187.

Figure 187 Typical Enterprise Guest Wireless Deployment



Multiple alternatives for deploying guest access may be deployed. However, this design guide discusses only guest wireless designs based around a dedicated guest SSID configured for open access with no encryption. This is often done because the organization's IT department usually has no knowledge of, or control over, the hardware or software capabilities of the guest wireless device. Hence, open access is the least common denominator applicable to all wireless devices.

Guest wireless traffic from the campus or a branch location is configured to be auto-anchored (tunneled via Ethernet-over-IP) from the internal wireless controllers located within either the services module (as shown in Figure 187) or the data center to the guest wireless controller. This may provide a somewhat higher level of security, in that guest wireless devices are not terminated on the "inside" of the corporate network. This is often desirable from a customer perspective because the security posture of guest devices cannot be determined.

This design guide section discusses wireless guest access primarily from the perspective of how it integrates with the network infrastructure and with the Cisco ISE server for AAA services within an overall BYOD deployment. For details regarding the configuration of wireless controllers for supporting

guest access, see the Cisco Unified Wireless Guest Access Services chapter of the Cisco Enterprise Mobility 4.1 Design Guide at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html.

IP Addressing and DNS

As with other devices, guest wireless devices require IP addresses and name resolution (DNS) services. A local DHCP server can be deployed on the subnet which supports guest wireless access. This option works well if the ASA firewall performs NAT between the inside and guest wireless DMZ interfaces. Although this may be the most secure option, in terms of isolating guest IP addressing from the rest of the corporate network, it is also somewhat cost prohibitive and more difficult to administratively maintain. This cost can be offset by implementing an ASA firewall configured with a DHCP pool to hand back IP addresses directly to wireless clients. The advantage of this option is again the isolation of guest IP addressing from the rest of the corporate network and the fact that DHCP from guest devices do not have to be allowed through the ASA firewall. The downside is the management of a separate IP addressing pool for guest wireless devices within the ASA firewall.

IP addressing for guest wireless devices can also be provided through a DHCP server on the inside of the corporate network. This option works well if NAT is not implemented between the inside and the guest wireless DMZ interfaces. The remainder of this section assumes no NAT functionality for the guest wireless DMZ interface. The advantage of implementing a centralized DHCP server is the centralized control of IP addressing for guest devices. The downside is that DHCP has to be allowed through the ASA firewall to the internal DHCP server.

Cisco wireless controllers can be configured to proxy for wireless clients to an internal DHCP server. This is a common deployment model for wireless controllers. With this configuration the DMZ interface of the ASA firewall needs to allow inbound DHCP packets from the IP address of the wireless controller associated with the guest WLAN interface through the ASA firewall. Alternatively, instead of the guest wireless controller proxying for wireless devices, the ASA firewall can be configured to relay DHCP to an internal DHCP server. With this configuration, guest wireless clients directly send DHCP through the wireless controller, which are then relayed to an internal DHCP server by the DMZ interface of the ASA firewall. Note that DHCP profiling of end devices via a Cisco ISE server can be accomplished by relaying the DHCP discover to both the internal DHCP server as well as the ISE profiling server. However, there may be no need or desire to profile guest devices, since they require only temporary access.

Note The network administrator should always weigh the benefits achieved from enabling DHCP server or DHCP relay functionality against the incremental risks of enabling such additional features on the ASA firewall to determine the appropriate security policy for the organization.

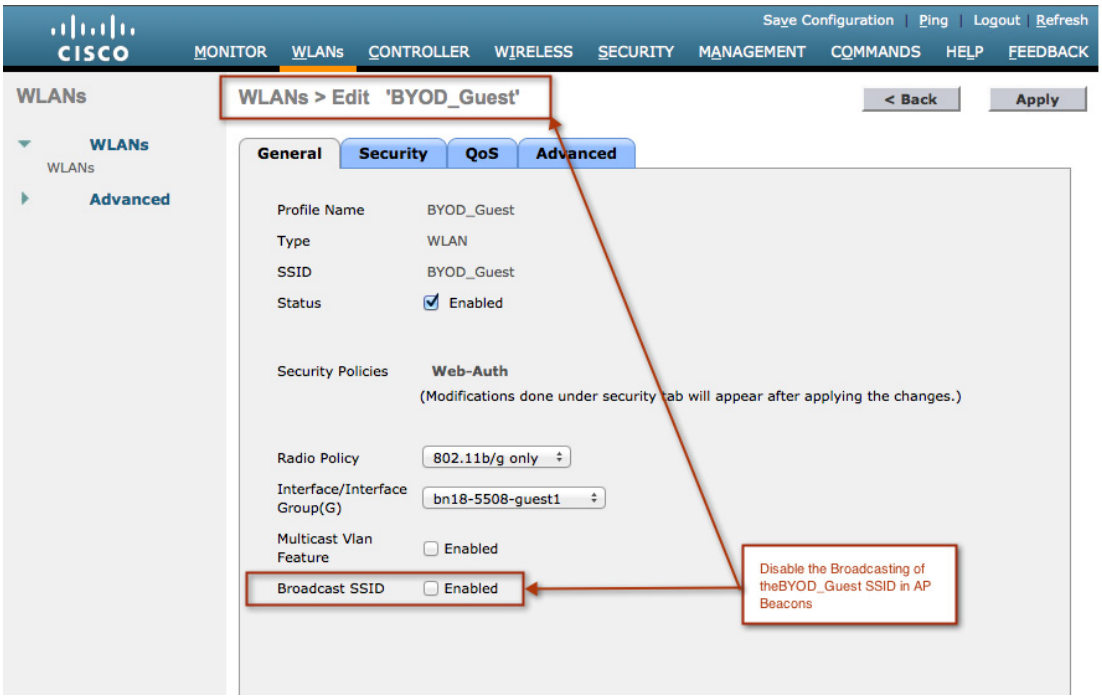
An increasing issue with guest wireless networks is IP address depletion. This may be the result of opening up the traditional guest network to employee personal devices. It may also be the unintentional result of having an office in a densely populated area where the general public is connecting to the open SSID corresponding to the organization's guest WLAN, thinking that it provides "hot spot" wireless services. As the proliferation of consumer wireless devices continues and as organizations continue to adopt BYOD strategies, this problem may become more widespread. If branch locations are offering guest services, the required address pool can become quite large.

There are a number of methods which can be implemented to help alleviate the issue of IP address depletion. From a security perspective, the optimal solution is to try to tune the Access Point (AP) radios such that the SSID corresponding to the guest WLAN—along any of the organization's other wireless SSIDs for that matter—are not visible outside the physical boundaries of the organization. However, this is not always possible while still maintaining adequate wireless coverage across the entire floor space.

A second method is to decrease the lease time on the DHCP server for the IP subnet corresponding to the guest WLAN. This does not prevent the general public from connecting to the open SSID corresponding to the organization's guest WLAN. However, when end users realize they do not have the Web Auth credentials needed to access anything, they may reconnect to another SSID. The IP addresses handed-out to these devices are made available to hand-out again more quickly if the DHCP lease time is decreased. The downside is the additional overhead on the DHCP server and slightly additional overhead on the wireless device itself from having to renew leases faster.

A third method is to hide the SSID corresponding to the guest WLAN by not broadcasting it in AP beacons. Cisco wireless controllers provide an easy means of achieving this by simply un-checking the Broadcast SSID checkbox for the WLAN corresponding to the guest SSID, as shown in Figure 188.

Figure 188 Disabling the Broadcast of the SSID Corresponding to the Guest WLAN in AP Beacons

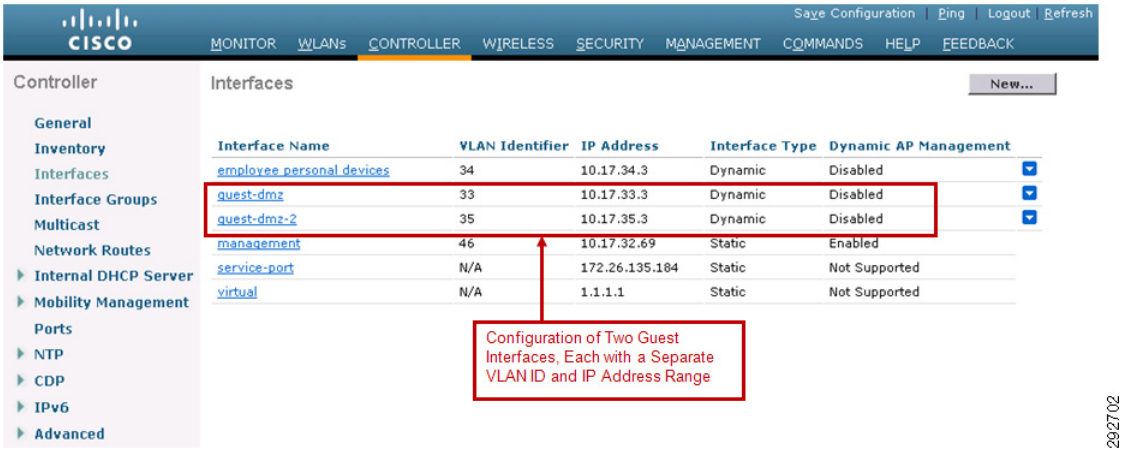


This is by no means a foolproof method of keeping unwanted devices from connecting to the open SSID corresponding to the guest WLAN, since it can still be discovered by other means. However, it does make it harder to find and connect to it, potentially reducing the number of unwanted devices and therefore the number of IP addresses being issued by the DHCP server. The downside is that guests have to manually type in the name of the SSID when trying to connect to the organization's guest wireless network. However, the name of the SSID can also be included with the credentials provided to the guest either prior to or at the time of arrival to organization's site.

Another option is to provision a larger contiguous IP subnet address space for the guest wireless network, simply by changing the IP subnet mask of the existing guest IP address space. This works well if the adjacent IP address space is available and unused. If this cannot be done, a second guest DMZ interface can be provisioned on the wireless controller to increase the IP address space available to hand

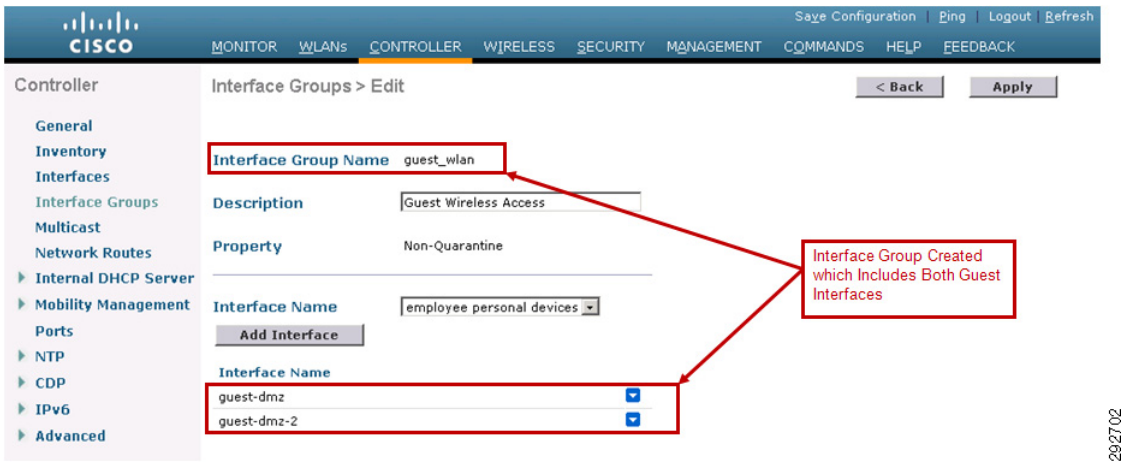
out to devices on the guest WLAN. An example is shown in Figure 189.

Figure 189 Example of the Configuration of a Second Guest DMZ Interface



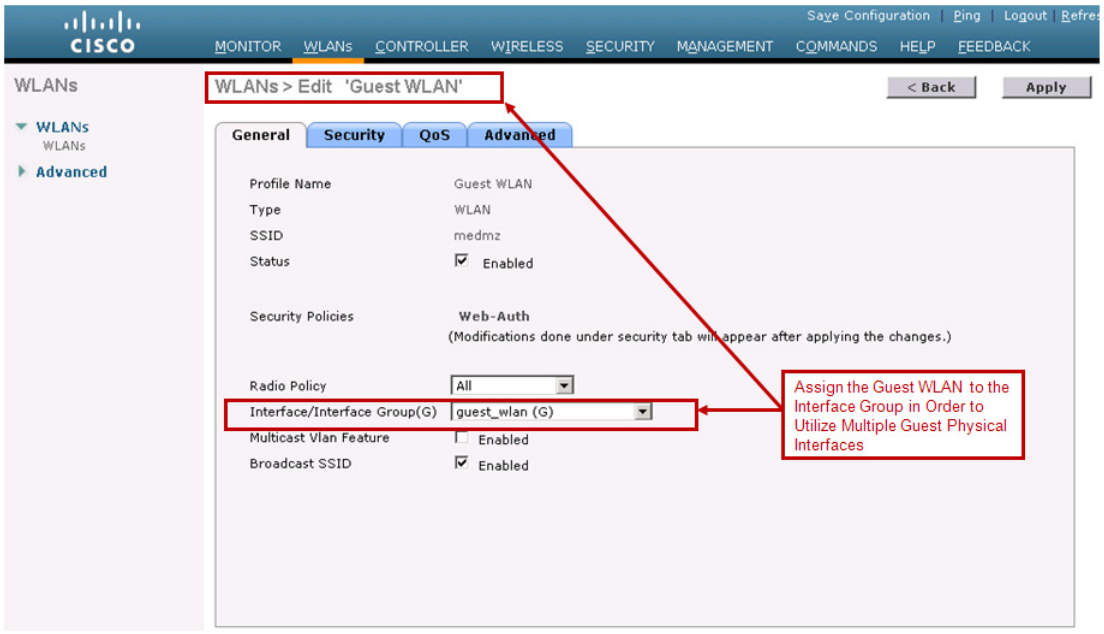
In this example, the first guest DMZ utilizes the IP subnet space of 10.17.33.0 / 24. The second guest DMZ utilizes the IP subnet space of 10.17.35.0 / 24. A new interface group can then be created on the wireless controller and the two guest DMZ interfaces added to the interface group. An example is shown in the figure belowFigure 190.

Figure 190 Example of an Interface Group which Includes Both Guest DMZ Interfaces



Finally the guest WLAN is configured to terminate wireless clients using the interface group, instead of an individual interface. An example of where this is configured is shown in Figure 191.

Figure 191 Configuring the Guest WLAN to Utilize an Interface Group Versus an Interface



Note Each individual DMZ interface may still experience IP address depletion resulting in the device not being able to establish connectivity to the guest WLAN. However, with two DMZ interfaces the total IP address space is increased.

Wireless guest devices also need name translation services (DNS) to reach locations on the Internet. Also, when web authentication (Web Auth) is implemented, the URL within the guest's Web browser must resolve to an IP address. This is necessary for Web Auth to redirect the session to the Guest Portal to request guest credentials. Name translation services can be provided by allowing guest devices to reach either an external DNS server deployed on another DMZ segment off the ASA firewall or an internal DNS server deployed on the inside of the corporate network. Allowing guest devices access to an external DNS server provides the advantage that internal sites and services can be hidden from the guest devices. However, if the wireless guest network is extended to include employee personal devices, as discussed in Authentication and Authorization, the network administrator needs to determine if an external DNS server can still provide the necessary name translation services.

Note DHCP packets from client to server utilize UDP source port 68 and destination port 67. DHCP packets from the server to the client utilize UDP source port 67 and destination port 68. DNS uses UDP port 53.

Increasing the pool of available addresses is the most direct method to ensure guests are not prevented access due to address depletion. It is worth noting that this approach does not discourage adjacent guests from associating to the wrong network. Web Auth or some other method is needed to control access to guest resources. It is also considered good practice to audit the actual number of guest users with the anticipated number. Comparing the number of guest that have passed through the Guest Portal with the number of addresses that are leased out from the DHCP server is a good means to determine how many unintentional guests are associating with the network. The lease time can be adjusted down if the number of leased addresses far exceeds the anticipated number of guests.

Authentication and Authorization

Most organization's IT departments choose to have guest wireless users authenticate first, before allowing access to the Internet. This step is sometimes accompanied with the guest user reading and agreeing to an Acceptable Use Policy (AUP) or End User Agreement (EUA) before accessing the Internet. Since the organization's IT department typically has no control over the hardware or software capabilities of guest wireless devices, the authentication and authorization decision is often based on a guest userid and password only. In other words, from a BYOD perspective, the device with which the guest is accessing the network may not be considered for the policy decision. A typical way of implementing guest user authentication is through the guest user's Web browser, known as Web authentication or Web Auth. With this method of authentication, the wireless guest must first open their Web browser to a URL located somewhere within the Internet. The browser session is re-directed to a Web portal which contains a login page which requests login credentials. Upon successful authentication, the guest user is either allowed access to the Internet or redirected to another Web site.

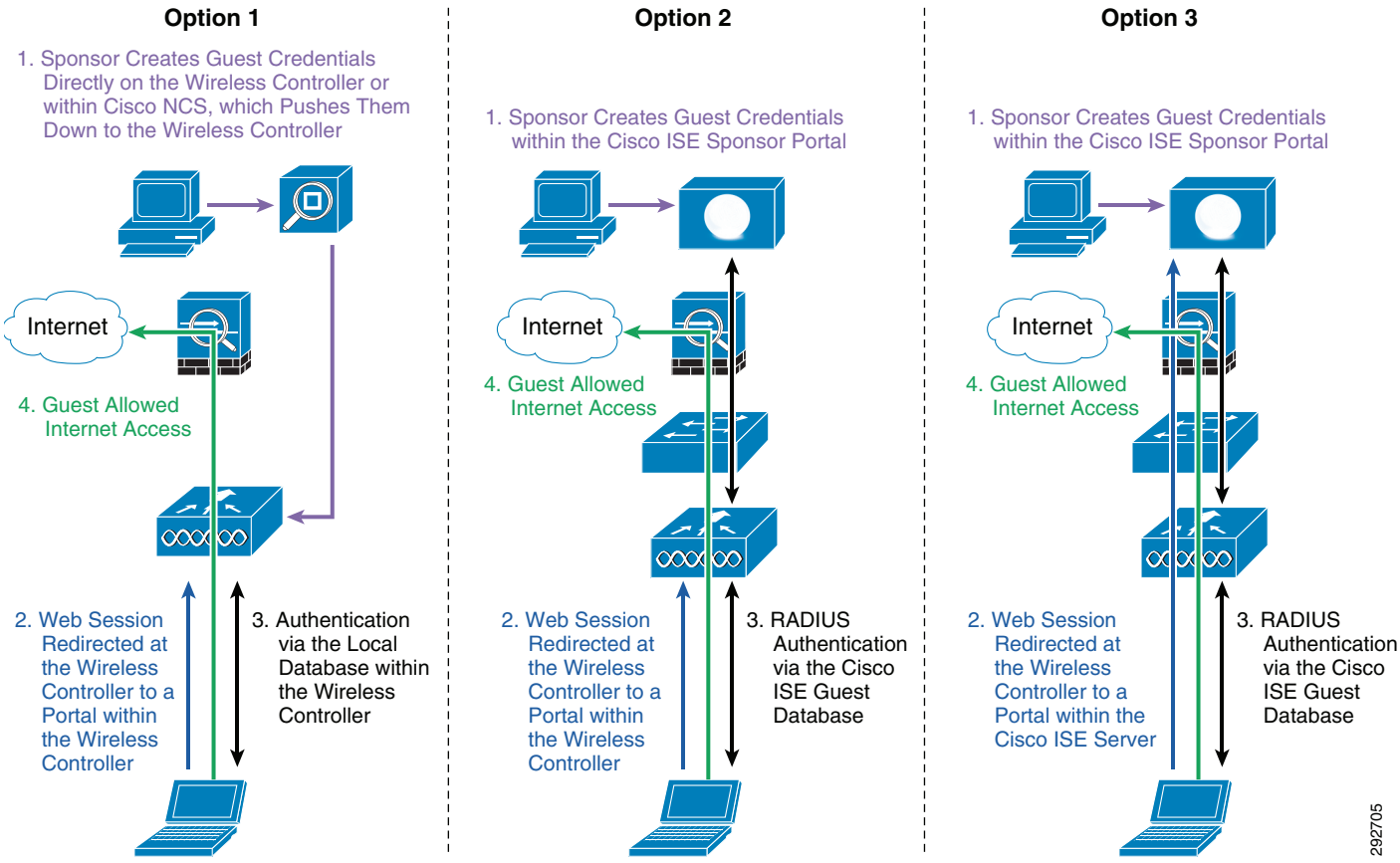
Note This authentication method is also known as "captive portal".

Cisco offers a comprehensive range of mechanisms for accomplishing Web Auth of guest wireless users designed to meet various customer requirements and deployment sizes. Figure 192 summarizes some of the available options based on the following:

- Which device performs the Web session redirection
- Which device provides the guest Web portal (i.e., the login page and optionally the AUP or EUA)
- Which device performs the actual guest authentication

A major requirement of guest access is the ability of a sponsor, such as a lobby administrator, to access a portal to create temporary guest credentials which are valid for a limited time. Hence, this functionality is also included within the discussion below.

Figure 192 Example Options for Guess Wireless Access with Web Authentication



Web Auth Option 1—Wireless Controller Web Portal with Wireless Controller Authentication and Sponsor Portal

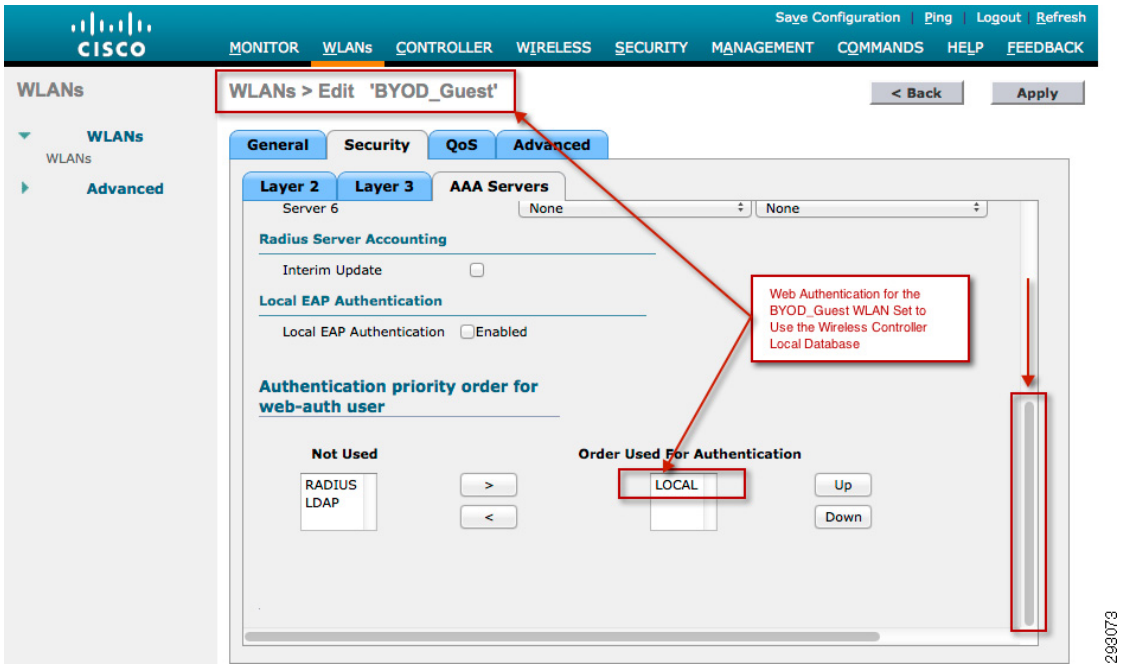
From the perspective of implementing the Limited Access and Enhanced Access BYOD designs discussed in previous sections, adding guest wireless access to those designs would not involve any modification to Cisco ISE policy, since ISE is not involved in providing guest access with this option. The web session of the guest device is redirected by the guest wireless controller to a Web portal containing the login screen within the guest wireless controller. The guest's credentials are then checked against the local database within the guest wireless controller. The advantage of this option is that the entire management of guest wireless access is confined to the guest wireless controller within the DMZ. The downside of this option is that guest credentials are maintained separately within the guest wireless controller.

Note This option is sometimes referred to as Local Web Auth (LWA).

Wireless Controller Configuration

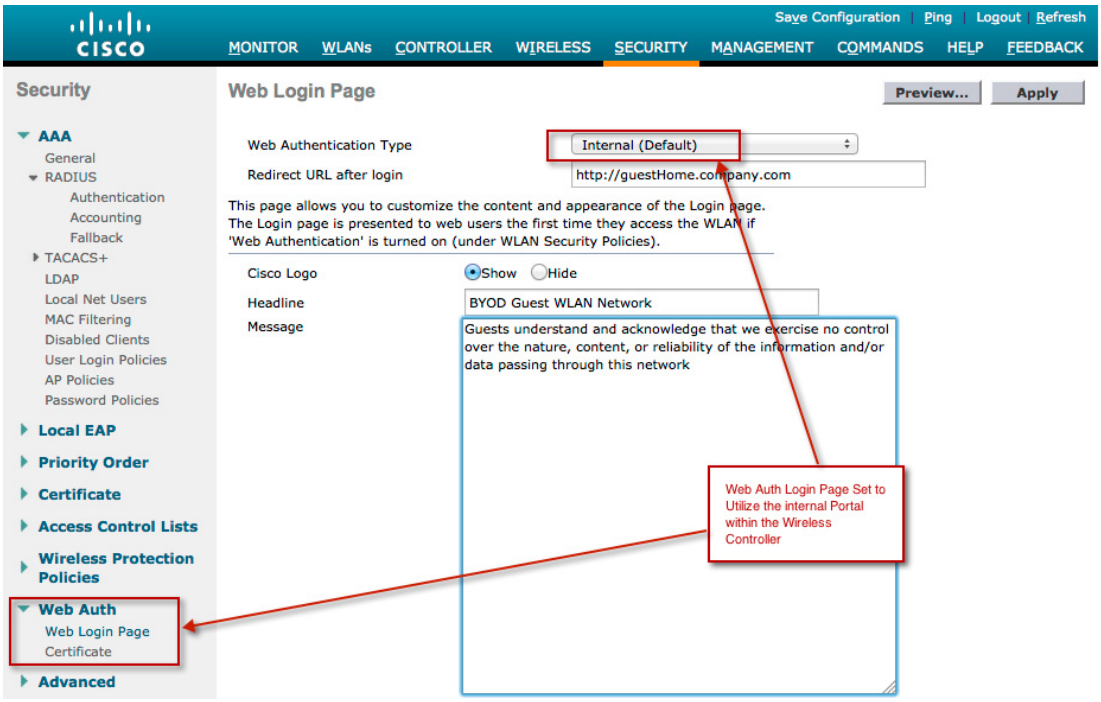
To implement this option, the network administrator must configure the guest WLAN to use the local database within the guest wireless controller for Web Auth. An example is shown in Figure 193.

Figure 193 Guest Web Authentication via Local Database



Additionally, the network administrator must configure Web Auth to utilize the internal Web login page within the guest wireless controller for the redirection portal, as shown in Figure 194.

Figure 194 Example Configuration for Wireless Controller Internal Guest Portal

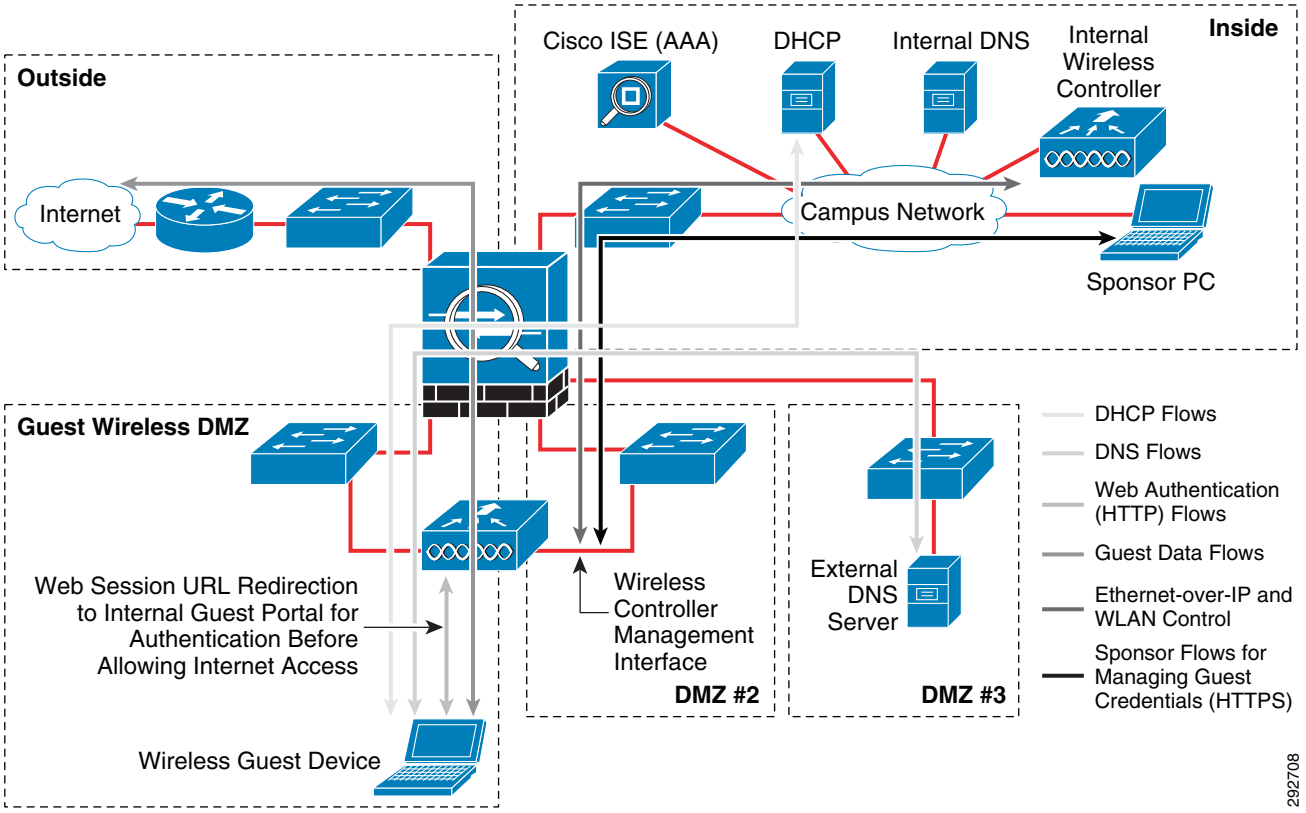


A pre-authentication ACL is not necessary when utilizing the local database for authentication and the local guest Web portal for login. DHCP and DNS related packets are automatically passed by the wireless controller when Web Auth is configured. Note that no pre-authentication ACL means that all other traffic is blocked prior to a successful Web authentication.

ASA Firewall Configuration

Figure 195 shows an example of the flows that need to pass through the Cisco ASA firewall to support this option.

Figure 195 Example of Flows that Need to Pass Through the Cisco ASA Firewall for Option 1

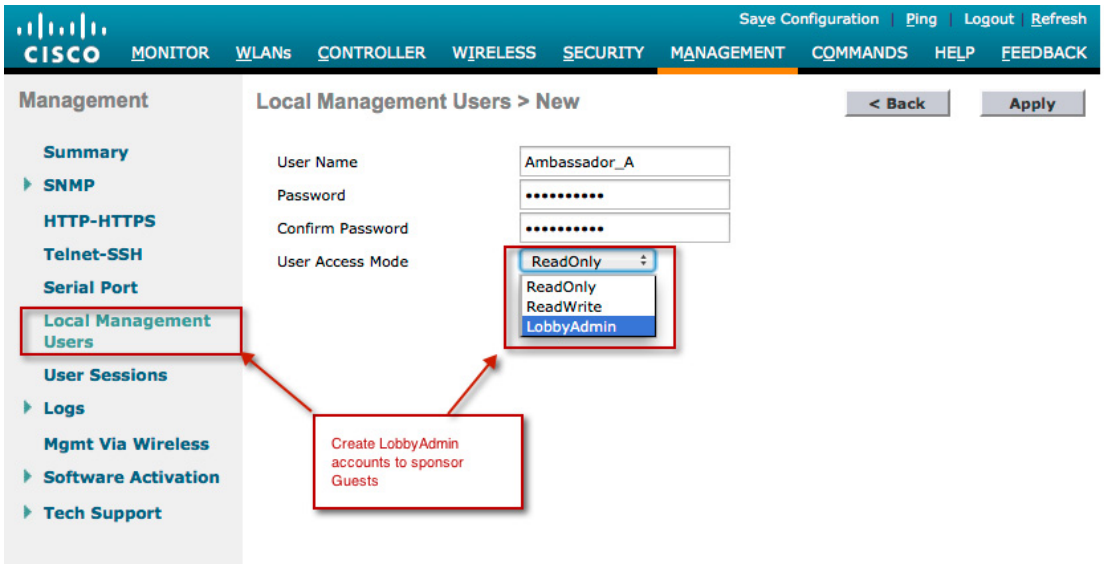


Besides allowing inbound DNS and DHCP (assuming the deployment of an internal DHCP server), the ASA firewall should be configured to block all other traffic generated from guest wireless devices onto the internal network. Note that the ASA firewall configuration may also need to allow HTTPS connections initiated from sponsors on the inside of the network to the wireless guest management interface (or the service port interface for those platforms which support it and if out-of-band management is provisioned) to configure guest credentials. An Ethernet-over-IP (IP protocol 97) auto-anchor mobility tunnel, as well as the WLAN control port (UDP port 1666) between the management interfaces of the two wireless controllers, must be allowed through the ASA firewall. Note that the wireless controller management interface should be on a separate subnet from the actual guest wireless devices—either on another DMZ interface of the ASA firewall or on the inside of the firewall.

Cisco Wireless Controller Sponsor Portal

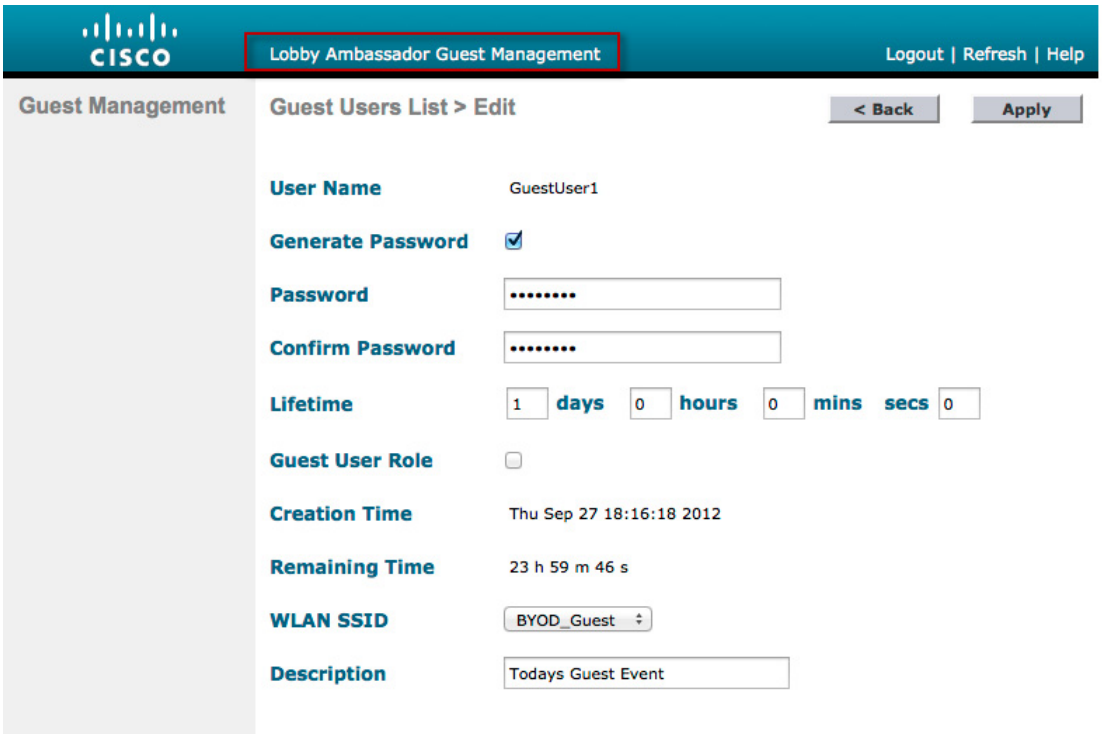
Cisco wireless controllers provide a basic sponsor portal functionality for creating and managing guest credentials. The wireless controller has three administrative access levels controlled via the local database—ReadWrite, ReadOnly, and LobbyAdmin. The LobbyAdmin access level allows a sponsor to access a Web portal function on the wireless controller for adding guest users. An example of creating a LobbyAdmin user is show in Figure 196.

Figure 196 Example of Creating a Lobby Admin Account



Once a user account is created for the sponsor portal, that account can be used on the wireless controller to reach the sponsor portal Web page. This page is used for adding guests within the wireless controller and is shown in Figure 197.

Figure 197 Example of the Wireless Controller Sponsor Portal for Adding Guests



Access can be granted for any WLAN or restricted to a single WLAN which is mapped to the BYOD_Guest SSID (as shown in Figure 197). The lifetime of the guest access can be specified, however the credentials are active immediately upon configuration. Guest credentials cannot be configured to become active at a future date. The wireless controller also has no capability to deliver the guest credentials to the actual guest prior to arrival via mechanisms such as E-mail, SMS, etc.

Multiple sponsors, each with LobbyAdmin access, can be configured within the guest wireless controller to support multiple departments or multiple lobby administrators needing to provide wireless guest access. However, any sponsor with LobbyAdmin access can view, edit, and remove credentials for any guest configured on the wireless controller. If multiple wireless controllers are deployed within the DMZ for guest access, the guest credentials may need to be manually duplicated across each of these by the sponsor.

Note Even though guest credentials are created on the wireless controller, the authentication of the sponsor can be shifted from a local account with LobbyAdmin access privileges to a Microsoft AD account accessed via a RADIUS server with the equivalent of LobbyAdmin access privileges. This is done by passing the RADIUS dictionary attribute-value (AV) pair: "Service-Type -- [6] EQUALS Callback Administrative" when authenticating the sponsor.

Cisco Prime Infrastructure Sponsor Portal

The Cisco Prime Infrastructure server also provides a very basic sponsor portal functionality for creating and managing guest credentials. The advantage is that sponsors do not have to access individual guest wireless controllers to provision guest credentials. Instead they only need access to the internal Cisco Prime server sponsor portal. The Cisco Prime server pushes guest credentials out to one or more guest wireless controllers via templates, eliminating the need for the sponsor to duplicate guest credentials across multiple wireless controllers. Note that guest credentials still reside on the guest wireless

controller local database when pushed down via Cisco Prime Infrastructure. The server has the capability to deliver the guest credentials to the actual guest prior to arrival via mechanisms such as E-mail, SMS, etc.

Web Auth Option 2—Wireless Controller Web Portal with Cisco ISE Authentication and Sponsor Portal

Option 2 moves the authentication of wireless guests (i.e., the guest credentials) from the local database on the guest wireless controller to a centralized AAA server, such as Cisco's Identity Services Engine (ISE). The Web session of the guest is still redirected by the guest wireless controller to an internal portal containing the login screen. However, the guest credentials are checked against an identity user group within the Cisco ISE server.

An advantage of this design is the centralization of guest credentials and the point of authentication and authorization. This provides the following benefits:

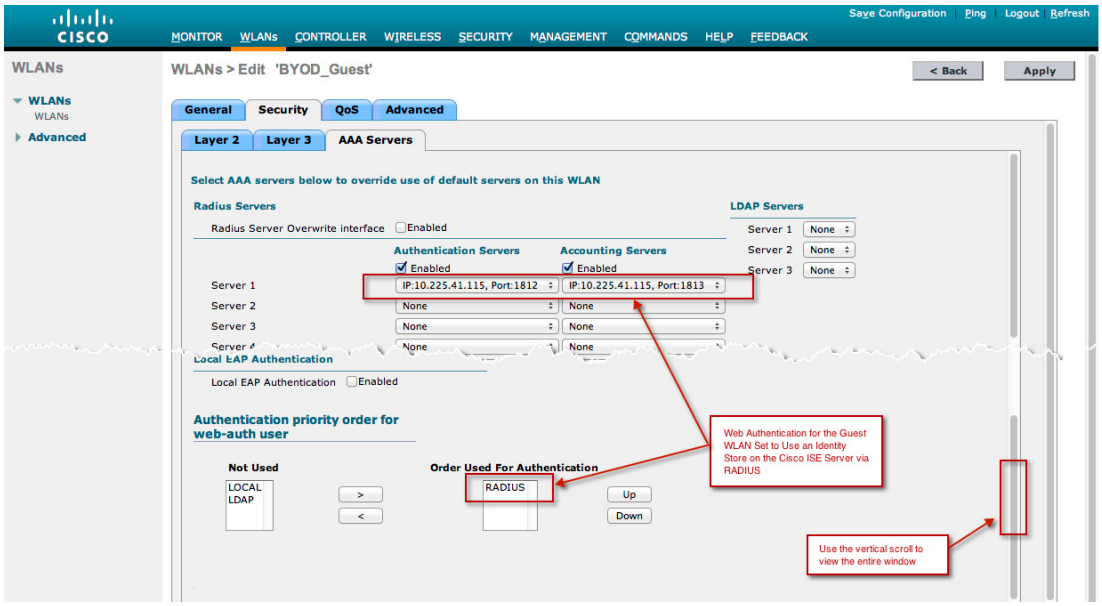
- Authentication logs can be audited and monitored for suspicious behavior, which could indicate attempts to gain unauthorized access to the Internet from the guest WLAN.
- Sponsors can be authenticated and authorized based on their user group credentials within a directory services server, such as Microsoft's Active Directory.
- Sponsor access can be better limited, preventing employees from configuring guest credentials for themselves and utilizing the guest network for employee personal devices if the business policy of the organization does not wish to allow this.
- Authentication logs can also be used to audit access to the Cisco ISE sponsor portal.

A disadvantage of this design is that a separate Web login portal is still maintained on each guest wireless controller. However, the administrative overhead of maintaining it may be relatively low if it does not change often.

Wireless Controller Configuration

To implement this option, the network administrator must configure the guest WLAN to use RADIUS within the guest wireless controller for authentication, as shown in Figure 198.

Figure 198 Guest Web Authentication via RADIUS

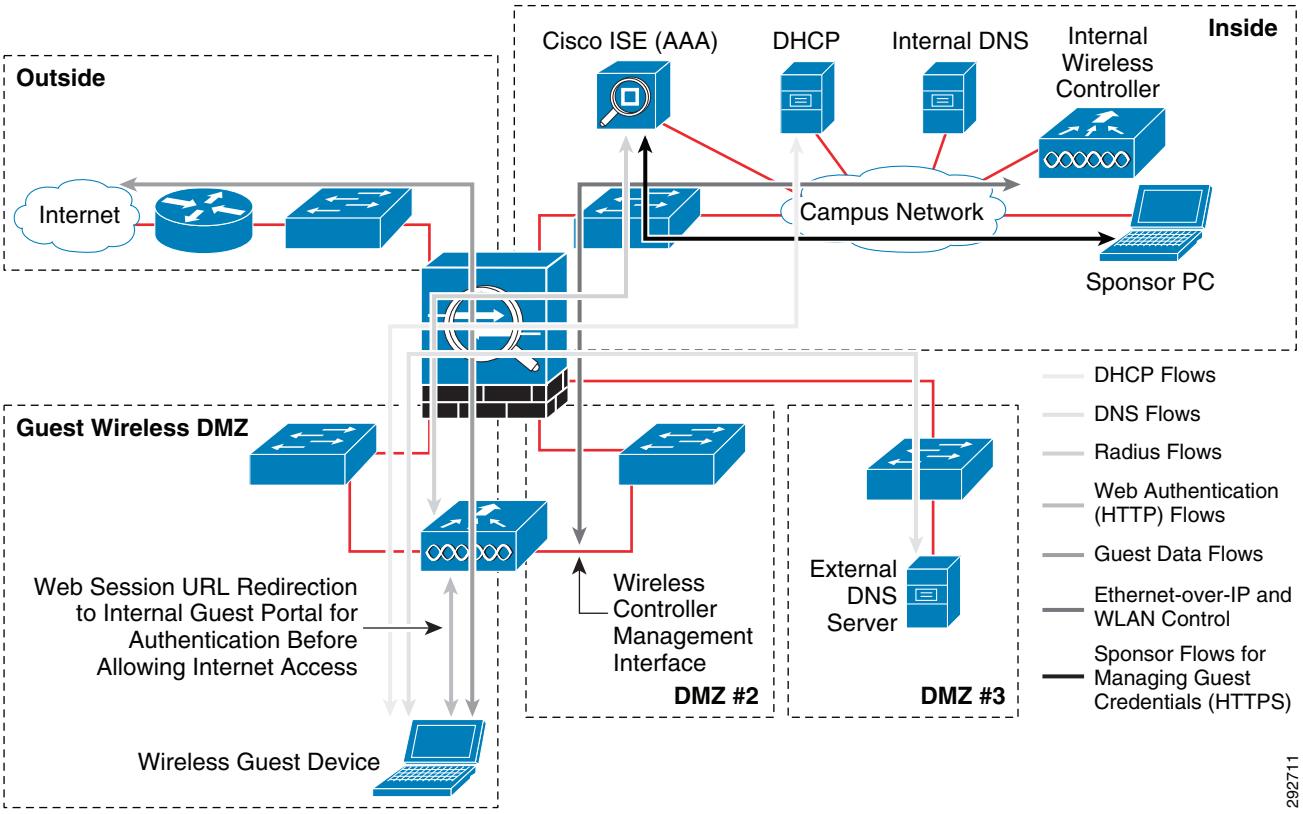


The network administrator must still configure Web Auth to utilize the internal Web login page within the guest wireless controller for the redirection portal, as shown in Figure 194. A pre-authentication ACL is again not necessary when utilizing Cisco ISE for remote authentication along with the local Web portal. Since the RADIUS session is initiated by the wireless controller itself, it is not affected by the pre-authentication ACL.

ASA Firewall Configuration

Figure 199 shows an example of the flows that need to pass through the Cisco ASA firewall to support this option.

Figure 199 Example of Flows that Need to Pass Through the Cisco ASA Firewall for Option 2



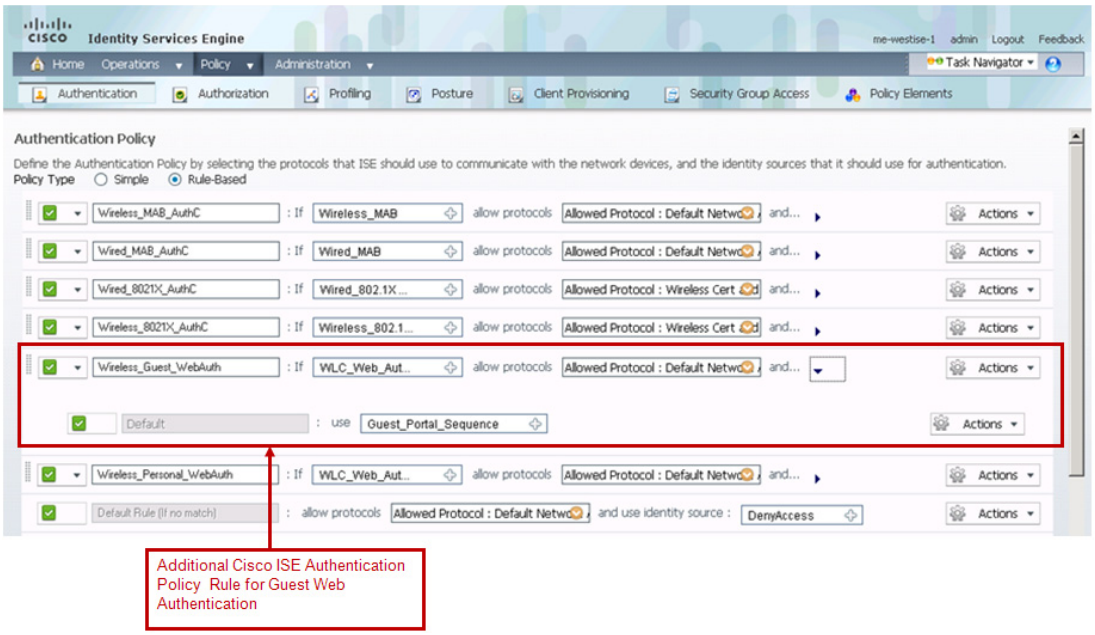
This option requires a RADIUS session to be allowed through the ASA firewall between the guest wireless controller management interface and the Cisco ISE server. An Ethernet-over-IP (IP protocol 97) auto-anchor mobility tunnel, as well as the WLAN control port (UDP port 1666) between the management interfaces of the two wireless controllers, must still be allowed through the ASA firewall. Besides allowing inbound DNS and DHCP (assuming the deployment of an internal DHCP server), the ASA firewall should be configured to block all other traffic generated from guest wireless devices onto the internal network.

Note The guest wireless controller uses the IP address of the management interface as the source for the Web Auth RADIUS session.

Cisco ISE Policy Configuration

From a Cisco ISE policy perspective, an additional authentication rule needs to be added to the Limited Access Use Case design policies. This rule allows wireless controller Web authentications, originated from the SSID corresponding to the guest WLAN, to utilize a separate Cisco ISE user identity sequence for wireless guest access. An example of such a policy rule is shown in Figure 200.

Figure 200 Example of Cisco ISE Authentication Policy Allowing Guest Wireless Access



The logical format of the example authentication policy rule is as follows:

```
IF (WLC_Web_Authentication AND Wireless_Guest_WebAuth)
    THEN (Allow Default Network Access AND USE Guest_Portal_Sequence)
```

WLC_Web_Authentication is a system-generated compound condition which is used here to match Web authentication requests from Cisco Wireless LAN Controllers. It matches the following two standard RADIUS dictionary attribute-value (AV) pairs:

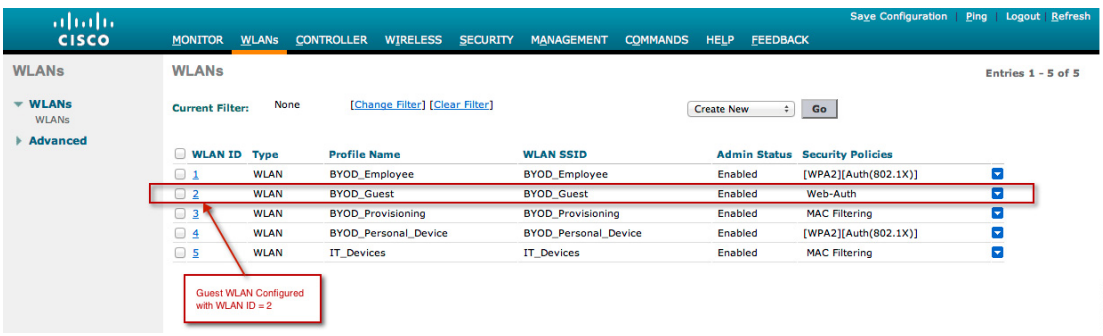
```
Service-Type - [6] EQUALS Login
NAS-Port-Type - [61] EQUALS Wireless - IEEE 802.11
```

Wireless_Guest_WebAuth is a user-defined simple authentication condition for guests accessing the Internet via Web Auth through the open guest SSID. It matches the following RADIUS AV pair from the Airespace dictionary:

```
Airespace-Wlan-Id - [1] EQUALS 1
```

The Airespace-Wlan-Id is the identification number (WLAN ID) of the WLAN corresponding to the Guest SSID for this example, as shown in Figure 201.

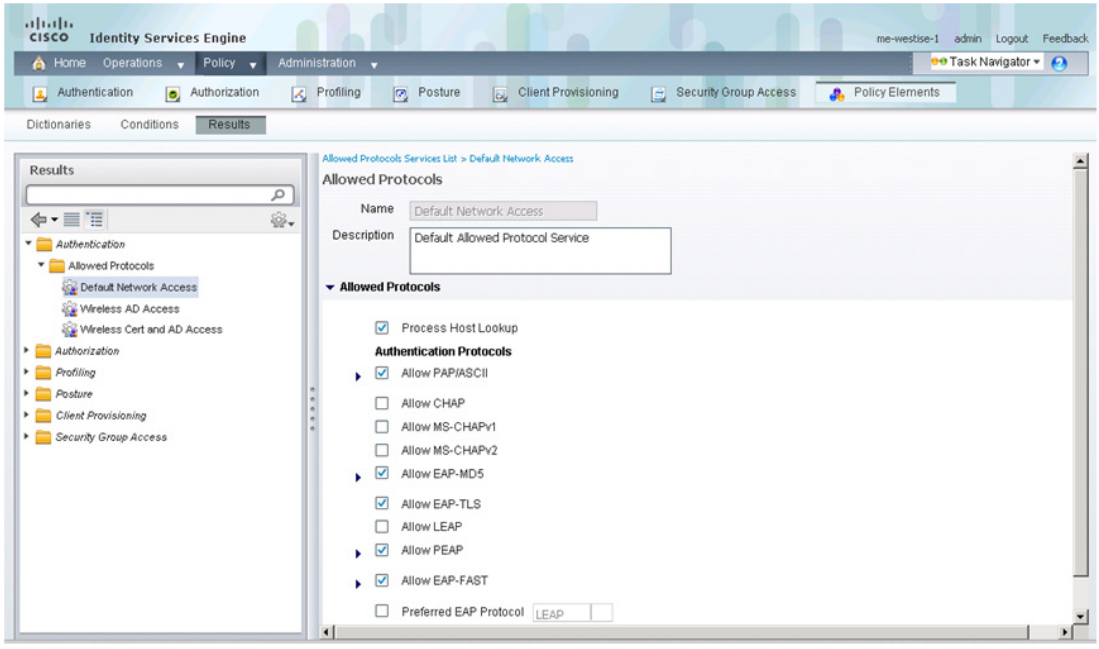
Figure 201 Example Guest Wireless Controller WLAN IDs



The inclusion of the WLAN ID within the authentication policy rule allows the Cisco ISE authentication policy to differentiate Web Auth requests coming from the SSID corresponding to the guest WLAN and apply a different outcome.

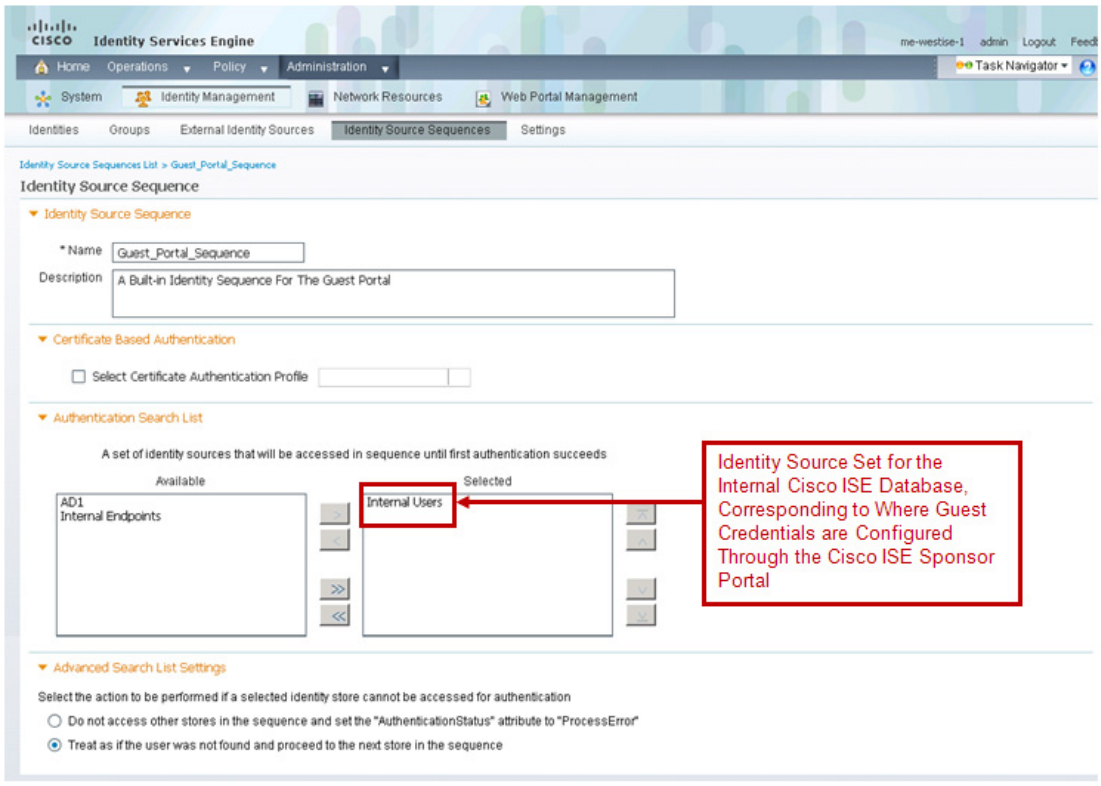
Default Network Access is a system-generated authentication result, which allows various protocols to be used for the Web Auth. An example is shown in Figure 202.

Figure 202 Example of Allowed Protocols Under Default Network Access



Guest_Portal_Access is a user-defined identity source sequence. An example is shown in Figure 203.

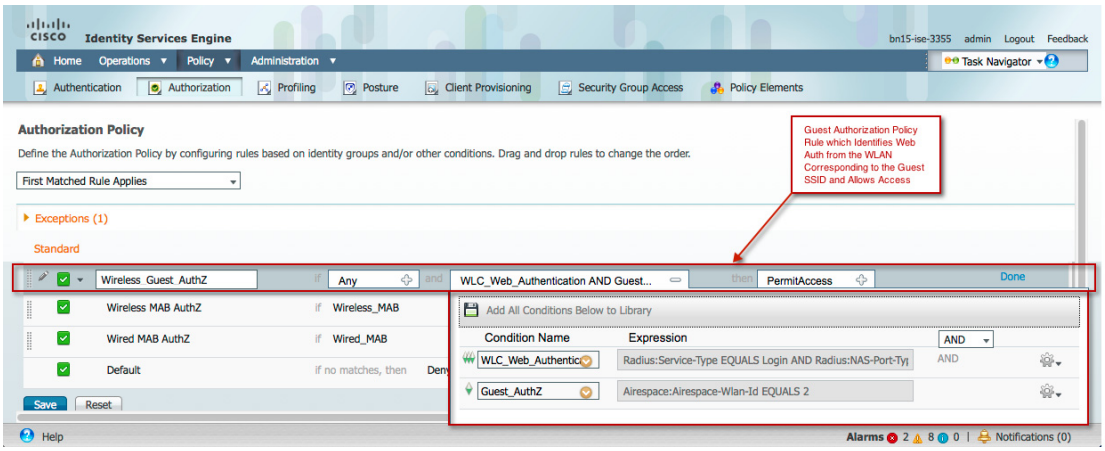
Figure 203 Example of Guest_Portal_Access Identity Source Sequence



The Guest_Portal_Sequence in the example above uses the Internal Users identity source only. This corresponds to where guest credentials are held when they are configured through the Cisco ISE sponsor portal, which is discussed later in this section. Although an identity source sequence is not strictly needed when only a single identity source is specified, configuring a sequence allows guest wireless access to be easily extended to include employee personal devices by adding an additional identity source. This is discussed in Web Auth Option 3—Cisco ISE Web Portal with Cisco ISE Authentication and Sponsor Portal.

From a Cisco ISE policy perspective, an additional authorization rule also needs to be added to the Limited Access Use Case design policies. This rule permits access for wireless controller Web authentications originated from the SSID corresponding to the guest WLAN. An example of the policy rule is shown in Figure 204.

Figure 204 Example of Cisco ISE Authorization Policy Allowing Guest Wireless Access



The logical format of the example authorization policy rule is:

```
IF (WLC_Web_Authentication AND Guest_AuthZ)
    THEN Permit Access
```

WLC_Web_Authentication was discussed with regard to the authentication policy above.

Guest_Authz is a user-defined simple authorization condition for guests accessing the Internet via Web authentication through the WLAN corresponding to the open guest SSID. It matches the following RADIUS AV pair from the Airespace dictionary:

```
Airespace-Wlan-Id - [1] EQUALS 2
```

The Airespace-Wlan-Id is again the identification number (WLAN ID) of the WLAN corresponding to the Guest SSID. This allows the ISE authorization policy to differentiate Web Auth requests coming from the guest WLAN and permit them.

Note Simple Conditions such as Guest_Authz are optionally used to give attribute and value pairs a descriptive name. This allows the policy to be more readable and easier to support.

Web Auth Option 3—Cisco ISE Web Portal with Cisco ISE Authentication and Sponsor Portal

Option 3 moves both the redirection of the guest Web session and the point of authentication from the wireless controller to the Cisco ISE server. The guest Web session is redirected by the guest wireless controller to a portal containing the login screen located within the Cisco ISE server.

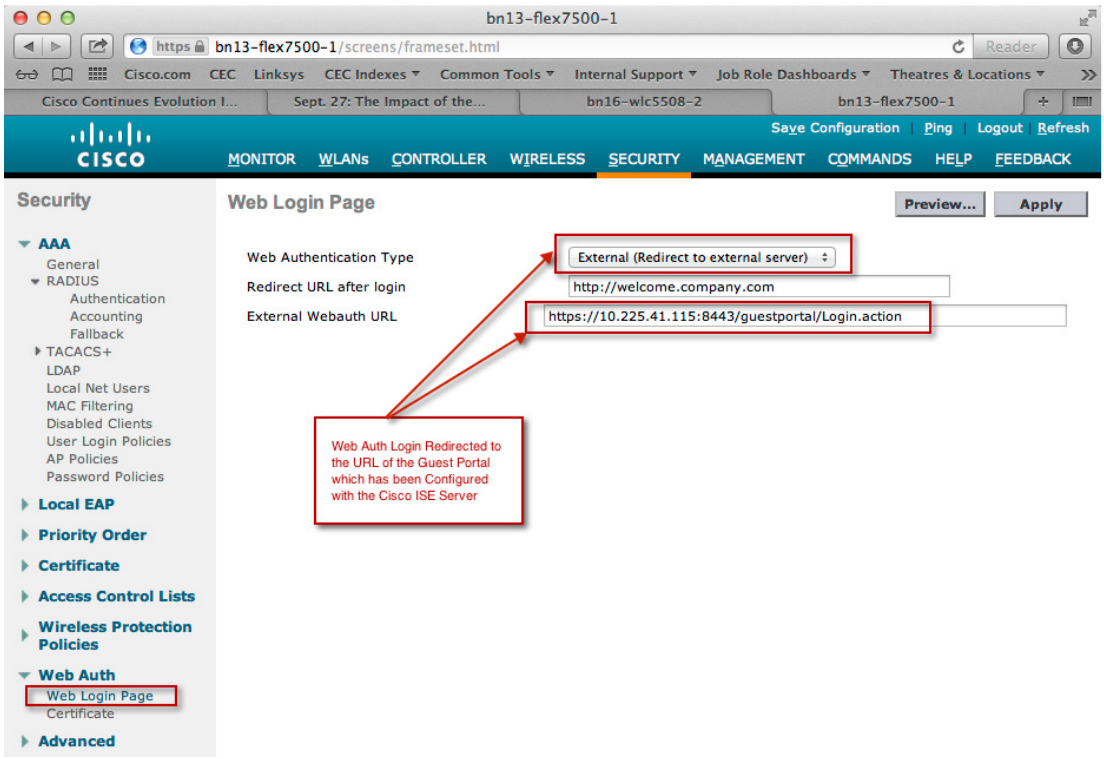
Note This option is sometimes referred to as Central Web Auth (CWA).

By positioning the Web Auth login page (and optionally the AUP or EUA) in a central location, the network administrator can provide one unified login page for all wireless guest access without having to download the login page to each guest wireless controller.

Wireless Controller Configuration

To implement this option, the network administrator must configure Web Auth within the guest wireless controller to utilize a remote server for the redirection portal, as shown in Figure 205.

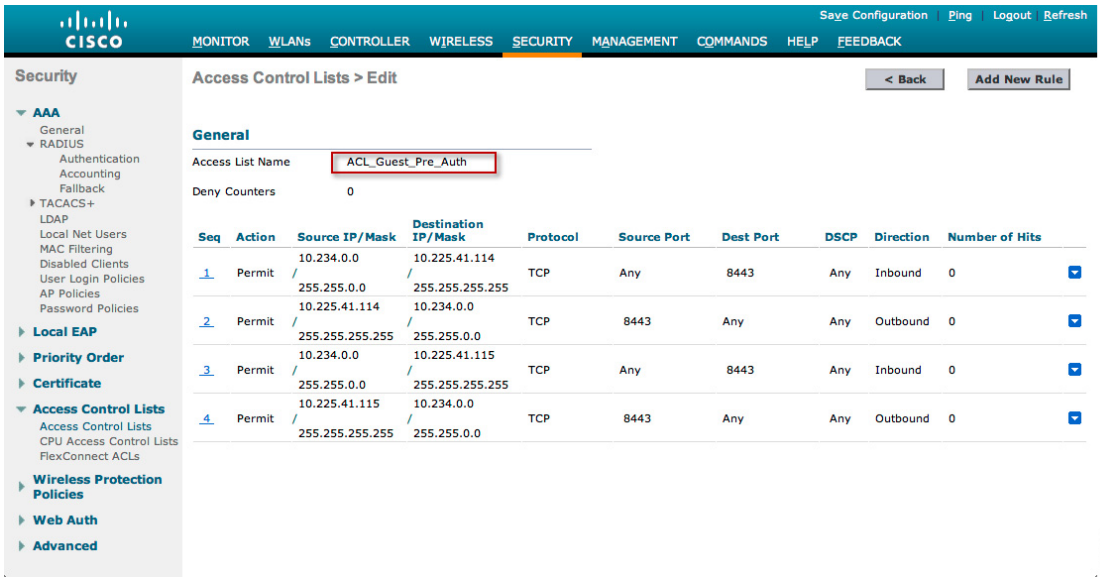
Figure 205 Example Configuration for Wireless Controller External Guest Portal



The Cisco ISE server has the capability to host multiple guest portals. Hence, from a Cisco ISE deployment and policy perspective, one guest portal can be used for on-boarding corporate owned devices and employee personal devices, as discussed in the previous sections which covered the Limited Access and Enhanced Access BYOD designs. A second Cisco ISE guest portal can be configured for guest wireless access, which is discussed in Cisco ISE Sponsor Portal.

A Web Auth pre-authentication ACL is necessary when utilizing a remote Cisco ISE guest portal for login and optionally the AUP or EUA. The Web Auth pre-authentication ACL must allow all possible IP addresses associated with the guest wireless subnet (which can be handed out to guest wireless devices) to be redirected to TCP port 8443 of the Cisco ISE guest portal. An example of a Web Auth pre-authentication ACL is shown in Figure 206.

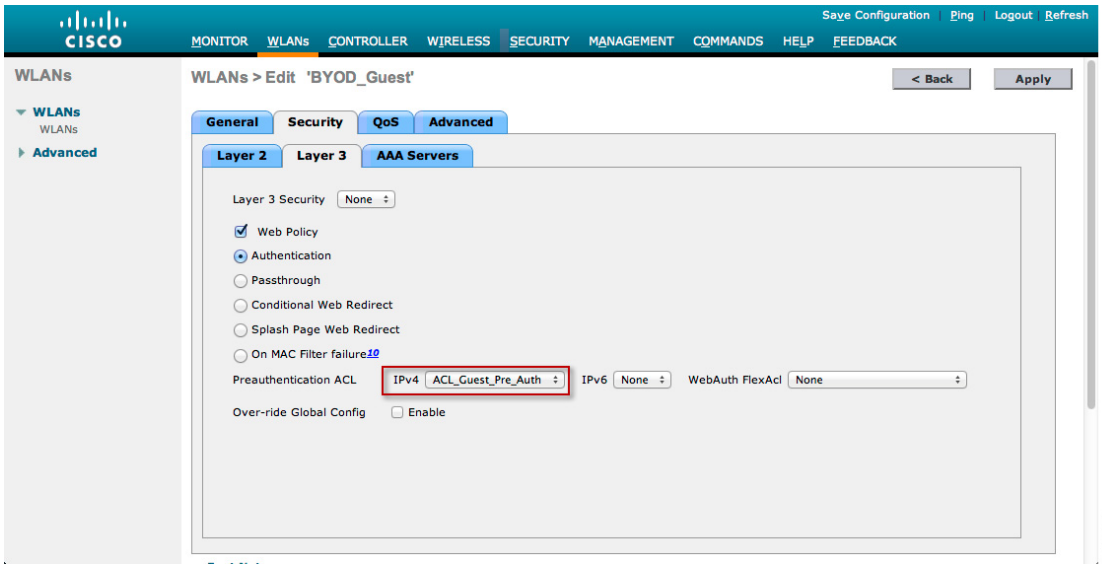
Figure 206 Example of a Pre-Authentication ACL for Guest Wireless Access via Web Auth



When specifying an ACL down to the port level within the guest wireless controller, both inbound (from the wireless guest devices to the Cisco ISE server) and outbound (from the Cisco ISE server to the wireless guest devices) rules must be configured. Specifying an inbound rule only does not automatically allow return traffic through the wireless controller, as is done with a stateful firewall. Likewise, specifying a single rule of the form above, with a direction of "Any", also does not work. The wireless controller does not reverse the source and destination IP addresses for the return traffic.

Once the ACL is configured, it must be applied as a Web Auth pre-authentication. This is done in the Guest WLAN Layer 3 Security policy, as shown in Figure 207.

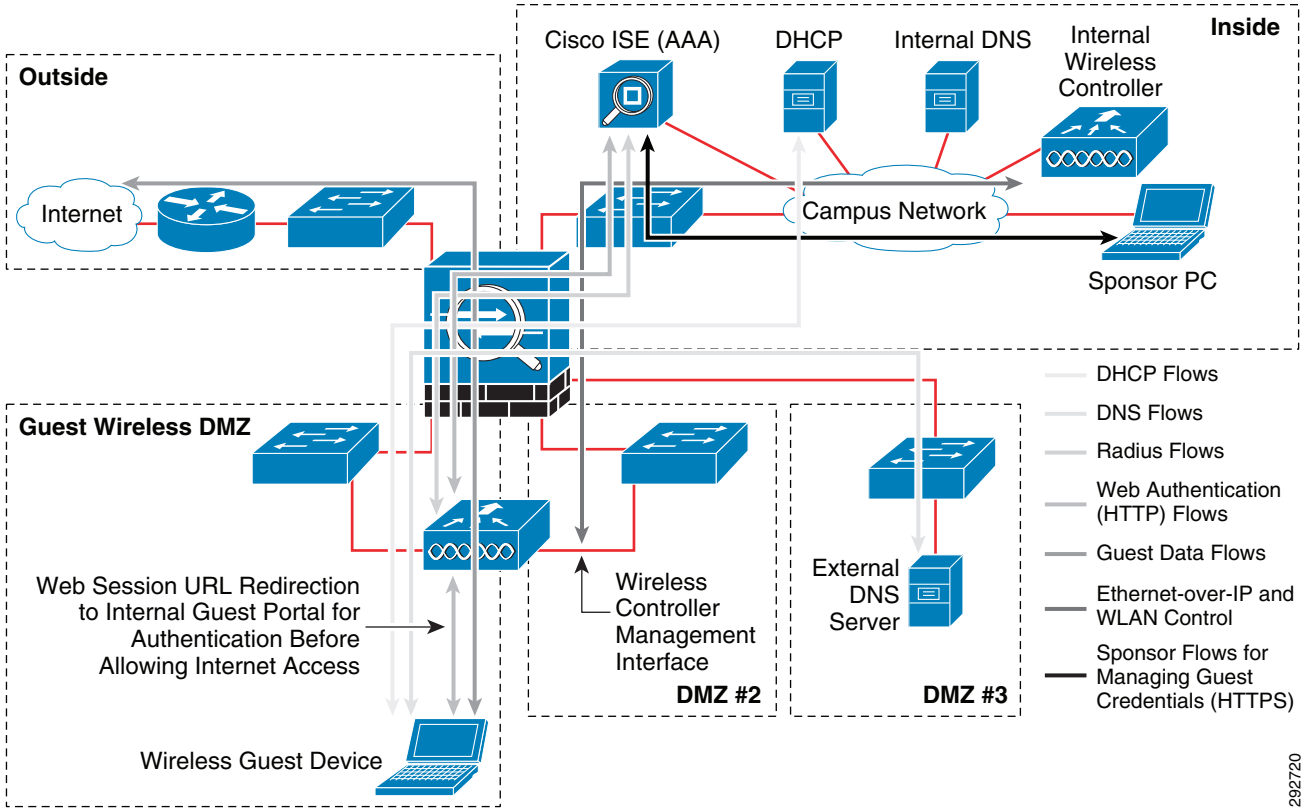
Figure 207 Applying an ACL as a Web Auth Pre-Authentication ACL



ASA Firewall Configuration

Figure 208 shows an example of the flows that need to pass through the Cisco ASA firewall to support this option.

Figure 208 Example of Flows that Need to Pass Through the Cisco ASA Firewall for Option 3



This option requires a RADIUS session to be allowed through the ASA firewall between the guest wireless controller and the Cisco ISE server. In addition, this option requires the guest Web session to be re-directed and allowed through the ASA firewall to the inside of the network, where the Cisco ISE server sits. By default the Cisco ISE guest portal uses TCP port 8443 for the guest portal. An Ethernet-over-IP (IP port 97) auto-anchor mobility tunnel, as well as the WLAN control port (UDP port 1666) between the management interfaces of the two wireless controllers, must still be allowed through the ASA firewall. Besides allowing DNS, DHCP (assuming the deployment of an internal DHCP server), and TCP port 8443 for the HTTPS redirection, the ASA firewall should be configured to block all other traffic generated from guest wireless devices onto the internal network.

Table 13 summarizes the relevant ports that need to be allowed through the ASA firewall.

Table 13 Ports to be Allowed Through the ASA Firewall

Application	Transport	Port
Ethernet-over-IP	TCP/UDP	97
WLAN Control	UDP	1666
ISE Guest Portal	TCP	8443
DNS	UDP	53

Table 13 Ports to be Allowed Through the ASA Firewall

Application	Transport	Port
BOOTPS (DHCP)	UDP	67
BOOTPC (DHCP)	UDP	68

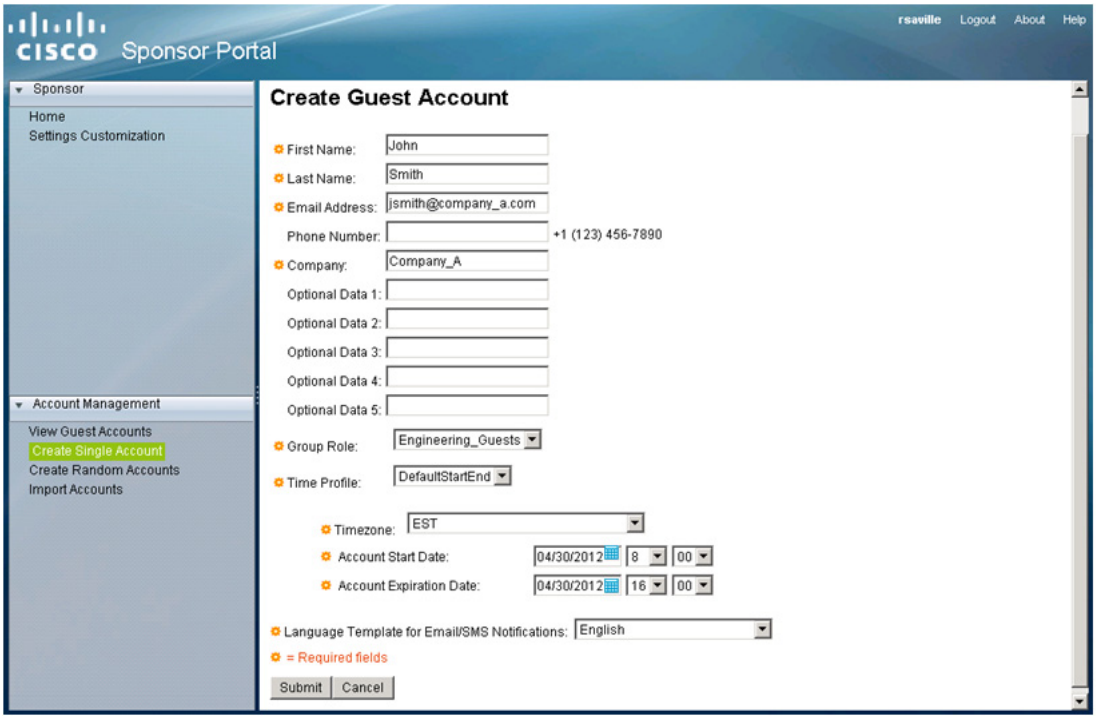
Cisco ISE Policy Configuration

The Cisco ISE authentication and authorization policy configurations are the same as discussed in Option 2. However, the Cisco ISE guest portal must be configured, as discussed in Cisco ISE Guest Portal.

Cisco ISE Sponsor Portal

The Cisco ISE sponsor portal provides more comprehensive functionality than the wireless controller sponsor portal discussed previously. The Cisco ISE sponsor portal can be accessed at: https://ISE_server:8443/sponsorportal/, where ISE_server is either the IP address or the name of the Cisco ISE server which can then be translated to an IP address via DNS. An example of the Web page for creating guest credentials within the Cisco ISE sponsor portal is shown in Figure 209.

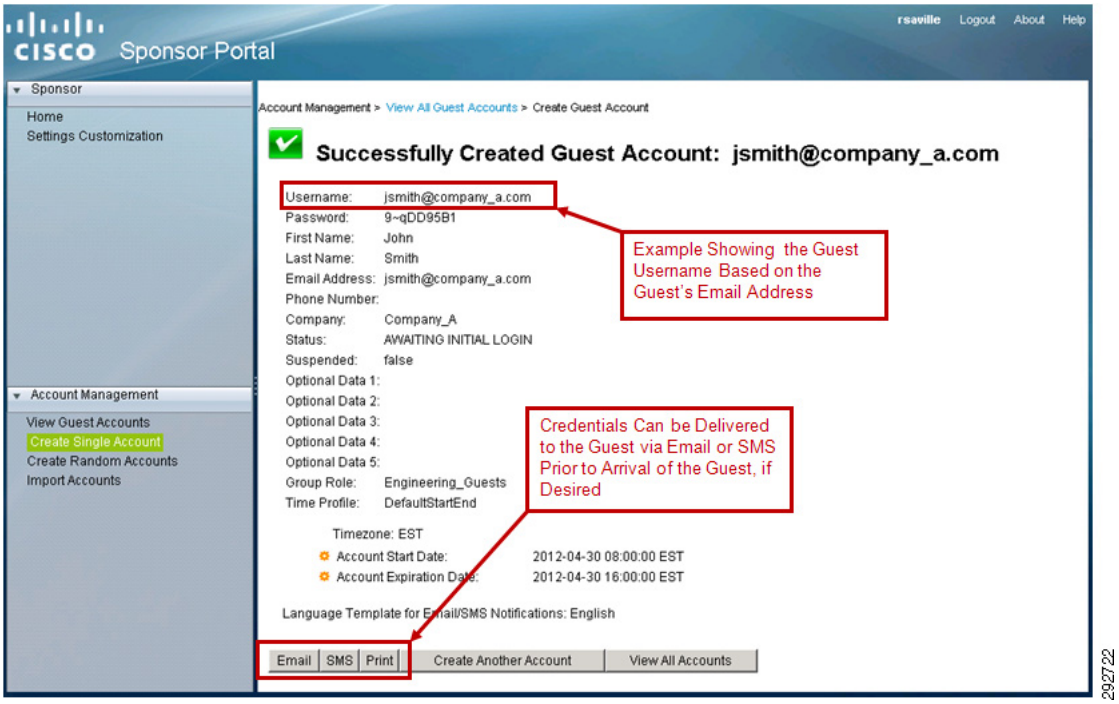
Figure 209 Creating Guest Credentials on the Cisco ISE Sponsor Portal



Information such as the company the guest is from, the guest's E-mail address and phone number, as well as optional user-defined data can be included. Optional data can include the WLAN SSID the guest needs to connect to (if the SSID is hidden), as well as the name, phone number, and department of the sponsor, for example. Depending upon the allowed time profiles, the credentials can be configured to become active at a future date and time and remain active for a period of time. The Cisco ISE sponsor portal also has the capability to deliver the guest credentials to the guest prior to arrival, via mechanisms such as E-mail and SMS. This is shown in Figure 210. Sending credentials via E-mail helps ensure the guest has

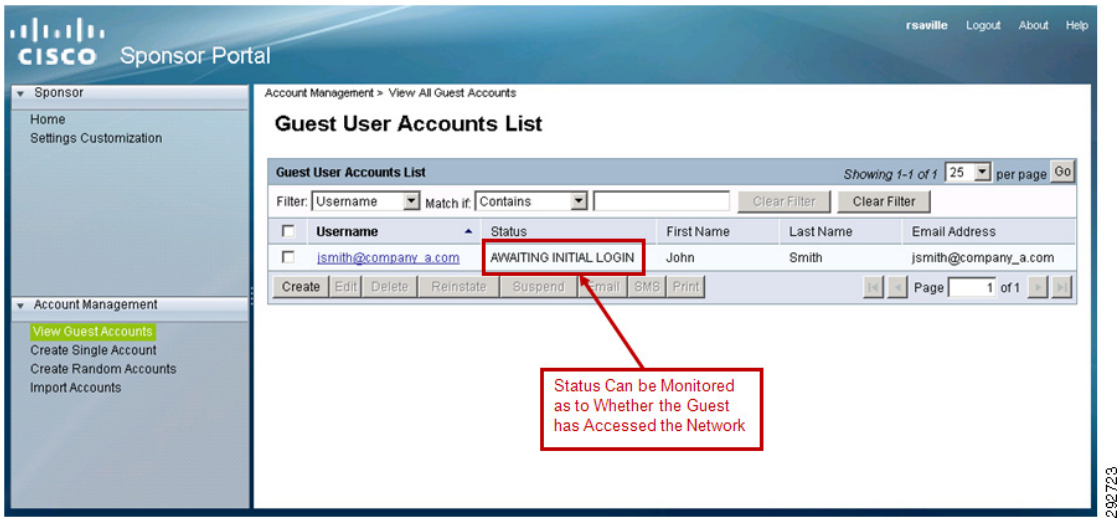
provided a valid E-mail address.

Figure 210 Example Guest Credentials



Once guest credentials are created, they can be monitored and managed by the sponsor via the Cisco ISE sponsor portal, as shown in Figure 211.

Figure 211 Monitoring Guest Credentials from the Cisco ISE Sponsor Portal



Note that in Figure 211, the guest username was based upon an E-mail address versus just the first and last name of the guest. Corporate E-mail addresses often contain the name of the company within the address. The next section discusses extending guest wireless access to allow employee personal devices as well. Use of the E-mail address within the guest username is one possible way to differentiate between guests and employees who may have the same first and last names.

Configuring the Cisco ISE Sponsor Portal

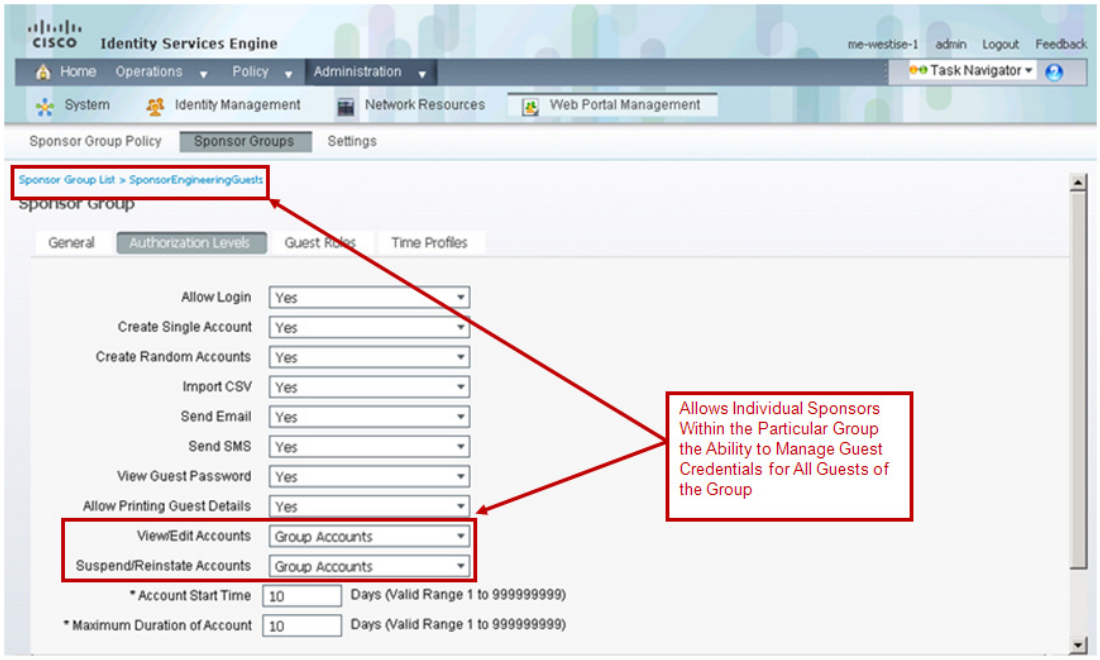
Configuration of the Cisco ISE sponsor portal is controlled via the network administrator through the Web Portal Management section of the Cisco ISE server. Different levels of sponsor responsibility—ranging from individual sponsors who can only view and edit guest accounts they have created, to group sponsors who can view and edit guest accounts for a particular group, to sponsors who can view and edit all guest accounts—can be created within the Cisco ISE server.

Multiple sponsor groups, each with their own members, can be created through the Sponsor Groups tab under the Web Portal Management section of the Cisco ISE server. Figure 212 shows an example where separate groups have been added for guests sponsored by the Engineering department and the Marketing department.

Figure 212 Example of Multiple ISE Sponsor Groups

Different authorization parameters can then be configured for each sponsor group by double clicking the particular sponsor group and selecting the Authorization Levels tab, as shown in Figure 213.

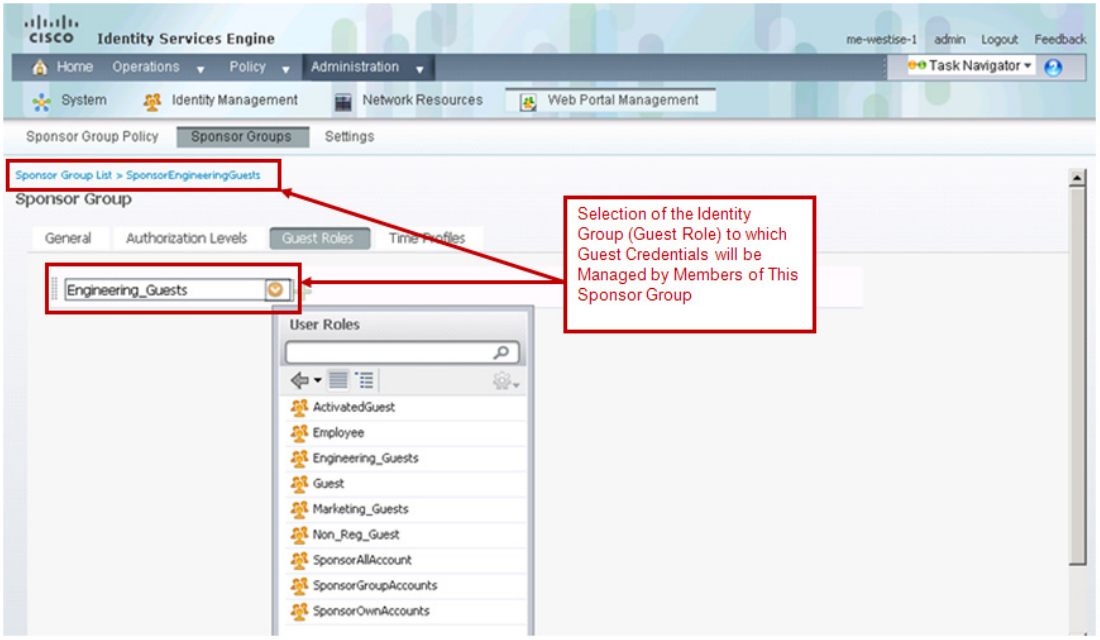
Figure 213 Example of Authorization Levels for an Individual Sponsor Group



This example shows a configuration where any member of the sponsor group is allowed to view, edit, suspend, and reinstate a guest credential created by any other member of the sponsor group. However, members of different sponsor groups cannot modify guest credentials created for this group.

The Guest Roles tab is used to select the user identity group (i.e., guest credential database) into which the guest credentials created by a member of this sponsor group are placed. An example is shown in Figure 214.

Figure 214 Example of Guest Roles for an Individual Sponsor Group

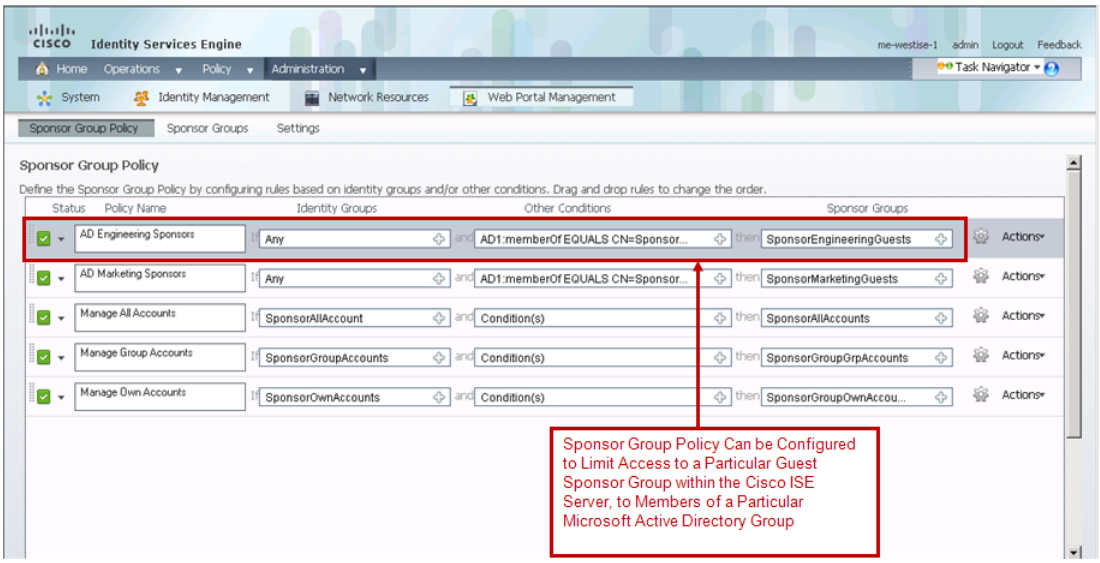


Note that the user identity group has to have been previously configured within the Cisco ISE server for it to be selected. This is done through the Identity Management section of the Cisco ISE server. This allows different sponsor groups to add guest credentials to different identity groups.

The Time Profiles tab allows the network administrator to determine which time profiles (either default or pre-configured within ISE) are applied to the particular sponsor group. This allows the network administrator the ability to have some control over the maximum amount of time that guest credentials can be configured for within the Cisco ISE server.

Once the sponsor groups are created within the Cisco ISE server, the Sponsor Group Policy tab can be used to create policies controlling who has access to which sponsor groups. Individual sponsor credentials can be defined directly on the ISE server. More commonly, the organization may wish to leverage existing Microsoft Active Directory groups to differentiate among different sponsors. Figure 215 shows an example of this.

Figure 215 Example of Microsoft AD for Sponsor Group Membership



In this example, access to the sponsor group is limited to those members of the Microsoft Active Directory domain who are members of the group called “Users/Sponsors_Engineering”. The exact condition for this example is of the form:

```
AD1:memberOf EQUALS CN=Sponsors_Engineering,CN=Users,DC=labdomain,DC=com
```

The Microsoft Active Directory domain is “labdomain.com” in this example. Note that the Microsoft Active Directory server must be configured as an external identity source to select this option. In this example it is known by the name “AD1”.

By tightly controlling members of the Microsoft AD groups which have sponsor access to ISE, the network administrator can limit the use of the guest wireless network to its original intended purpose—guest wireless access—instead of employee personal devices, if desired.

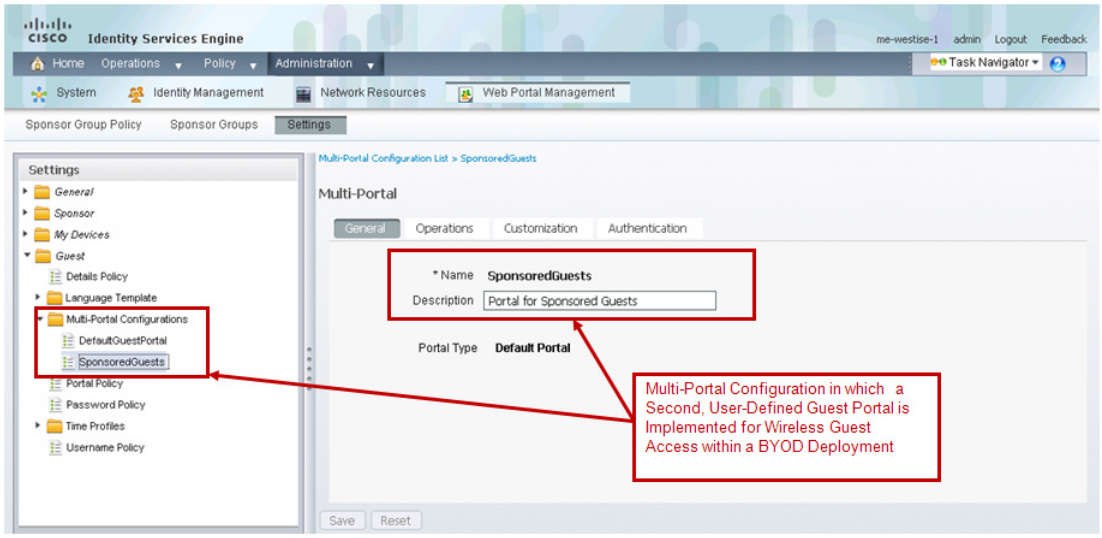
Cisco ISE Guest Portal

As mentioned previously, Cisco ISE has the capability to support multiple guest portals. The Cisco ISE server has a system-generated DefaultGuestPortal configuration. This allows the network administrator to provision a guest portal in order for employees or IT staff to on-board corporate-owned or employee personal devices, as discussed in Enhanced BYOD Access and Limited BYOD Access.

Configuring the Cisco ISE Guest Portal

An additional guest portal for wireless guest access can be defined within the Cisco ISE server through the Guest—>Multi-Portal Configurations folder within the Settings tab under the Web Portal Management section of the Cisco ISE configuration. An example is shown in Figure 216.

Figure 216 Example Multi-Portal BYOD Deployment

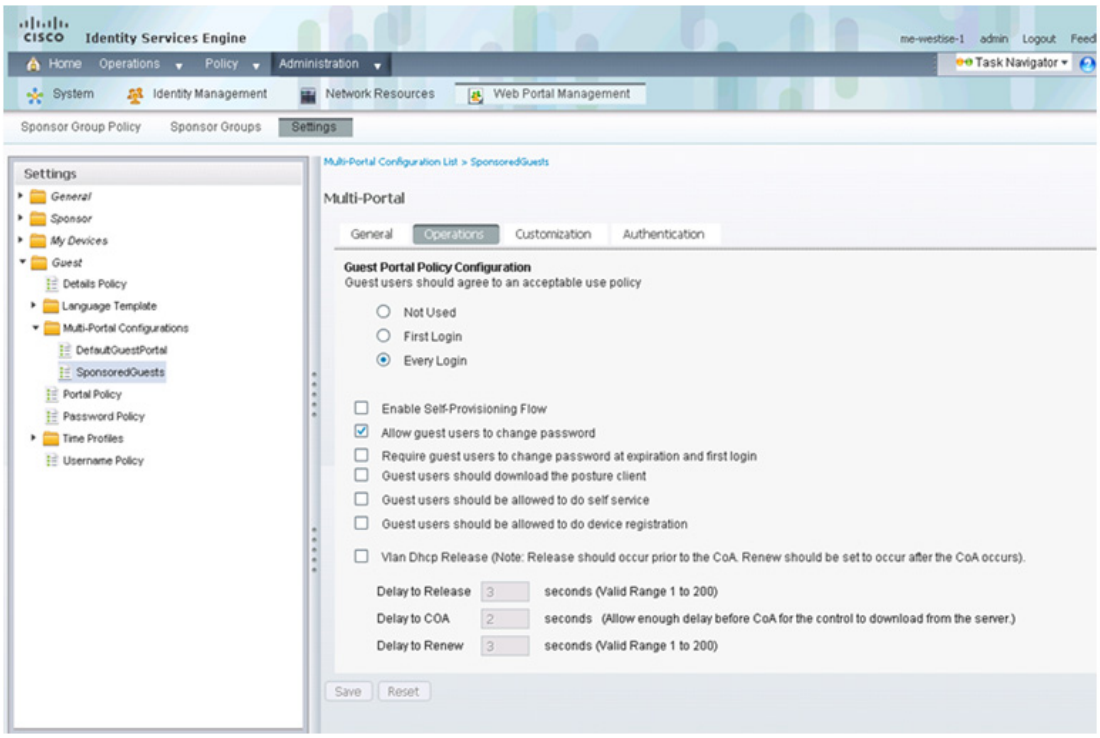


When a user-defined guest portal is implemented, the following is the form of the URL which needs to be configured within the guest wireless controller Web Auth Web Login Page as shown in Figure 205:
http://*ISE_server*:8443/guestportal/portals/*name_of_user-defined_portal*/portal.jsp

ISE_server is either the IP address or the name of the Cisco ISE server which can then be translated to an IP address via DNS. *Name_of_user-defined_portal* is the name of new user-defined guest portal, which is SponsoredGuests in the example above.

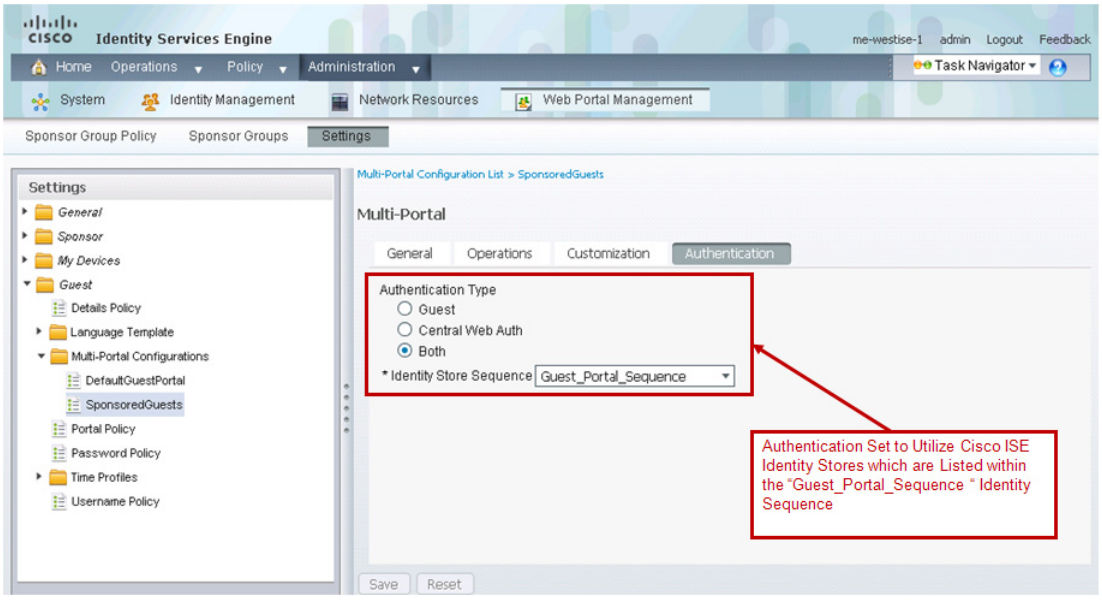
Once the new guest portal is defined, the Operations tab can be used to display an Acceptable Use Policy (also known as an End User Agreement or EUA), as well as control whether the guest can or must change the sponsor provisioned password. Note that the Operations tab can also be used to force the guest to register their devices with the Cisco ISE server before accessing the Internet from the guest wireless network. This version of the design guide assumes that the guest device itself is not considered in the decision to allow access to the guest wireless network. Hence, this use-case is not discussed. Figure 217 shows an example of the Operations tab.

Figure 217 Example of Operations Tab



The Authentication tab determines whether the internal database, one or more external identity stores, or both are checked for the guest credentials. An example is shown in Figure 218.

Figure 218 Example of Authentication Settings for a User-Defined Guest Portal



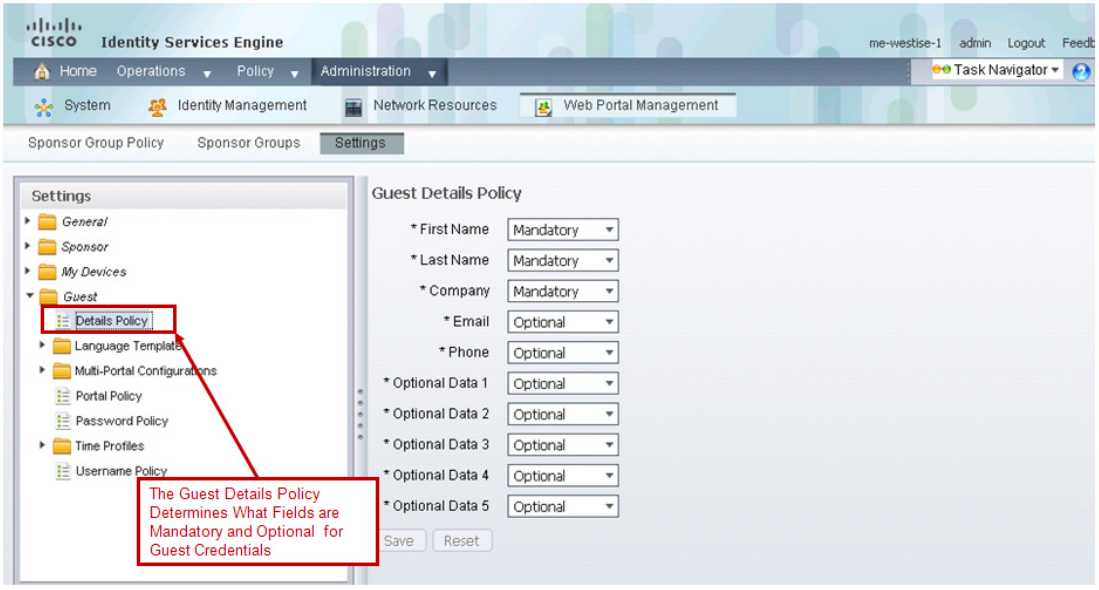
For this example the authentication type is set to Both, meaning Guest and Central Web Auth. Further, the identity source sequence called “Guest_Portal_Sequence” is chosen. This identity source sequence utilizes “internal users” when only wireless guest access is deployed, as shown in Figure 203. This

allows guests credentials to pass both the guest portal access and the ISE authentication policy. This configuration also allows guest access to be easily extended to include employee personal devices simply by adding Microsoft Active Directory identity store, as discussed in Extending Guest Wireless Access to Employee Personal Devices

Note Cisco ISE authentication logs may show the guest user authentication appearing twice with this configuration, although the guest is only authenticated once via Web Auth.

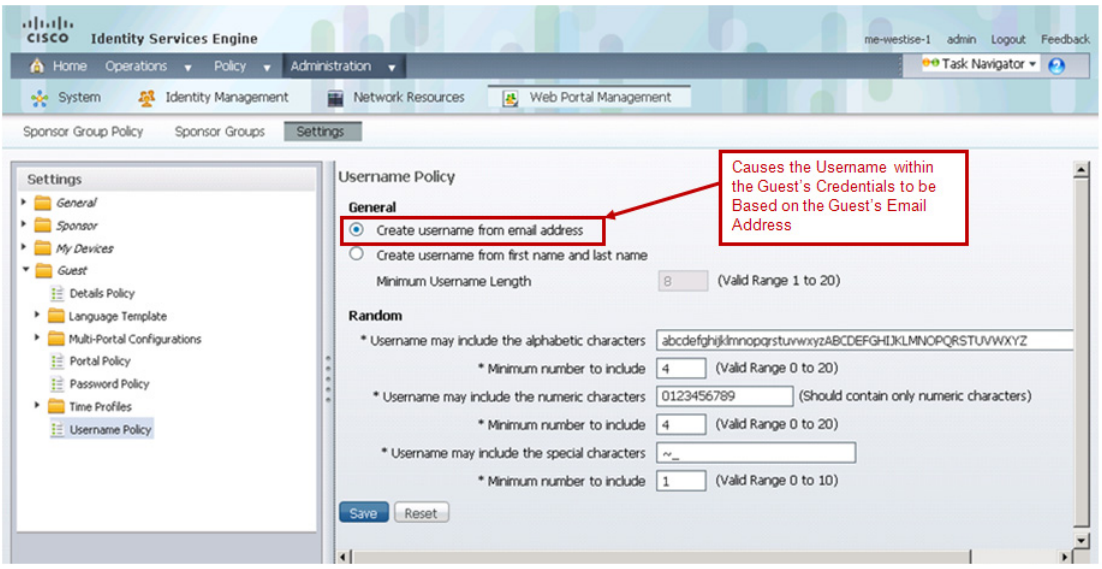
The Guest folder within the Settings tab under the Web Portal Management section of the Cisco ISE configuration is used to configure additional global guest parameters. For example, the Details Policy web page is used by the network administrator to specify which parameters are mandatory and which are optional. An example is shown in Figure 219.

Figure 219 Example of Guest Details Policy



Additional Web pages under the Guest folder control other global guest configuration parameters, such as Username Policy and Password Policy. The Username Policy is where the guest username can be selected to be based upon their E-mail address, as shown in Figure 220.

Figure 220 Example of Guest Username Policy



Finally, the Time Profiles folder can be used to select one of the existing time profiles for guest user access or to create a custom time profile. Time profiles are selected by the sponsor when configuring guest credentials to control when the guest user has access to the network and for how long.

Authentication and Authorization Summary

Table 14 summarizes the options discussed above for guest wireless access with Web Auth.

Table 14 Options for Guest Wireless Access with Web Authentication

Option	Where does the redirection of the Web session occur?	Where does the Web portal reside?	Where does the authentication of the end-user occur?	Is there a portal function for adding temporary guest credentials?
1	Wireless controller	Wireless controller	Wireless controller via local guest database	Yes, via LobbyAdmin level access to the DMZ wireless controller or centralized Cisco Prime Infrastructure server.
2	Wireless controller	Wireless controller	Cisco ISE server via RADIUS between the wireless controller and the Cisco ISE server	Yes, via access to a centralized Cisco ISE sponsor portal
3	Wireless controller	Cisco ISE server	Cisco ISE server via RADIUS between the wireless controller and the Cisco ISE server	Yes, via access to a centralized Cisco ISE sponsor portal

Additional Considerations

When implementing guest wireless access for devices such as Apple iOS or Mac OS X Lion, the network administrator should be aware that these devices have implemented a feature which automatically detects the presence of a captive portal deployment. It does this by generating an HTTP request to an Apple Website and looking for a response. If a redirect is received, then a captive portal deployment is

assumed. This feature only applies to SSIDs which have open access, as is typical with most guest wireless networks. When a captive portal deployment is detected, the iOS or Mac OS X Lion device automatically displays a dialog window for authentication without the end-user having to launch the Web browser. This feature is intended to make it easier for non-browser based applications to access the Internet, without the end-user having to launch a Web browser, by performing Web Auth via the pop-up window. Many HTML-based mobile applications do not use the browser as the user interface. This is known as Captive Portal Network Assistance (CPNA) and is effectively a light weight HMTL-based user interface. Unfortunately the interface is not properly interacting with the iOS profiler manager. The symptoms are different based on the version of iOS. In iOS5, the user was not allowed to install the WiFi profile without canceling the CPNA, forcing the device off the provisioning SSID. In iOS6, the user is automatically brought to the profile manager, but after installing the profile, the user is not returned to the CPNA to receive the certificate. In both cases, the CPNA is not able to successfully on-board the device

Cisco wireless controllers have implemented a workaround that bypasses this feature, allowing Apple iOS or Mac OS X Lion devices to operate within a captive portal deployment with HTTPS connectivity to a guest portal with a self-signed certificate. The network administrator needs to establish an SSH session to the guest wireless controller and issue the following command:

```
configure network web-auth captive-bypass enable
```

This command causes the wireless controller to answer back the HTTP request, spoofing the iOS or Mac OS X Lion device into thinking that there is no captive portal deployment. Once the end user opens a browser and attempts to navigate to any site, they are redirected to the portal and prompted for credentials using the normal Web Auth process. Note that non-browser based applications are not able to access the network until the end user opens a Web browser and proceeds through the normal Web Auth process. This includes HTML-based applications such as WebEx.

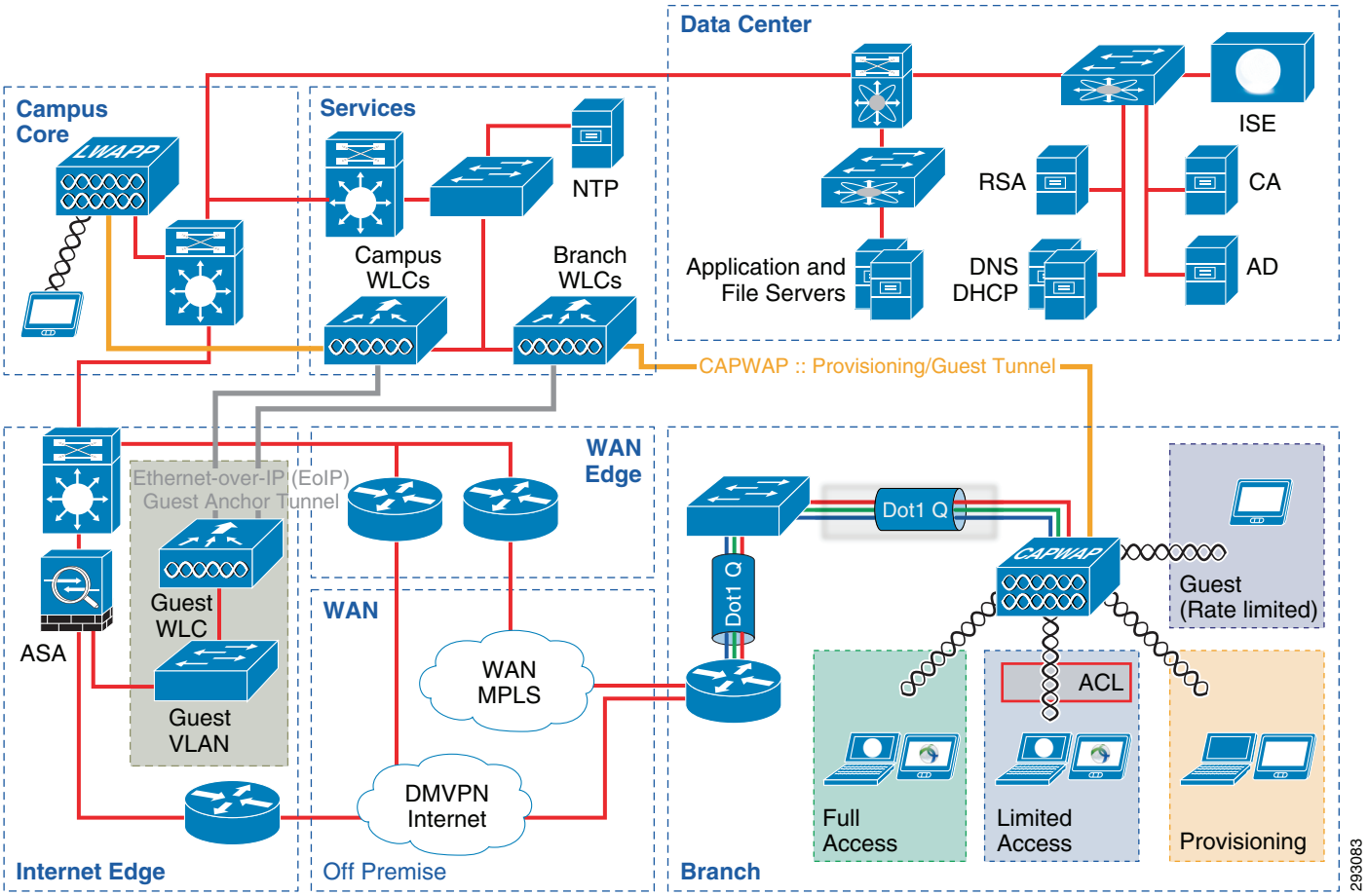
Wireless Guest Access at the Branch

Branch networks frequently offer wireless guest services. There are two basic architectures that can be deployed. The first is a centralized model in which all branch wireless guest traffic is tunneled via CAPWAP to a central controller located within the campus, known as the foreign controller. Wireless guest traffic is then further tunneled via EoIP to an anchor controller located in the DMZ. This is the preferred method presented in this design guide.

An alternate method is to use FlexConnect to locally terminate guest traffic in a secure segment located within the branch. The advantage of the second approach is that guest traffic does not consume expensive corporate WAN bandwidth. Instead guest traffic is isolated within the branch and uses a local branch Internet path. Future versions of this design guide may explore this option. In addition, there many other possible WAN deployment models that may be leveraged to provide guest users with access to the Internet. A collection of white papers that explain various WAN archtiecures is available at: http://www.cisco.com/en/US/netsol/ns816/networking_solutions_white_papers_list.html.

The guidance presented here follows a centralized model. The FlexConnect wireless controller which services branch locations and which provides on-boarding to branch BYOD devices is also used as a foreign controller to tunnel wireless guest traffic to a guest wireless controller within the campus Internet edge. Figure 221 shows the various components required for this model.

Figure 221 Guest Wireless Access at the Branch



Because separate wireless controllers are deployed for campus and branch wireless access, the same guest SSID can be configured on both wireless controllers, but with different characteristics, such as rate limiting. This is one advantage of deploying separate wireless controllers for branch and campus locations.

Due to the limited amount of WAN bandwidth available at branches, network administrators often have the requirement to limit the amount of bandwidth that guest users can utilize below that which guest users can utilize within a campus. The next section discusses rate limiting of wireless guest traffic at the branch. Most other aspects of branch wireless guest access are essentially carried over from the campus wireless guest design. For example, branch wireless guests can continue to use Cisco ISE for the guest portal. Logically the wireless topology for branch guest traffic is the same as wireless access for campus guest traffic. The main difference is that the capacity of the transport will vary over the guest SSID to a larger extent than what would be expected in the campus where the physical path is typically supported by gigabit Ethernet.

Rate-Limiting Guest Wireless Access

The prevalence of mobile devices and the expectation of universal network access have resulted in a steady increase in the loads on the guest network. This solution offers rate-limiting tools that can be used to manage these loads. Rate limiting can be configured in various ways—per-user or per-SSID as well as upstream and downstream.

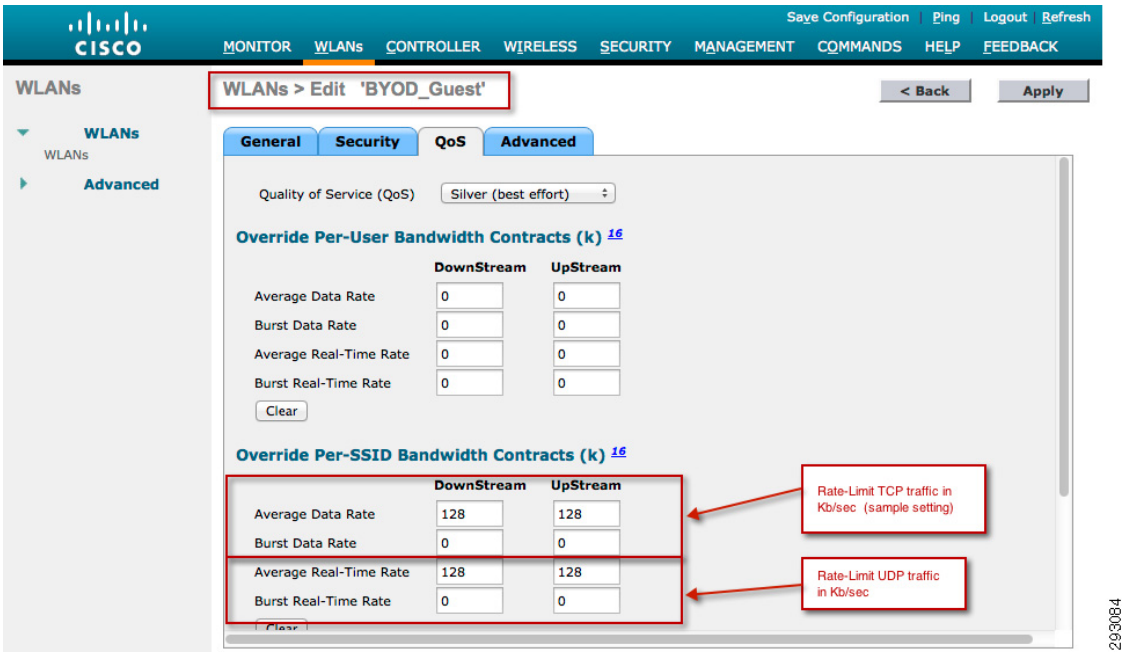
Note Per-SSID rate limiting is actually per-BSSID, since the rate limiting is per SSID per access point per radio. However, this design guide refers to this as per-SSID rate limiting.

Per-user rate limiting applies to each specific wireless device. Per-SSID is an aggregate rate shared by all devices within a given SSID. In both cases, upstream rate limiting occurs on the radio. Downstream per-SSID rate limiting also occurs on the radio while downstream per-user rate limiting occurs on the wireless controller.

Rate-limiting in this context is analogous to policing. Packets determined to be in excess of the configured rate are dropped and not metered or buffered. Policers implement a token bucket. The bucket is credited with tokens at a rate that equals CIR. When the bucket is full, no additional tokens are added. Tokens are removed from the bucket when a packet is transmitted, provided a token is available. If no tokens are available, the packet is discarded. The size of the token bucket determines the burst rate. As long as tokens are available, packets are transmitted at line rate. In an effort to keep the configuration intuitive, users configure the burst rate directly and the algorithm determines the appropriate bucket size. If the burst rate is set to 0, a default bucket size is used. An example of how to configure rate limiting of the Guest SSID is shown in Figure 222.

One unique characteristic of wireless is that not all transmissions occur at a single rate. Signal strength and signal-to-noise ratio (SNR) will determine the actual speed of the physical medium for any single station. Unlike wired networks where the speed is fixed at the port rate, wireless rates can vary for each host on the subnet and may even change as the station moves closer or further from the access point. With wireless rate limiting, the time required to drain a full token bucket depends on the access speed of the wireless client and is not fixed. Stations that associated at 54 Mbs will be able to drain a token bucket faster than those at 1 Mbs. If per-SSID rate-limiting is in place, all clients on a particular AP share a single bucket. If per-User rate-limiting is in effect, then each station is assigned a unique bucket. It is possible to do both per-client and per-SSID rate limiting. In this case a token must be available and is removed from both the shared SSID bucket and per client bucket before the packet is transmitted. While this may provide more fairness to a slower user trying to access a shared token, it increases the amount of state information that must be maintained, increasing processing requirements on the controller. Because many deployments of guest wirless access simply provide best-effort service levels, extra processing requirements are not typically merited. As such, only per-SSID shaping is shown here. There may be other situations where a business case does justify doing both per-user and per-ssid rate limiting simultaneously.

Figure 222 Example Configuration for Rate Limiting the Guest SSID



The primary branch design presented within this design guide uses FlexConnect with local branch termination for corporate wireless clients and central termination for guest traffic. Corporate approved devices may send data to servers located within the central datacenter. Alternatively, they may send data to a local server. Where access to a local server is required, FlexConnect with local termination can save WAN bandwidth by eliminating the need to transfer data through a CAPWAP tunnel over the WAN to a central controller. Locally terminated traffic may still travel over the WAN when access to servers located within the data center is required, but these packets will not be tunneled within CAPWAP. In this case, normal QoS techniques can be applied. Hence, wireless packets are classified along with wired traffic. This common classification for corporate wired and wireless devices applies in both the upstream and downstream direction. With the design presented within this document, CAPWAP tunnels are used for all guest traffic—traffic from personal devices which have not on-boarded, as well as wireless control traffic (traffic from the wireless controller and the branch access points). Therefore, of all the CAPWAP traffic leaving the branch, the majority of packets will likely belong to guest users. This can help disguish guest traffic from corporate traffic.

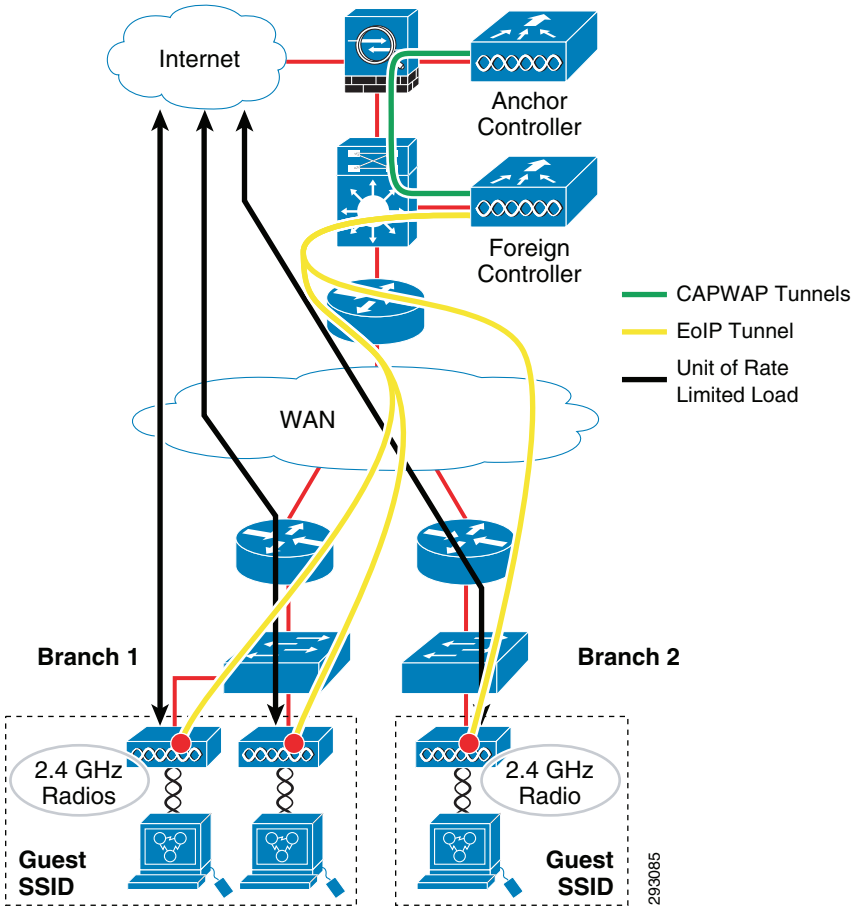
The example configuration shown above allows for two classification rates, the data rate and the real-time rate. Within the context of this configuration, Data is meant to be all TCP flows and Real-Time is meant to be all UDP flows. As a best practice for QoS, it is recommended to prevent UDP and TCP from competing directly with each other for bandwidth due to differences in how dropped packets influence flow. Providing distinct token buckets for each protocol prevents any undesirable interaction between UDP and TCP.

Rate limiting is configured on the foreign controller. When guest access is offered at both the campus and branch locations, there will be two foreign controllers tunneling to an anchor controller. The rate limit configured on each foreign controller can be different and unique for that class of users. Typically the foreign controller services campus guests will have a higher bandwidth contracts than the foreign controller servicing branch guest users because of the higher campus bandwidth available when compared to the WAN.

There are other caveats to be aware off when rate limiting. Because SSID rate limiting occurs at the radio itself, each radio will limit the SSID to the configured rate. This means that if Branch_A and Branch_B are each members of the BYOD_Guest SSID, each branch will limit guest traffic without regard to the

current load in the Guest SSID at the neighboring branch. However, this means if the Guest SSID is present on two radios at the same branch and the rate is configured for 1 Mb/s, the combined rate could be as high as 2 Mb/s over the WAN at that single branch. Even within a single AP, if the Guest SSID is using the 2.4Ghz radio and the 5 Ghz radio, the total bandwidth could be double the configured guest rate limit. As stated earlier, the feature's primary purpose is to protect the radios. Because of this, rate limiting may necessitate the over subscription of WAN bandwidth intended for guest use. To minimize the extent of oversubscription, the Guest SSID should not be enabled on the 5 Ghz radio. In addition, the number of APs participating in this SSID should be the minimum required to provide adequate coverage. AP groups can be used to manage which APs are participating. Rate limiting a single BYOD_Guest SSID across all branch locations may result in different WAN rates at different branches, as illustrated in Figure 223.

Figure 223 Rate-Limiting the Guest SSID



In Figure 223, assume the rate limiting of the BYOD_Guest SSID is configured for 1 Mb/sec. At Branch 1, the local WAN circuit could experience as much as 2 Mb/sec of guest traffic while the WAN aggregation circuit at the head-end could experience up to 3 Mb/sec of guest load. If a single SSID is in use for guest traffic, then the configured rate should be appropriate for the least common denominator, which is the slowest branch location that will be hosting guest traffic. There are some options available to better manage guest loads at the branch that are disucussed below.

Multiple Guest SSIDs and AP Groups

Because traffic limits are established per SSID and because not all branches have the same bandwidth available for guest use, the administrator may want to establish multiple Guest SSIDs based on the configured rate-limit. For example, the GUEST_128 SSID may be rate-limited to 128 Kb/s while the GUEST_256 SSID may be twice as fast. AP groups must be used to ensure both WLANs are not available at all branch locations. If the majority of branch locations have more than one AP that will host guest traffic, then the configured rate limit will be less than the actual desired rate to minimize oversubscription. AP groups can be used to manage how many radios are contributing to the total guest load for that location. Multiple Guest SSIDs in conjunction with AP groups can be used to ensure adequate guest coverage without excessive WAN loads. Creating informative names for the branch APs will simplify creating AP groups.

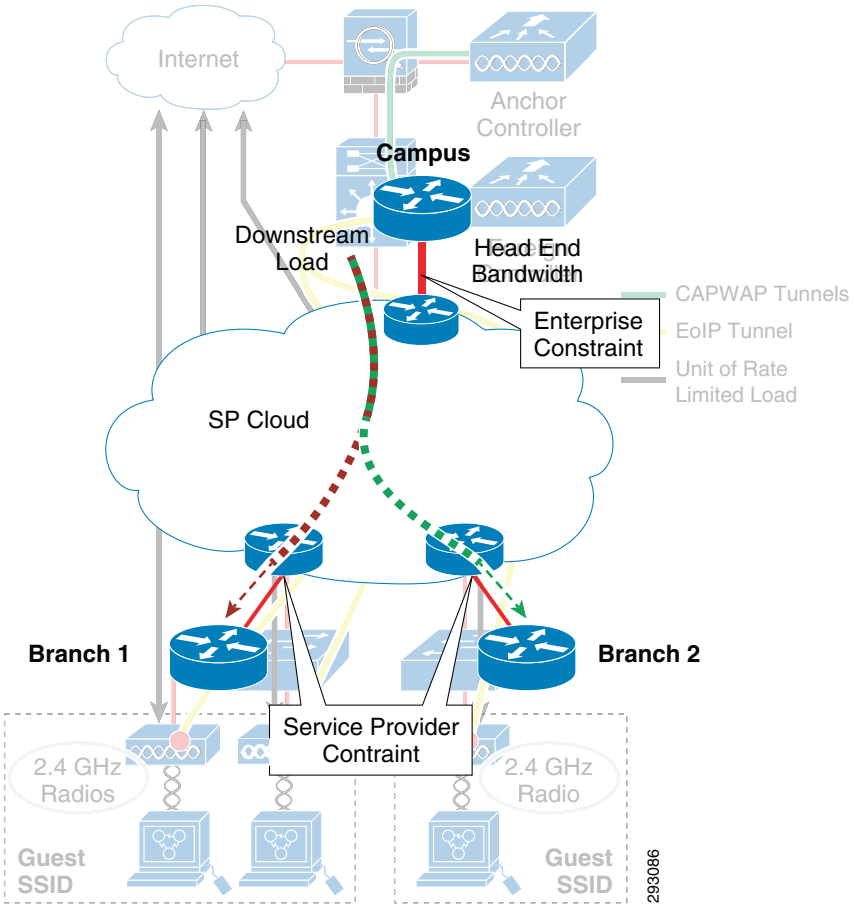
AP Groups are explained in greater detail in the *Flex 7500 Wireless Branch Controller Deployment Guide* at:
http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml#ap-gr.

Managing the Downstream Load

To recap, the primary branch design presented within this design guide uses FlexConnect with local branch termination for corporate wireless clients and central termination for guest traffic. Corporate approved device may send data to servers located within the central data center. Alternatively, they may send data to a local server. Where access to a local server is required, FlexConnect with local termination can save WAN bandwidth by eliminating the need to transfer data through a CAPWAP tunnel over the WAN to a central controller. Locally terminated traffic may still travel over the WAN when access to servers located within the data center is required, but these packets will not be tunneled within CAPWAP. In this case, normal QoS techniques can be applied. Hence, wireless packets are classified along with wired traffic. This common classification for corporate wired and wireless devices applies in both the upstream and downstream direction. With the design presented within this document, CAPWAP tunnels are used for all guest traffic—traffic from personal devices which have not on-boarded, as well as wireless control traffic (traffic from the wireless controller and the branch access points). Therefore, of all the CAPWAP traffic traveling towards the branch, the majority of packets marked with DSCP 0 will likely belong to guest users. This can help disguish guest traffic from corporate traffic.

There are two points in the downstream path where loads imposed by the guest users could impact corporate traffic. These are the outbound interface on the WAN aggregation router and the outbound interface on the PE router adjacent to the branch. Figure 224 highlights the areas of concern in the downstream direction.

Figure 224 Downstream Congestion Points



The Per-SSID rate limiting discussed in the previous section does not provide direct control of the load on the WAN aggregation head ends imposed by guest users at the branch. The guest load will be proportional to the total number of Branch APs hosting the Guest SSID times the per-SSID rate limit of the WLAN. Guest wireless traffic may be distinguishable from other WAN traffic because it will be in a CAPWAP tunnel and marked with the default DSCP setting. Some traffic from employees on-boarding personal devices will also be marked the same way. However, the percentage will be very small. It is possible to construct a policy that will mark CAPWAP packets with default DSCP values into the scavenger class. This will have the effect of setting guest traffic below the priority of default corporate traffic. When the bandwidth of the WAN aggregation circuit begins to saturate, this policy will allow wireless guest traffic to be discarded prior to corporate traffic. If on-boarding traffic is also dropped along with guest traffic, then employees will need to wait until the WAN loads are lowered prior to bringing a new device onto the network. This is implemented with traditional QoS policy maps on the outbound circuits of the WAN Aggregation router. Incidentally the same approach could be used on the branch uplink to manage situations where the number of APs at the branch could unreasonably oversubscribe the uplinks.

The service provider local links to the branch may also come under load as a result of the guest traffic. The per-SSID does benefit the branch WAN links in this direction by limiting the effective guest bandwidth as a result of application-based flow control. An example is TCP-based applications, which will manage their flow to minimize drops. Even though per-SSID in the downstream direction is applied at the radio towards the end station, the client application will throttle down to meet the rate available over the entire path. The last hop interface on the SP PE router also contributes to application throttling

if aggressive policers are used to enforce contracted rates. Assuming wireless guests are remarked scavenger and appropriate DSCP to EXP mappings are being used, then SP policers should disproportionately impact wireless guest TCP applications. Although guest Internet traffic rarely uses UDP, it also generally exhibits the same type of flow control behavior as TCP even though the protocol itself does not implement feedback as part of the transport layer. This is because UDP is often transactional based. When UDP is used for bulk transfer, blocks of data are numbered and acknowledged by the application, for example TFTP. A transmitter will not send a block of data until the receiver has acknowledged the previous block. If a block of data is dropped, the transmitter will wait for a timeout period before retransmitting the previous block. Two exceptions to UDP application based flow control are UDP-based IP video surveillance which may not use RTSP to monitor received data and UDP multicast. Neither of these are typical applications guest will use on the Internet. In any case, per-SSID rate limiting is an effective means to manage guest traffic on the SP's PE routers.

Basic Access Design

Previous sections of this design guide have examined on-boarding employee personal devices to provide full, partial, or Internet only access. The use of digital certificates provides an additional level of authentication security by preventing the spoofing of device MAC addresses. Additionally, the use of the guest portal for self-registration and the "My-Devices" portal streamline the on-boarding and maintenance of employee personal devices, resulting in lower IT operating costs associated with providing BYOD services.

Despite these benefits, a subset of organizations may still decide on a business policy which does not on-board wireless employee personal devices, yet provides some access to corporate services and the Internet for such devices. This may be because of one or more of the following reasons:

- The organization does not have the desire or the ability to deploy digital certificates on employee personal devices.
- The employee may decide to opt-out of having the organization "manage" their personal device.
- The organization does not wish to administratively manage and maintain separate lists of registered devices and devices which have full network access.
- The organization may wish to simply restrict employee personal devices to "outside" of the corporate firewall due to an unknown or un-trusted security posture of such devices.

Because of this, the following sections discuss design options for wireless employee personal devices which do not involve on-boarding such devices. The designs are based around extending traditional guest wireless access discussed in the previous section and providing similar guest-like wireless access for employee personal devices.

Note Throughout this section, it is assumed that corporate-owned devices will still be on-boarded as discussed in Limited BYOD Access. The use of a whitelist is still necessary to prevent employee personal devices from getting full access to the corporate network.

Extending Guest Wireless Access to Employee Personal Devices

The following sections discuss two methods for extending guest wireless access, discussed in the previous section, to also allow employee personal devices access to the guest network:

- Allowing employees to provision guest credentials for themselves.

- Extending guest Web authentication (Web Auth) to also utilize the Microsoft Active Directory (AD) database when authenticating guests and employees using personal devices.

Allowing Employees to Provision Guest Credentials for Themselves

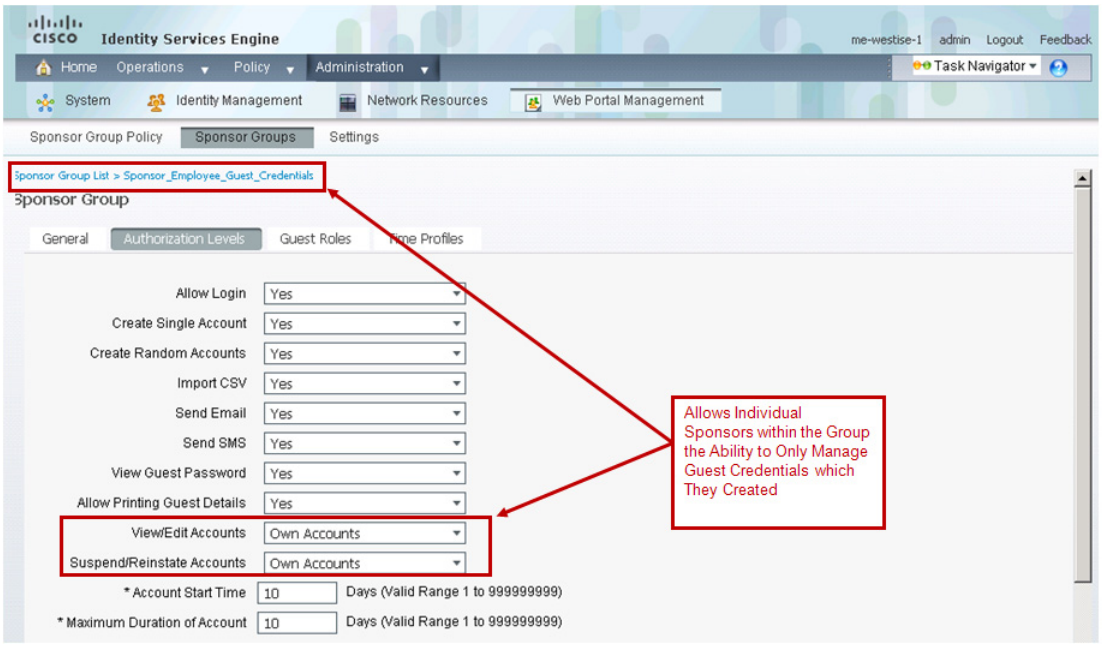
BYOD Guest Wireless Access discussed two means of provisioning guest credentials depending upon the deployment model, namely via either:

- Cisco wireless controller sponsor portal
- Cisco ISE sponsor portal

The most basic form of extending guest wireless access to employee personal devices is simply to allow employees to sponsor themselves as guests. Employees then manually connect to the open guest SSID to utilize personal devices on the wireless guest network.

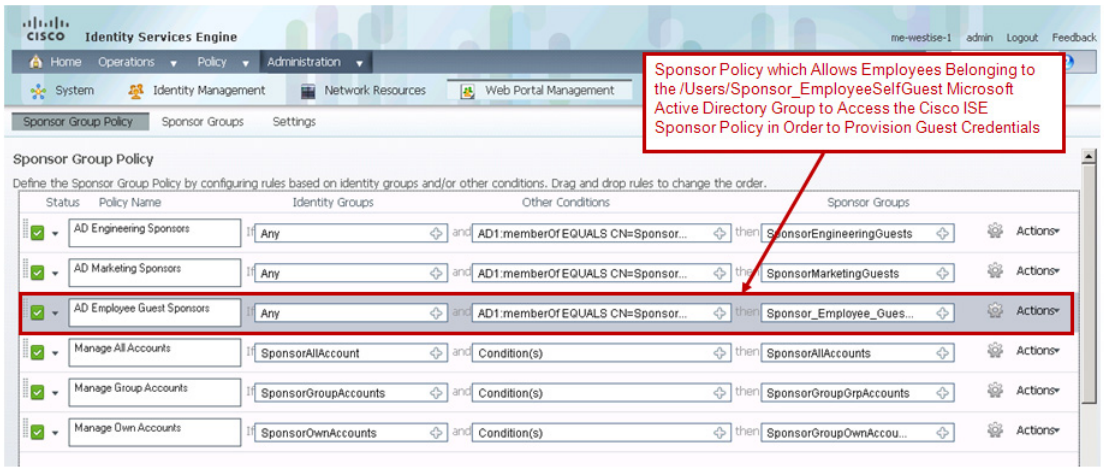
With the Cisco ISE sponsor portal, the sponsor authentication policy can be based on membership within a particular Microsoft AD group. This was discussed in Configuring the Cisco ISE Sponsor Portal, which discussed the use of Microsoft AD groups within the ISE sponsor group policy as a means to limit sponsor access to the Cisco ISE server. This can equally be used to allow broader access to the ISE sponsor portal simply by adding additional employees to those Microsoft AD groups. Alternatively a new sponsor group that allows individual employees to configure guest credentials, but restricts them to being able to only modify credentials that the individual employee provisioned, can be created. An example is shown in the figures below.

Figure 225 Example ISE Sponsor Group for Employees to Create Self Guest Credentials



Membership to this ISE sponsor group can then be restricted to a Microsoft AD group via the ISE sponsor group policy, as shown in Figure 226.

Figure 226 Example ISE Sponsor Group Policy for Employees to Create Self Guest Credentials



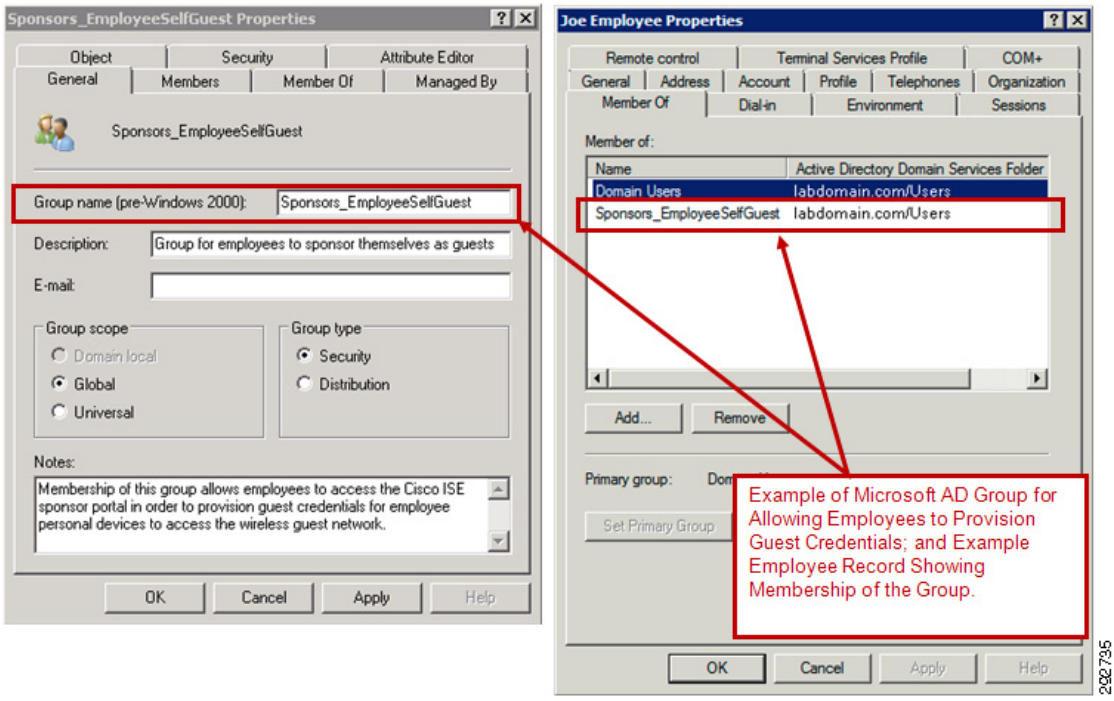
In this example, access to the sponsor group is limited to those members of the Microsoft Active Directory domain who are members of the group "Users/Sponsors_EmployeeSelfGuest". The exact condition for the example is of the form:

```
AD1:memberOf EQUALS CN=Sponsors_EmployeeSelfGuest,CN=Users,DC=labdomain,DC=com
```

The Microsoft Active Directory domain is "labdomain.com" in this example. Note that the Microsoft Active Directory server must be configured as an external identity source to select this option. In this example it is known by the name "AD1".

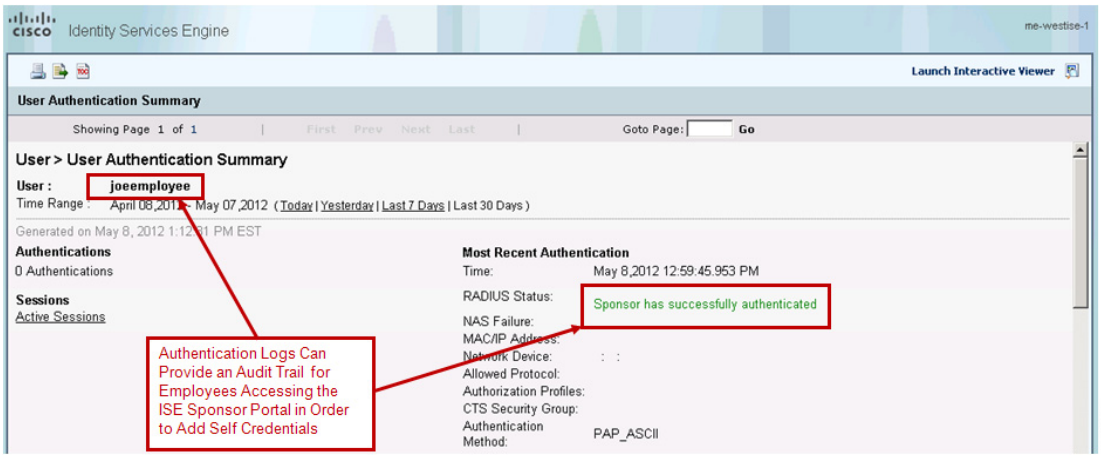
Figure 227 shows a basic configuration of the group within the Microsoft Active Directory server. Also shown is an example employee who has been made a member of the group.

Figure 227 Example Microsoft AD Group and User Configuration Screens



One advantage of this design is that an audit trail exists through the ISE authentication logs for employees authenticating to the ISE sponsor portal. Although the ISE authentication logs do not specifically show if the employee created or modified a guest credential, they can be used to gain a rough idea of which employees are accessing the ISE sponsor portal and how often.

Figure 228 Example of the Audit Trail for an Employee Accessing the ISE Sponsor Portal



Note that this method of allowing employees the ability to create guest credentials for themselves does not prevent them from creating credentials for true guests who are visiting the organization. Corporate business policy should dictate that true guest credentials only be added by authorized members of sponsor groups, as discussed in BYOD Guest Wireless Access. The next design option eliminates this issue by removing the ability for employees to create guest credentials for themselves altogether.

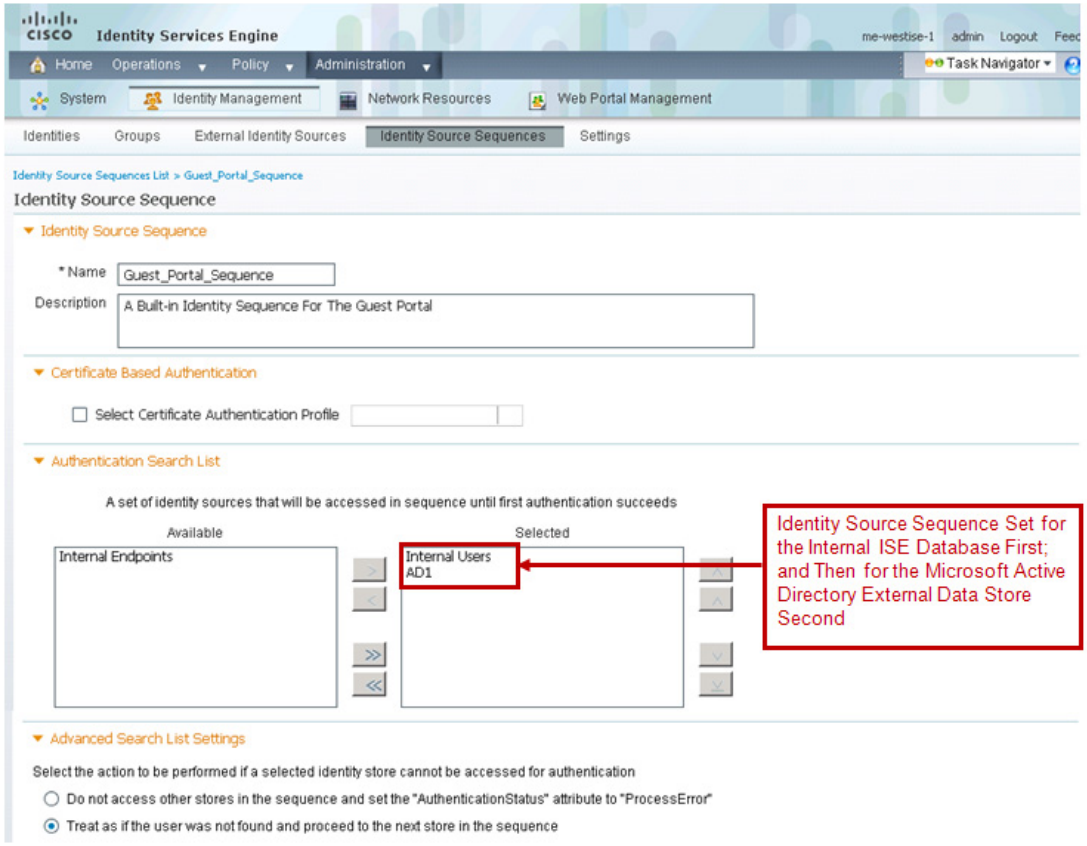
Extending Web Auth to Use Microsoft AD when Authenticating Employees with Personal Devices

The previous section discussed the most basic way of extending guest wireless access to allow employees with personal devices to access the guest network. That method was to simply allow employees to configure guest credentials for themselves via the Cisco ISE sponsor portal. Although this provides several advantages over utilizing a shared sponsor account on the guest wireless controller for adding credentials, it still has several shortcomings. Employees must still provision temporary guest credentials for themselves. There is an audit record of the employee accessing the Cisco ISE sponsor portal. However, there is no easy way of tying together the credentials created by the employee with the actual employee. The ISE authentication logs only show the guest credentials accessing the guest wireless network and not the employee userid. Finally, there is nothing preventing the employee from sponsoring a true guest, other than corporate business policy.

An alternative means of providing access to the guest wireless network for employee personal devices is to simply allow the ISE server to check multiple identity sources for credentials when performing Web authentication (Web Auth). For example, the ISE server could first check its internal identity groups (local database) for guest credentials. If the credentials are not found there, then check the Microsoft AD external identity store to see if the person accessing the guest network is an employee instead of a guest.

Web Auth Option 2—Wireless Controller Web Portal with Cisco ISE Authentication and Sponsor Portal discusses the use of a user-defined identity source sequence called Guest_Portal_Sequence for authenticating guest access via Web Auth. The Guest_Portal_Sequence uses the Internal Users identity source only. This can easily be extended by adding a Microsoft Active Directory (AD1) external identity source to the sequence, as shown in Figure 229.

Figure 229 Example of Guest_Portal_Access Identity Source Sequence Extended to Include AD



This configuration now allows employees who are in the Microsoft Active Directory database to access the guest wireless network from their personal devices once they have performed Web authentication and accepted the Acceptable Use Policy (AUP) or End User Agreement (EUA).

Note This allows employees to access the guest wireless network from corporate-owned devices as well, since the authentication and authorization decision is based on Microsoft Active Directory userid and password only. The device itself is not considered within the authentication and authorization decision.

Note The same functionality can be accomplished via the configuration of the guest wireless controller itself when utilizing the sponsor portal within the Cisco wireless controller for guest access, rather than the Cisco ISE sponsor portal. This design is not discussed within this version of the design guide.

Deploying Guest-Like Wireless Access for Employee Personal Devices

The previous sections discussed options for extending access to the wireless guest network for employees with personal devices, either by allowing employees to configure guest credentials for themselves or by extending Web Auth to also check the Microsoft AD database where employee credentials are kept. With these options, employee personal devices share the same wireless SSID as

guest devices. Employee personal devices also share the same IP subnet address space as guest devices, since they terminate on the same DMZ segment of the ASA firewall. Essentially the employee's personal device is treated as a guest on the network, which can bring up in potential concerns.

Since IP subnet space is shared between guest devices and employee personal devices, there can be some concern that employee personal devices could deplete the IP addressing space, limiting the ability of guest devices to gain access to the guest network or vice-versa.

The ASA firewall guest DMZ interface ingress policy can be modified to allow certain application flows inbound from the guest network to a mirror of the company Web site server, dedicated for employee personal devices, sitting on other DMZ segments. This is discussed further in Accessing Corporate Resources. However, the ASA firewall policy would not be able to distinguish between guest devices and employee personal devices, since they share the same IP subnet address space. Therefore, application level access control at the mirror Web server itself is necessary to prevent guests from accessing services on it. Likewise, the ASA firewall guest DMZ interface ingress policy could be modified to allow traffic from a virtual client—such as a Citrix or VMware client—inbound to internal Citrix or VMware servers. Again, the ASA firewall policy would not be able to distinguish between true guest devices and employee personal devices, since they share the same IP subnet address space. Application level access control at the Citrix or VMware server would be necessary to prevent guests from accessing these servers.

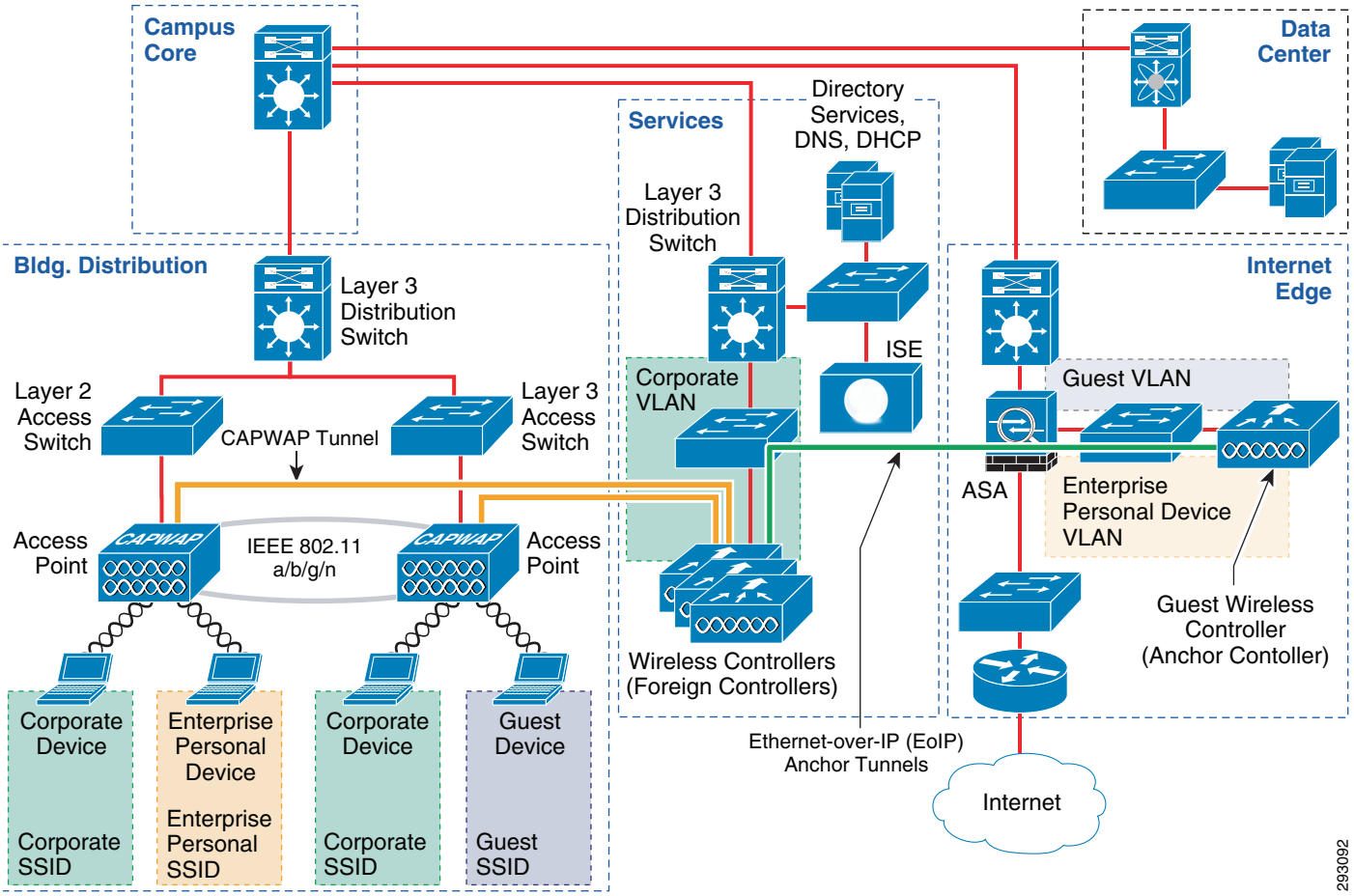
Since the guest SSID is typically open with no encryption, traffic from employee personal devices will be in the clear, unless the devices use either secure applications or some form of VPN tunneling, which encrypts the traffic. Although Web traffic can be made secure simply by requiring the use of HTTPS, not all applications used by employee personal devices may be encrypted. This leaves some vulnerability which must be considered by security operations personnel, especially any site that authenticates using the employee's corporate login and password. If internal company data is being accessed from employee personal devices via the guest wireless network, then that information should be encrypted to prevent eavesdropping. Allowing employee devices to launch a VPN client to establish an IPsec VPN session—either directly to the ASA firewall or out to the Internet and back to another corporate VPN concentrator—may be one alternative. Another option is the establishment of an SSL VPN tunnel to the ASA firewall for employee devices. Both of these options may also require per-user authentication.

Note Cisco's implementation of Web Auth uses HTTPS when redirecting the Web session and requesting credentials.

Because of these concerns, security operations personnel may be hesitant to allow anything but Internet access for any device accessing the guest network, whether it is a true guest device or an employee personal device.

This section discusses another option in which a second guest-like wireless SSID is provisioned for employee personal devices. This SSID is auto-anchored to another DMZ segment off of the ASA firewall, in a similar fashion as the wireless guest SSID. An example is shown in Figure 230.

Figure 230 Example Guest-Like Wireless Access for Employee Personal Devices



With the auto-anchor mobility feature of Cisco wireless controllers, packets from the wireless client are encapsulated through a mobility tunnel using Ethernet-over-IP between the internal wireless controller (known as the foreign controller) to the guest wireless controller (known as the anchor controller), where they are de-capsulated and delivered to the wired network.

Note In this version of the design guide, it is assumed that employees with personal devices would need to manually associate with this SSID. Future versions may investigate other alternatives that make use of RADIUS change-of-authentication (CoA) functionality or device profiles.

An advantage of this option is that the employee personal device SSID does not have to be configured with open access and can be encrypted, unlike the guest SSID discussed throughout this design guide. Instead, the employee personal device SSID can be secured via mechanisms such as 802.1x authentication and WPA-2/AES encryption to prevent eavesdropping of traffic from employee personal devices. Employees can be authenticated via the Cisco ISE server using the external Microsoft AD identity source as they associate with the SSID.

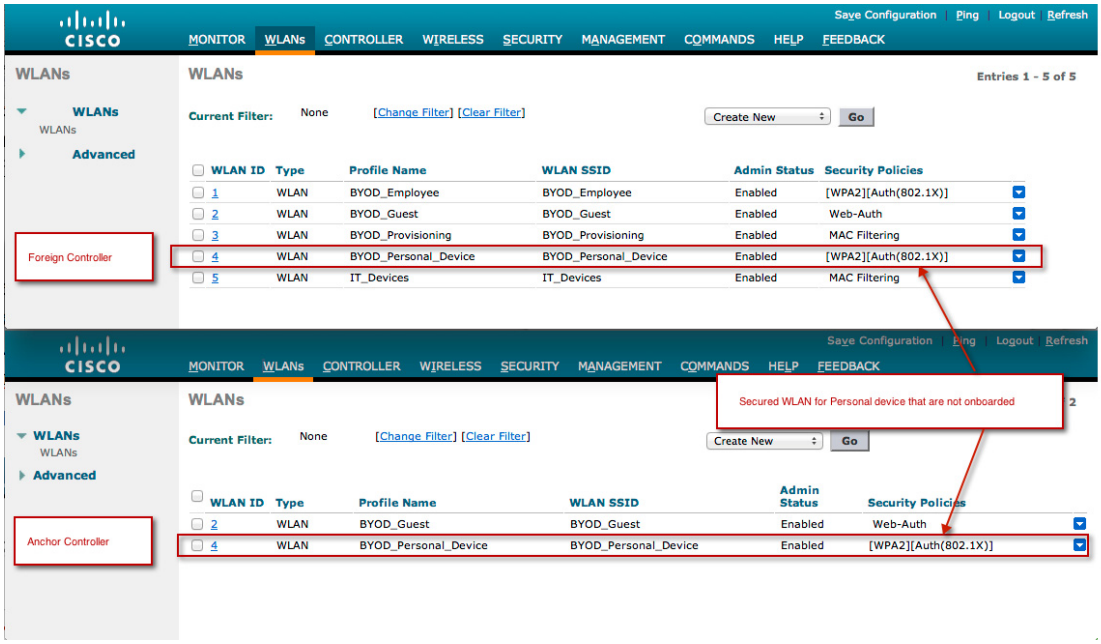
Another advantage of this option is that employee personal devices can be isolated from guest devices by provisioning separate VLANs for each SSID. Separate DMZ segments—implemented as separate physical interfaces off of the ASA firewall or as separate VLAN sub-interfaces off a single physical interface of the ASA firewall—can be deployed. Each DMZ interface now has a separate IP subnet address space and a separate access-control policy. This expands the IP addressing space deployed for

guest devices as well as employee personal devices and removes the issue of employee personal devices causing IP address starvation issues for guest devices and vice-versa. The guest DMZ can be configured to allow only Internet access for guest devices. The employee personal device DMZ can be configured to allow Internet access, as well as access to a mirror Web server sitting on another DMZ segment. Additional access can be allowed by modifying the ASA firewall personal device DMZ interface ingress policy to allow traffic from a virtual client—such as a Citrix or VMware client—inbound to internal Citrix or VMware servers. Access can also be extended by allowing employee personal devices to launch a VPN client to establish an IPsec VPN session, either directly to the ASA firewall or out to the Internet and back to another corporate VPN concentrator. Another option is the establishment of an SSL VPN tunnel to the ASA firewall for employee personal devices.

Wireless Controller Configuration

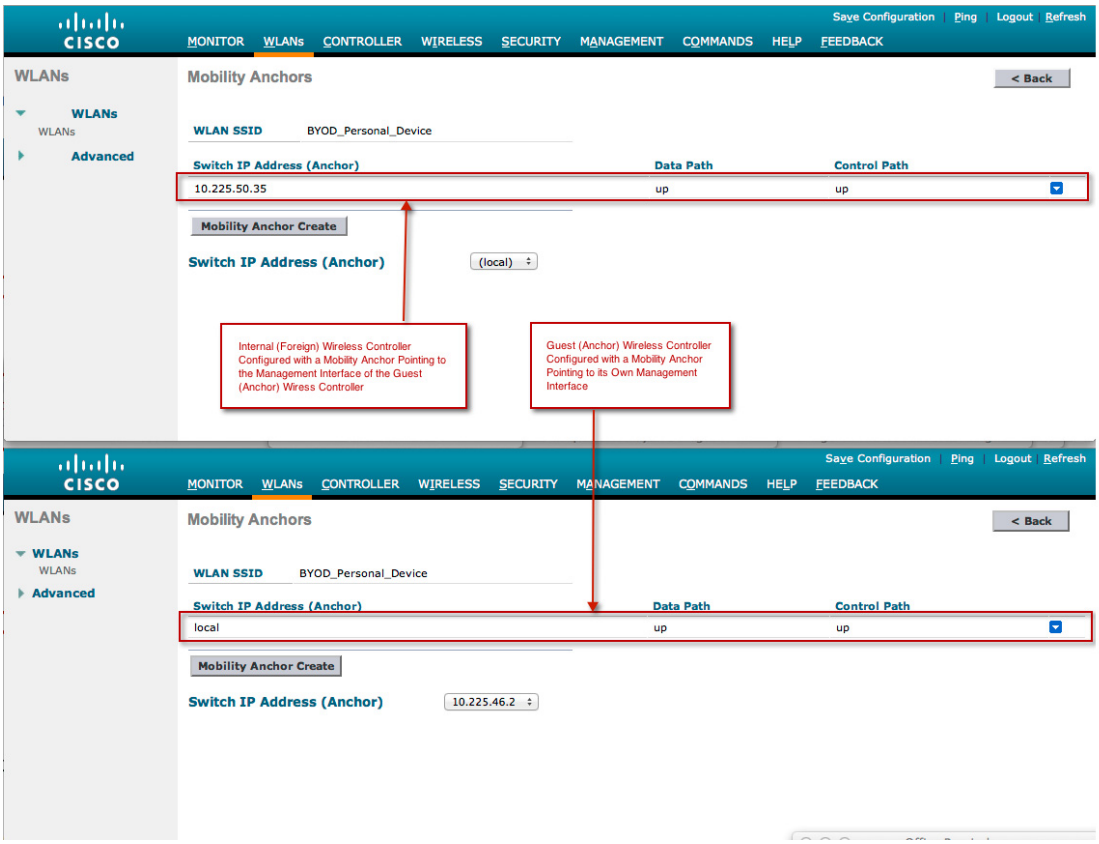
To deploy this option in which a second guest-like wireless SSID is provisioned for employee personal devices, both the internal wireless controllers and the guest wireless controller need to be configured with a new WLAN for employee personal devices, with a unique SSID different from the corporate WLAN and the guest WLAN. An example is shown in Figure 231, in which the new WLAN is called the Employee_Personal_Devices_WLAN.

Figure 231 Example Configuration of the Wireless Controllers for the Employee Personal Devices WLAN



The internal (foreign) wireless controller needs to be configured with a mobility anchor pointing at the management interface of the guest (anchor) wireless controller. In branch scenarios, the controller servicing branch APs will be the foreign controller for the branch personal device WLAN. The guest (anchor) wireless controller can be used as the anchor for both foreign controllers and needs to be configured with a mobility anchor pointing at itself. An example is shown in Figure 232.

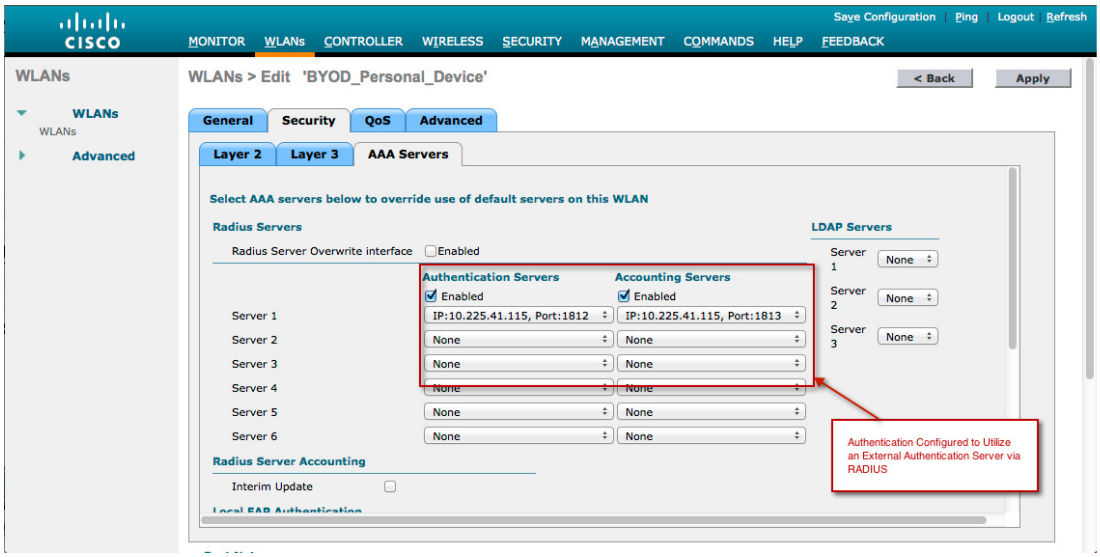
Figure 232 Example Configuration of Mobility Anchors on the Wireless Controllers



The mobility anchors establish the mobility tunnel through which packets from the wireless client are automatically encapsulated and sent from the internal wireless controller (foreign controller) to the guest wireless controller (anchor controller), where they are de-capsulated and delivered to the wired network.

The network administrator must also configure the employee personal devices WLAN to use RADIUS within both the internal wireless controller and the guest wireless controller for authentication. This is shown for the internal wireless controller in Figure 233.

Figure 233 Authentication via RADIUS for the Employee Personal Devices WLAN

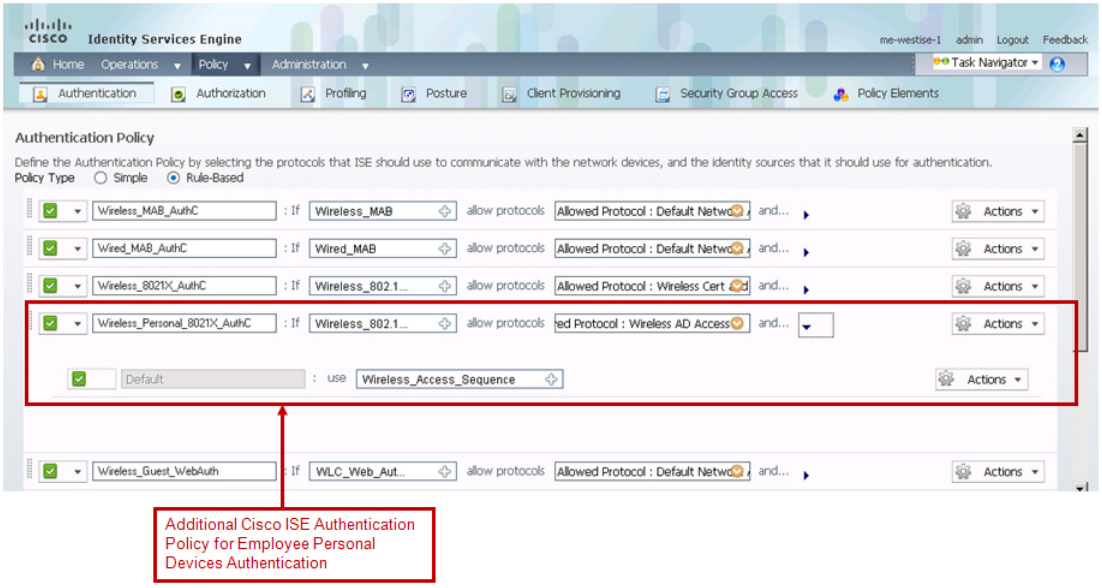


Since Web Auth is not involved with this option, there is no redirection of Web sessions to a guest portal and hence no configuration required within the guest wireless controller for Web Auth or any requirement for a pre-authentication ACL. When an employee personal device connects to the SSID, the RADIUS session is initiated by the internal (foreign) wireless controller management interface to the Cisco ISE server for authentication and authorization. Upon successful authentication, the employee's personal device is then anchored to the guest (foreign) wireless controller.

Cisco ISE Policy Configuration

From a Cisco ISE policy perspective, an additional authentication rule needs to be added to the Limited Access BYOD design policy. This rule allows wireless controller Web authentications, originated from the employee personal devices SSID, to utilize a separate Cisco ISE user identity sequence for wireless employee personal device access. An example of such a policy rule is shown in Figure 234.

Figure 234 Example of Cisco ISE Authentication Policy Allowing Wireless Employee Personal Device Access



292742

The logical format of the authentication policy rule for this example is:

```
IF (Wireless_802.1X AND Wireless_Personal_8021X_AuthC)
    THEN (Allow Wireless AD Access AND USE Wireless_Access_Sequence)
```

Wireless_802.1x is a system-generated compound condition that is used here to match 802.1x-based authentication requests from Cisco wireless controllers. It matches the following two standard RADIUS dictionary attribute-value (AV) pairs:

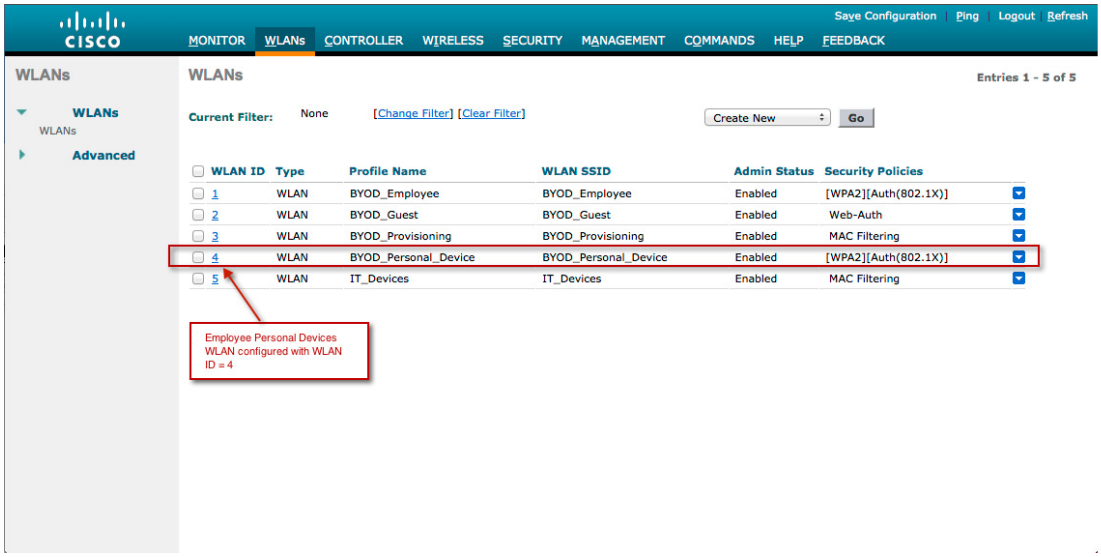
```
Service-Type - [6] EQUALS Framed
NAS-Port-Type - [61] EQUALS Wireless - IEEE 802.11
```

Wireless_Personal_8021X_AuthC is a user-defined simple authentication condition for users of non-on-boarded employee personal wireless devices that access the network via a secure guest-like SSID. It matches the following RADIUS AV pair from the Airespace dictionary:

```
Airespace-Wlan-Id - [1] EQUALS 4
```

The Airespace-Wlan-Id is the identification number (WLAN ID) of the Employee Personal Devices WLAN for this example, as shown in Figure 235.

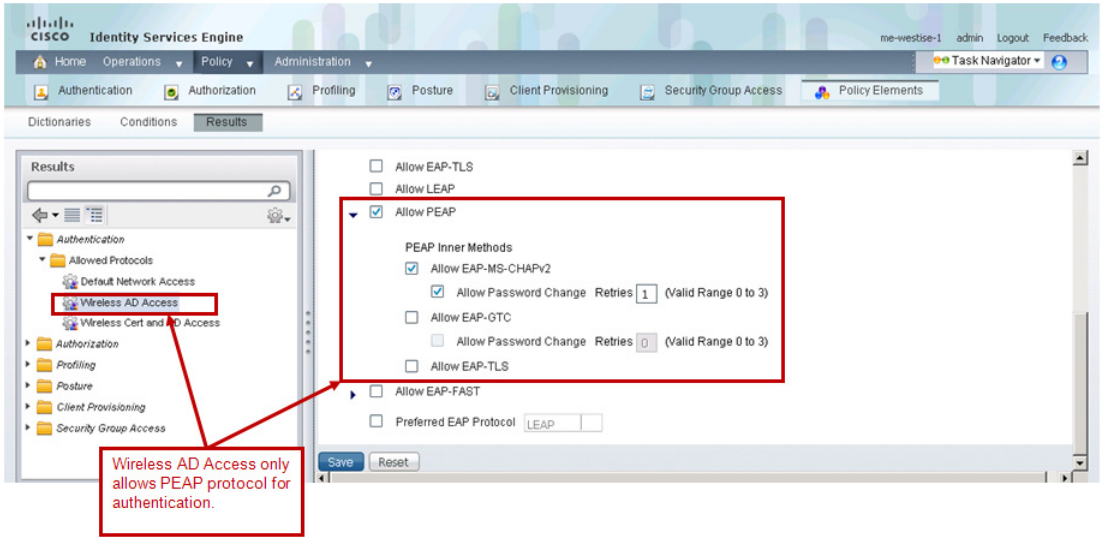
Figure 235 Example Wireless Controller WLAN IDs Showing Employee Personal Devices WLAN and SSID



This allows the ISE authentication policy to differentiate 802.1x requests coming from the SSID corresponding to the employee personal devices WLAN and apply a different policy outcome.

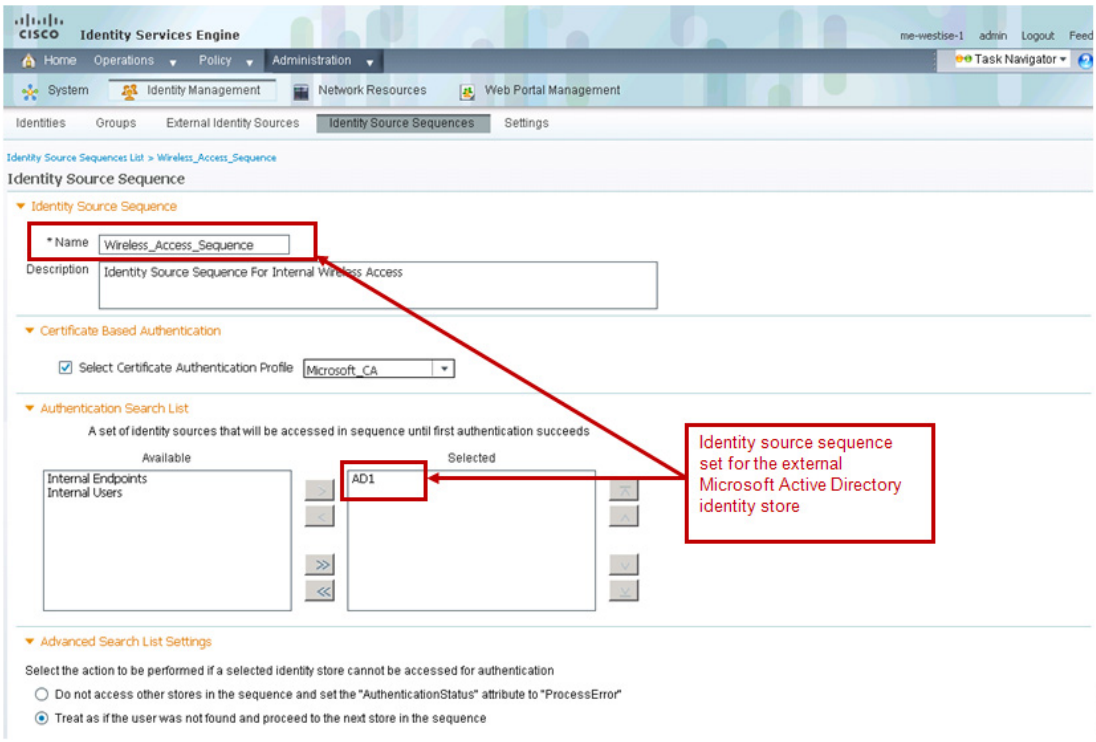
Wireless AD Access is a user-defined authentication result, which allows only the PEAP protocol to be used for authentication. Note that additional protocols can be selected as needed. This example simply uses PEAP for illustration purposes. An example is shown in Figure 236.

Figure 236 Example of Allowed Protocols Under Wireless AD Access



Wireless_Access_Sequence is a user-defined identity source sequence. An example is shown in Figure 237.

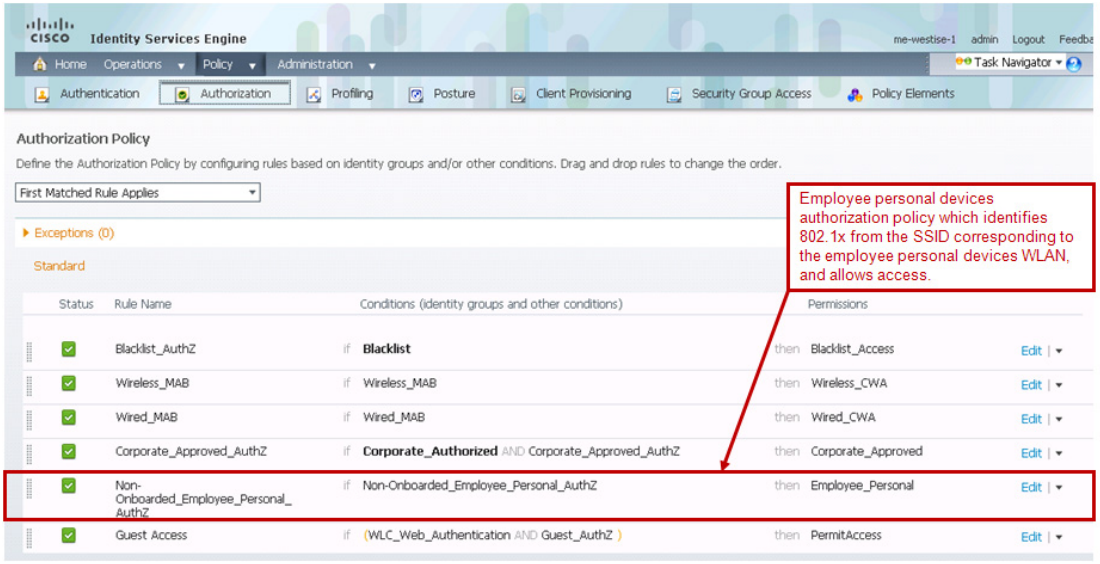
Figure 237 Example of Wireless_Access_Sequence Identity Source Sequence



Wireless_Access_Sequence in the example above uses the AD1 identity source only. This corresponds to the Microsoft Active Directory identity store, where employee credentials are typically held within an organization. Although an identity source sequence is not strictly needed when only a single identity source is specified, configuring a sequence allows it to be easily extended to include additional identity sources if needed.

From a Cisco ISE policy perspective, an additional authorization rule also needs to be added to the Limited Access and Restricted Access BYOD design policies. This rule permits access for wireless controller 802.1x authentications originated from the SSID corresponding to the employee personal devices WLAN. An example of the policy rule is shown in Figure 238.

Figure 238 Example of Cisco ISE Authorization Policy Allowing Wireless Employee Personal Device Access



The logical format of the authorization policy rule for this example is:

```
IF (Any AND Non-Onboarded_Employee_Personal_AuthZ)
    THEN apply the Employee_Owned authorization result
```

Any is a system-generated authorization condition which literally means any device.

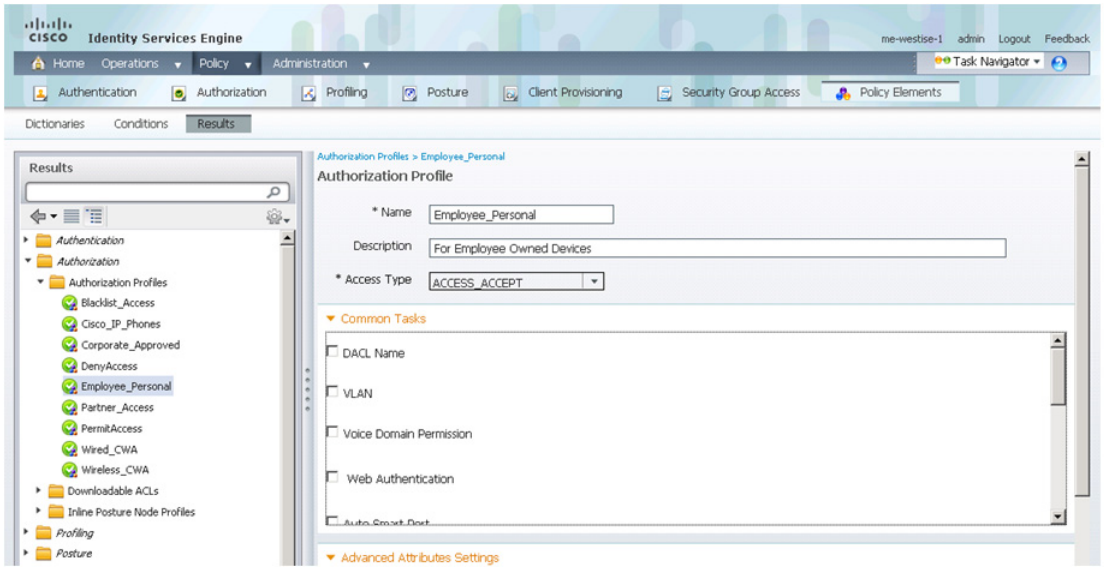
Non-Onboarded_Employee_Personal_AuthZ is a user-defined simple authorization condition for users of non-onboarded employee personal devices that access the network via WLAN corresponding to the employee personal devices SSID. It matches the following RADIUS AV pair from the Airespace dictionary:

```
Airespace-Wlan-Id - [1] EQUALS 4
```

The Airespace-Wlan-Id is again the identification number (WLAN ID) of the WLAN corresponding to the employee personal devices SSID. This was shown in Figure 235. This rule allows the ISE authorization policy to differentiate 802.1x authentication requests coming from the employee personal devices SSID and provides a different authorization result profile named Employee_Owned.

The Employee_Owned authorization result profile for this example simply permits access. A partial view of the authorization result profile is shown in Figure 239.

Figure 239 Example of an Authorization Result Profile for Employee Personal Devices

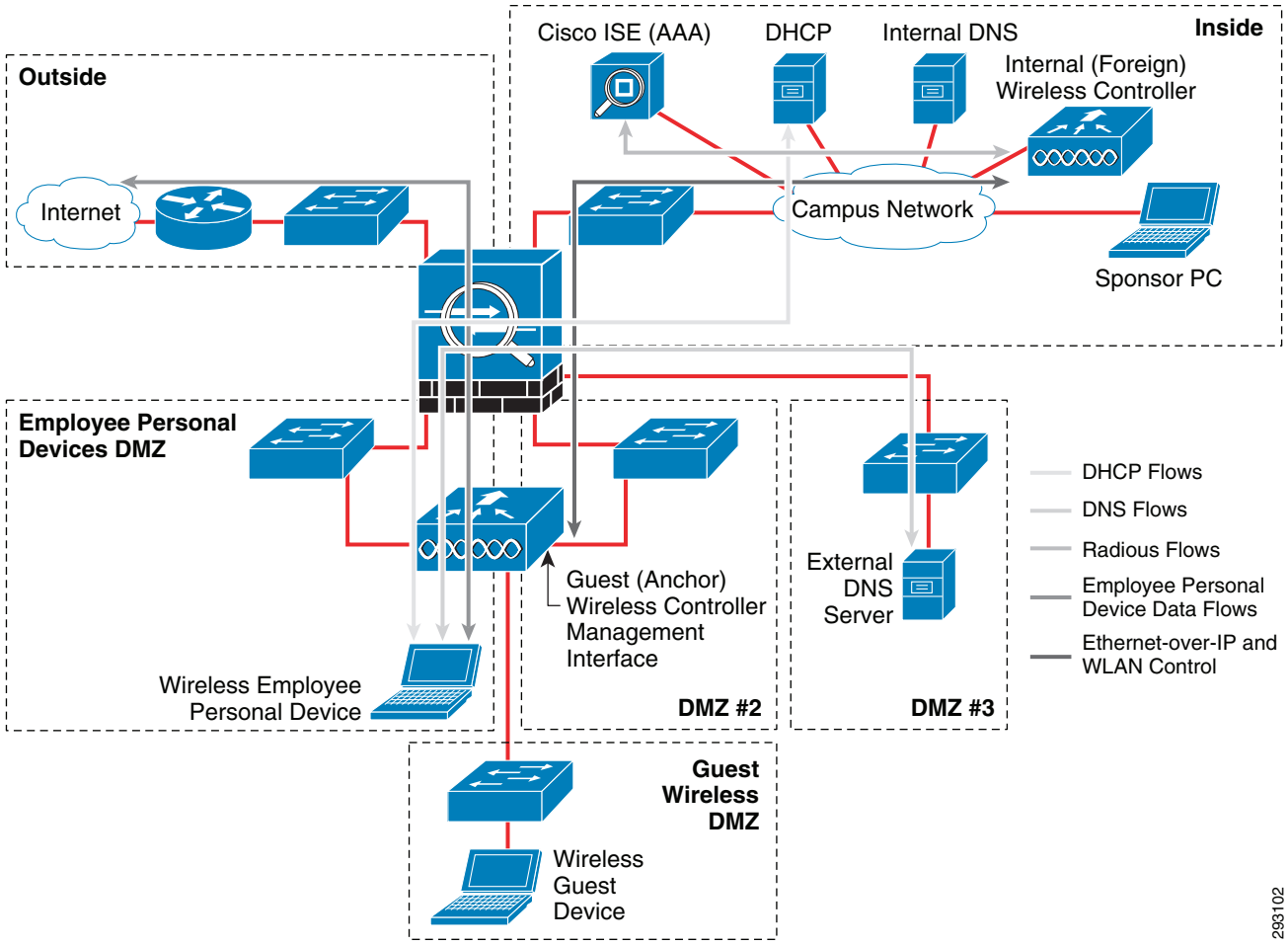


It is the functional equivalent of the system-generated PermitAccess authorization result profile. It is included here simply for illustrative purposes to point out that the authorization result can be modified to include restrictions, such as an access-control list (ACL) applied to the employee personal device as it connects to the WLAN.

ASA Firewall Configuration

Figure 240 shows an example of the flows that need to pass through the Cisco ASA firewall to support this option.

Figure 240 Example of Flows that Need to Pass Through the Cisco ASA Firewall for Employee Personal Devices



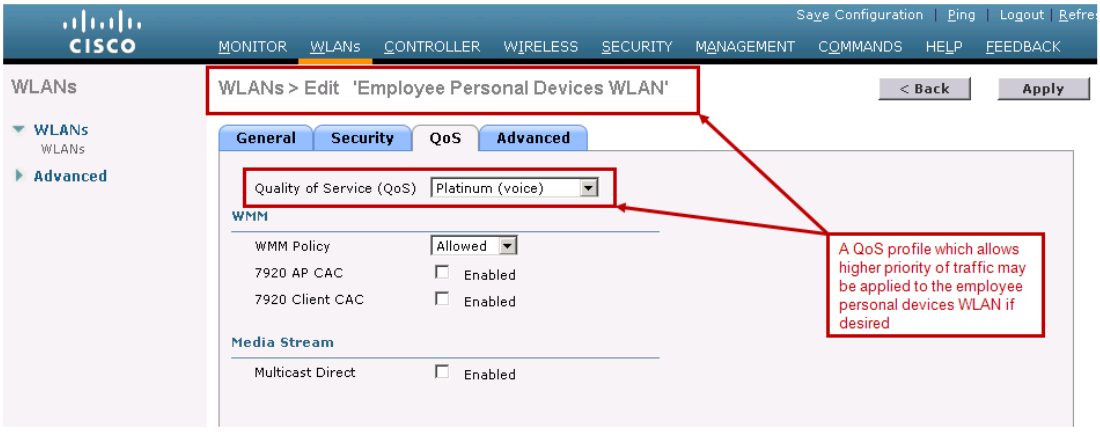
The RADIUS session is initiated by the internal (foreign) wireless controller management interface to the Cisco ISE server for authentication and authorization. Therefore, it does not need to be allowed through the ASA firewall for employees who are authenticating with personal devices. An Ethernet-over-IP (IP port 97) auto-anchor mobility tunnel, as well as the WLAN control port (UDP port 1666) between the management interfaces of the two wireless controllers, must still be allowed through the ASA firewall. Besides allowing DNS and DHCP (assuming the deployment of an internal DHCP server), the ASA firewall should be configured to block all other traffic generated from employee personal devices onto the internal network. Additional ports can be opened to accommodate the access of corporate resources as discussed in the following section and summarized in Table 13.

Note Additional ASA firewall ports may need to be opened to accommodate guest wireless access, depending upon the deployment model discussed in BYOD Guest Wireless Access.

Differentiated Quality of Service Treatment

With this deployment model, a separate QoS policy can be applied to employee personal devices, different from guest wireless devices. This is because wireless employee personal devices are terminated on a separate WLAN from wireless guest devices. As of Cisco Wireless Controller software version 7.2, QoS is applied per WLAN by way of a profile, as shown in Figure 241.

Figure 241 Example of QoS Profile Applied to a WLAN



This may be desirable if employee personal devices are going to be allowed to run virtual desktop client applications such as a Citrix client or VMware client or if employee personal devices run collaboration clients such as Cisco Jabber.

Note BYOD Guest Wireless Access discusses rate limiting per-SSID and per-User. These features can be used for Employee Personal Devices as they were for Guest. Rate limiting is configured on the foreign controller and not the anchor controller.

Accessing Corporate Resources

Because employee devices are associated to the network from a DMZ interface, which is effectively outside of the corporate firewall, they do not have access to company resources located inside the firewall. This may be perfectly acceptable and desirable. Employee devices still have access to the public Internet. This enables them to connect to cloud-based resources such as Cisco WebEx or partner Web sites. The employee device is afforded some level of usability, making the device useful as a productivity tool.

Companies may want to offer access to additional resources but still maintain the security offered by restricting employee devices to the guest side of the firewall. There are various options available to accomplish this objective, including:

- Setting up a mirror of the company website
- Allowing VPN access
- Allowing virtual desktop client access

Securing Mirror Sites for Personal Devices

One approach to bringing services to employee personal devices accessing the guest network is to set up a mirror of the company website in another DMZ segment, referred to as an employee device security zone (EDSZ) within this section. If employee personal devices connect to the guest wireless network, the website will only be accessible after the user has completed the Web Auth process and accepted an Acceptable Use Policy (AUP) or End User Agreement (EUA). This website does not need to be an exact match of an internal website, but could contain relevant content that employees can use on their personal

devices to make them more effective. In addition, the website could include content optimized for smaller mobile displays. Examples of applications that could be offered in the EDSZ include access to E-mail, a team wiki page, or the company news site.

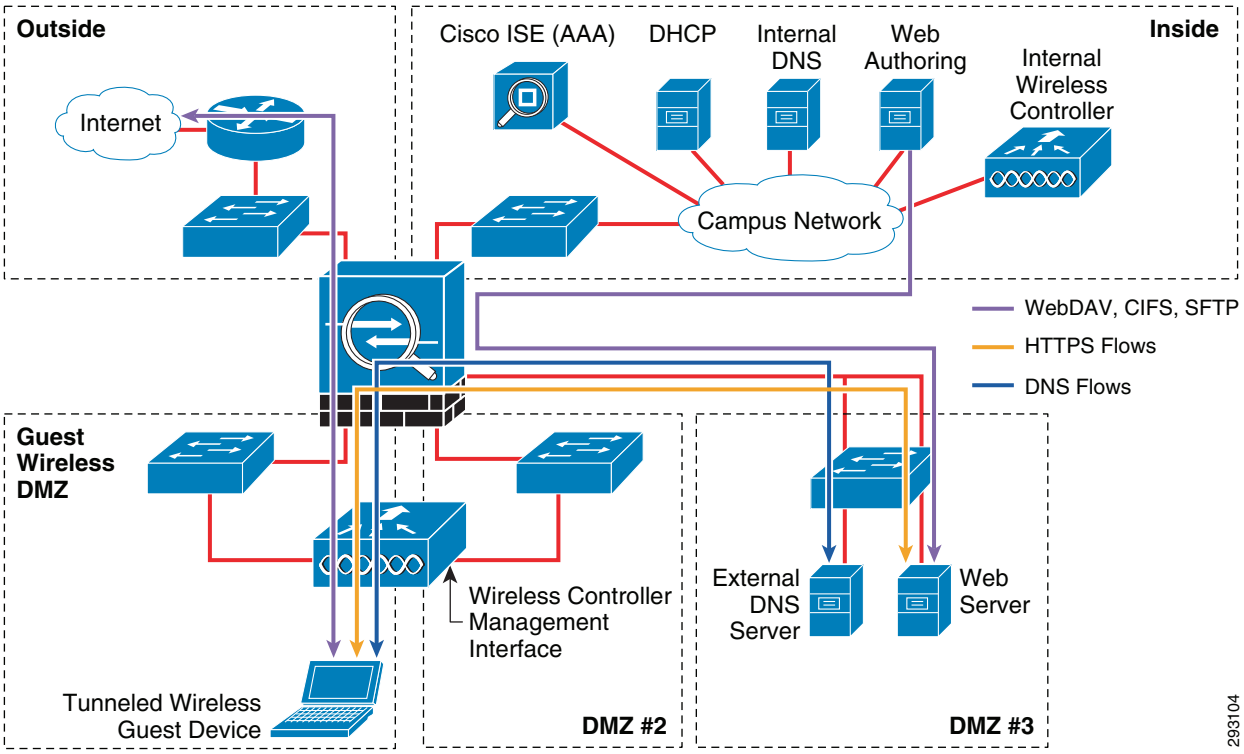
There are several methods available to setup a secure website. In general, the deployment is very similar to a typical DMZ Web service, except that rather than residing in an Internet facing DMZ, the server is located on a subnet accessible by employee personal devices. The intent of this section is not to provide detailed guidance on the deployment of a presentation server, application server, and database server. Site administrators should be familiar with the approach that best fits their security environment. Some high level considerations when setting up the server include:

- Dual attachment—Usually this is considered to be more secure. The client-side NIC should implement firewall services that allow inbound connections on TCP port 80 or 443. Only session requests initiated by the client subnets should be allowed towards the server. Session requests initiated by the server should not be allowed towards the client subnets. If the employee device wireless network is encrypted, then some organizations may be comfortable allowing users to attach via HTTP.
- The back-end NIC should be used to move content between the server and the data store or application server. It may also be allowed for remote administration of the site. Single-attached servers are possible although usually a dedicated and secured gateway is setup for the server-to-server communications that is separate from the server-to-Web client gateway.
- Content Delivery—Generally content is either static or dynamic. Static content can be pushed overnight or as needed to keep the website current. Dynamic content could allow the employee device to post information to the site. The website could use a local data store that is synchronized with an external data store or have a secured channel to an application server.
- User Authentication—Some method should be used to ensure only authorized and authenticated users are able to view site content. Utilizing Microsoft Active Directory or a local user database are two possible methods. Active Server pages (ASP.NET) can also be used to leverage the login controls used with Microsoft Internet Information Server (IIS) servers and provide a more sophisticated authentication model such as single sign-on (SSO). Local databases are easier to setup but require a high level of administrative overhead and are usually only appropriate in very small organizations.
- Secure Sockets—Websites in the employee device security zone (EDSZ) should implement secure socket layer (SSL) or transport layer security (TLS) if employees are sending sensitive information, such as their login credentials. This can be relaxed somewhat if the EDSZ has been implemented with wireless encryption. On the other hand, if employee devices reside in the traditional guest network where wireless packets are not typically protected with encryption and are co-mingled with actual guest traffic, then SSL/TLS websites are needed. This is particularly important if employees are passing their corporate credentials to a mirror website.
- Web Server software—There is a wide range of Web server software available. Deciding which type of server to deploy impacts what security features are available. Common choices include Microsoft IIS, Apple, and Tomcat. Wikipedia has a comparison of Web server software that can illustrate the choices available (http://en.wikipedia.org/wiki/Comparison_of_web_server_software). It is also possible to host sites on a secure cloud service. This service could be restricted to IP addresses or require client side certificates. With proper security precautions, a cloud-based site could also allow mobile employees access to some traditional corporate resources such as payroll or benefits that are increasingly finding their way to the cloud.

Figure 242 illustrates a simple scenario where static content is deployed in a DMZ dedicated for employees using personal devices. A Windows 2008 server is deployed with Microsoft IIS 7.0 as well as some other network services specific to the DMZ, such as DNS and Read-Only Directory Services (RODS). Users are authenticated against the corporate Microsoft Active Directory server. The RODS service requires DNS to be installed on the same server. The Web server is typically a dedicated box.

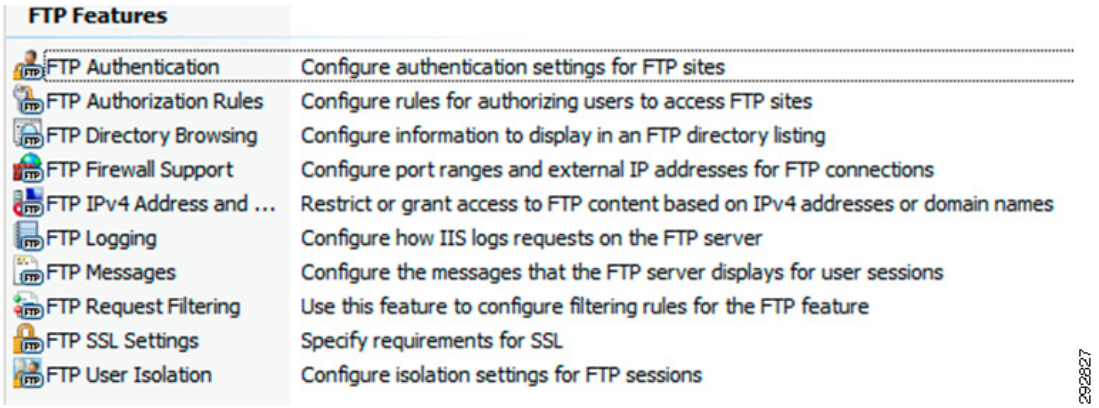
However, in some situations it may be desirable to run RODS and IIS on the same server to simplify basic authentication using Microsoft AD. It is more appropriate when supporting a small-to-modest number of employee devices.

Figure 242 Example of a Mirror Web Site for Employee Personal Devices



Moving content to the secured server can be done by various means. One approach is to use FTP, however because FTP is not secured, a better approach is to use either SFTP or FTP over SSL. By default, Microsoft IIS does not ship with a secure FTP server. Microsoft supports FTP over SSL rather than SFTP. Administrators must copy the installation package from Microsoft's Web site (http://learn.iis.net/page.aspx/310/what-is-new-for-microsoft-and-ftp-in-iis-7/) and install the feature on their server. If FTP is already running, the administrator needs to deselect the FTP feature from the services manager prior to installing the FTP over SSL server. The improved FTP over SSL server offers additional tools not available in the standard FTP package that are used to manage access to the FTP site, as shown in Figure 243.

Figure 243 Example of Tools Available with the FTP over SSL Server



Anonymous authentication should be disabled and at least basic authentication should be enabled. There are other options that may be appropriate from some organizations.

Instead of FTP over SSL, administrators can choose to use Web Distributed Authoring and Versioning (WebDAV). This method offers more flexibility than FTP because many operating systems allow the connection to be mounted to the file system. By providing a directory handle, Web authoring applications as well as other applications can directly use the secured pipe. WebDAV is based on HTTP or HTTPS and provides the ability to authenticate and encrypt data. If employees are placed directly in the guest SSID, then WebDAV HTTPS should be used since passwords are sent. If employee devices are placed in an encrypted EDSZ, then WebDAV HTTPS could be used to provide an additional layer of encryption. The security considerations are detailed in section 20 of RFC4918.

Another option similar to WebDAV is CIFS. This protocol also allows local directory mounts of the remote site. It is commonly found in Microsoft environments, although Samba is available for non-Windows servers. Microsoft has also released SMB2 with Vista, which is an update to CIFS. There are several other approaches that provide a secure path between either the Web authoring site or the application server. A particular enterprise will likely leverage the same methods as the Web servers located in the traditional DMZ.

DNS Support

The employee devices need access to a DNS server. If the EDSZ Web server is using RODS, then DNS is already available on the Directory Server. It is installed by default when the RODS is setup unless the administrator explicitly chooses not to. Dynamic updates are secured and zone transfers are not enabled. If the Web server is not using AD for employee authentication, then DNS will be a standalone service.

Outlook Web Access for Employee Devices

E-mail is a foundational service that can be offered to employee devices. This can be accomplished by deploying a Web interface to the mail server such as Outlook Web Access (OWA) or ActiveSync for exchange environments. Some enterprises may already be offering this service for employees that need E-mail while traveling. In this case, the employee devices can continue to use the current Internet facing OWA server.

Microsoft does not support the OWA server in a DMZ zone. Instead, the OWA server should be behind the firewall. Holes can be opened for port 443. Another option is to setup Apache in the EDSZ as a reverse proxy. The Microsoft recommended approach is to run OWA on the client access server (CAS) and publish the CAS with Microsoft's Internet security and acceleration (ISA) server into the EDSZ.

This is a full blown deployment and may not be appropriate as a method to grant employee personal device access due to the complexity involved versus other methods, such as simply opening a hole in the EDSZ DMZ firewall for HTTPS to the enterprise CAS.

Another option is subscribing to Office365, which is Microsoft's cloud-based Exchange and Office environment. In this case, employees would use the public Internet service to gain access to their E-mail or other cloud-based enterprise resources. At this time, there is not a native Office365 application for either Android or iOS devices and users would be restricted to HTTPS access unless they were using a Windows 8-based mobile device. This method would also allow Direct-To-Cloud over 3G/4G or off-premise accesses to the same resources. Microsoft is only one of many cloud based enterprise environments offering E-mail services.

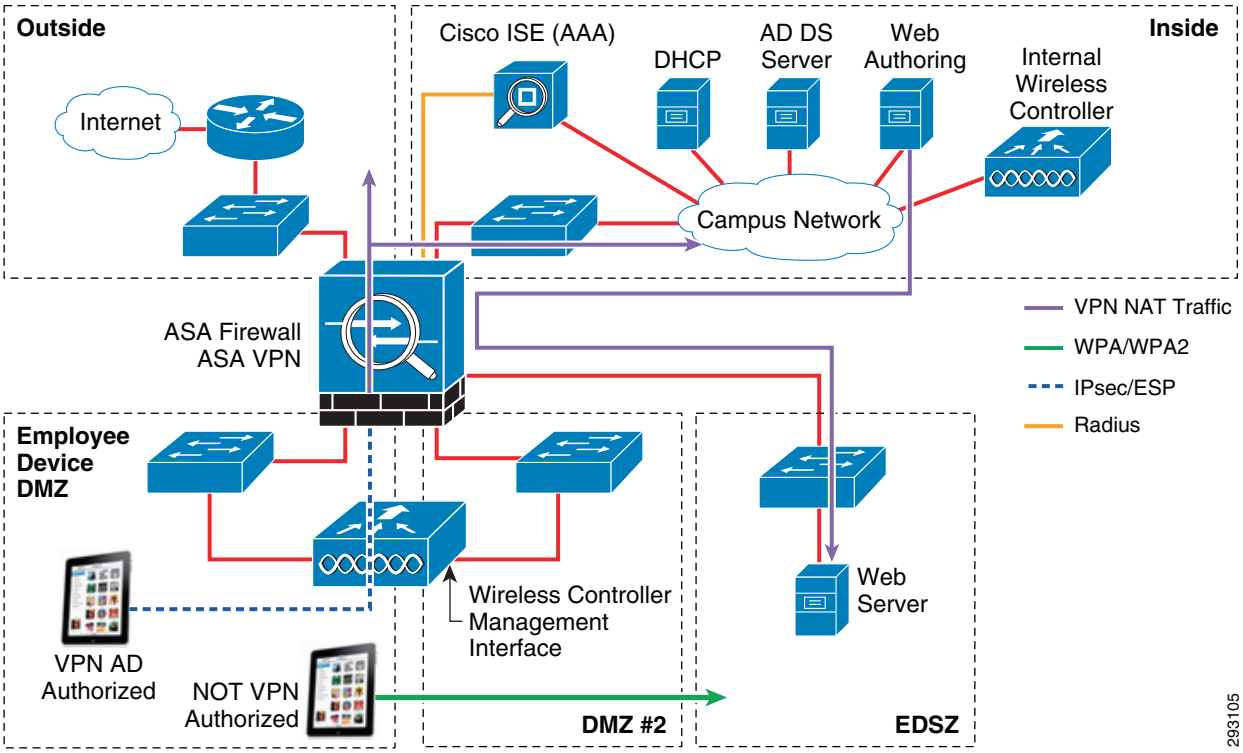
ActiveSync Support

Future versions of this document will discuss mobile device managers (MDM) that are used to manage the configuration profiles of mobile devices and provide additional security features needed for lost or stolen devices. Some of the MDM functionality is licensed from Microsoft, including remote-wipe, pin-lock enforcement, and others. ActiveSync is used to synchronize E-mail, calendar events, and contacts between the Microsoft Exchange server and the mobile device's E-mail application. Administrators may be interested in providing ActiveSync to devices in the employee device security zone (EDSZ). When properly configured and certified, ActiveSync can also provide the MDM security features mentioned previously. Providing this support is similar to OWA. The firewall policy in the EDSZ can be set to allow connections to ActiveSync on the CAS that may be published on an ISA server. ActiveSync is supported by WebDAV and should be used over HTTPS (TCP port 443).

VPN Client

Enterprises that restrict employee devices to a guest or dedicated EDSZ may want to allow a subset of these users the ability to launch the built-in VPN client to connect to the secured part of the network. There are two methods that can be employed. First, the device may already have access to the current Internet-facing VPN concentrator. In this case, the employee device would connect from the guest network out through the public Internet and then back in to the Internet DMZ where the VPN concentrator is located. If employee devices are co-mingled with actual guest traffic, then this may be the best approach. However, if a dedicated and secured SSID is deployed behind an ASA firewall specifically for employee personal devices, then this firewall could also provide VPN access for some privileged users. Alternatively, a dedicated VPN concentrator could be located in the EDSZ. After the device authenticates and joins the secured wireless domain, these users would connect to the VPN concentrator to gain additional secured access. Only employee devices in the dedicated security zone can reach the concentrator. The general layout of the network components are shown in Figure 244.

Figure 244 Employee Zone VPN Network Components



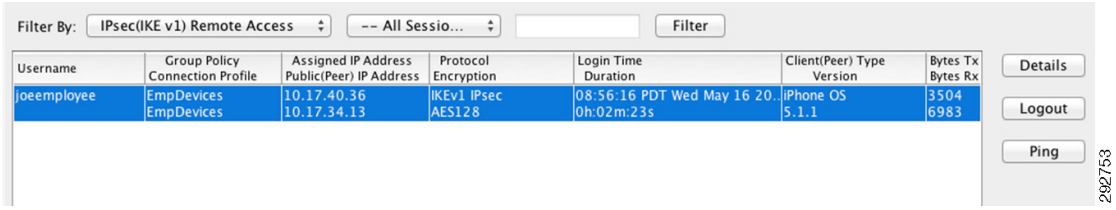
Apple iOS devices include a built-in Cisco IPSec client allowing ESP tunnel mode and XAUTH. Both Apple and Android devices offer L2TP with IPsec and pre-shared key (PSK). The ASA can be setup to accept both types of VPN clients. For this discussion, the focus is the Cisco VPN client found on Apple iOS devices.

The employee needs to know the name of the VPN concentrator, group, and group secret to configure the VPN client. Future version of this document will illustrate how the VPN configuration can be pushed to the employee device without user intervention. Certificates can also be pushed to the employee device to further secure access to the VPN concentrator. The use of certificates negates the need for a group and group secret.

Figure 245 iOS VPN Client Configuration

When the user connects to the VPN concentrator, they are asked for their Microsoft AD credentials. This information is passed by the Cisco ASA to the Cisco ISE server, where a policy decision can be made. This decision can include attributes from Microsoft Active Directory or any of the other parameters Cisco ISE can use to determine policy. If the user is authenticated and authorized by Cisco ISE, the ASA completes the VPN connection. Once connected, the ASA can apply additional security and access restrictions to the tunnel, further controlling what resources the employee device can reach. The ASA can also be used to monitor who is using the VPN portal, as shown in Figure 246.

Figure 246 ASA Management for VPN Connections



ASA provides additional information for managing VPN connections.

Virtual Desktop Client

Another available deployment model is to allow a virtual desktop to run on the employee device. The actual applications and associated data remain on the secured hosting server. Once the device disconnects from the network, the data is typically no longer available to the user. The enterprise can control which users are able to launch a virtual desktop and what applications are available on that desktop. The firewall between the EDSZ and the hosting server can be configured to allow specific connections.

There are a wide range of possibilities. In its simplest from, the employee could use VNC to connect back to their desktop or a dedicated server. A VNC client is available for both iOS and Android devices. This may be adequate for some small environments where availability and manageability are not a top priority. By default, the connection is not encrypted, which is a concern. Administrators may not have the necessary control over which applications are available on the hosting server. Employees may be tempted to attach to their desktop and E-mail back sensitive data to an external account. This temptation only arises as a means to bypass IT policy and should be considered before allowing remote desktops to attach to employee deployed VNC servers. The use case for employee devices with virtual VNC desktops needs careful review. The employee is likely sitting in front of the actual desktop, with a full keyboard and mouse and likely does not need a remote desktop. The best approach may be to block TCP port 5900 from traversing the firewall to unknown destinations.

Cisco offers the Virtual Experience Infrastructure (VXI) and partners with several companies that offer a virtual desktop on mobile iOS and Android devices including VMWare View, Citrix, and WYSE. Virtual desktops on employee devices are best suited in VXI environments where a centralized UCS server is securing and managing sessions. With VXI in place for corporate devices, extending access to employee devices may allow productivity gains. This can be done by opening the firewall to allow a connection to specific and well known servers. Beyond BYOD, virtual desktops are compelling because of the reduction in IT costs. Adding tablet support maximizes the benefit because the requirement for employee laptops is reduced. A small and lightweight VDI hardware appliance replaces the traditional desktop and mobile device support un-tethers the employee from the cube. Tablets with virtual desktops can offer much of the same functionality as employee laptops, but at a reduced cost and with stronger tools to address lost and stolen devices plus centralized data security inherent in VXI.

Finally AnyConnect provides a centralized virtual desktop that integrates with the ASA firewall. This is a good approach because security is the foundation of the system. AnyConnect desktops attach to the ASA firewall via SSL. Virtual desktops are evolving in capabilities and will be covered in more detail the next release of this document.

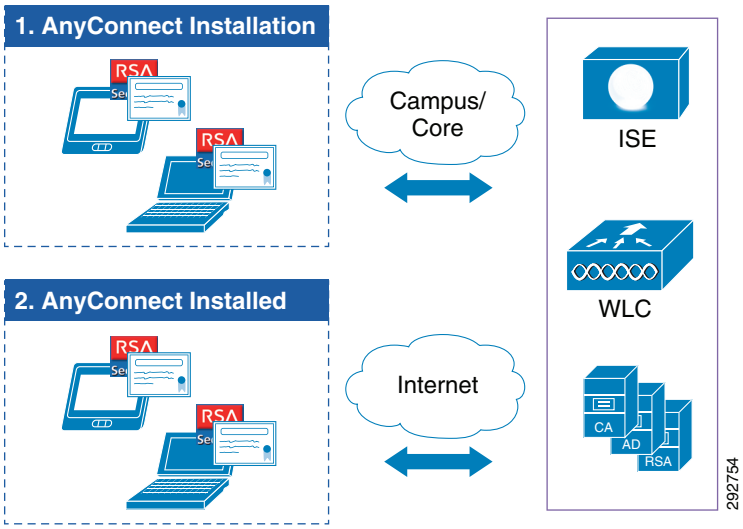
Summary

These types of alternate solutions offer a wide range of options to provide employees compute resources without compromising corporate data. Leveraging the guest environment can serve as part of a migration path to a fully certificate-based BYOD solution. Guest type deployments can be set up fairly quickly without the need to touch a large number of third-party devices and yet still meet the basic requirement of allowing employees to use their personal devices to increase the organization's productivity.

Remote Device Access

A BYOD design should be able to accommodate devices that attempt to connect remotely to access the internal resources. The device could be a workstation, tablet, smartphone, or any other device which is allowed to connect securely to the network. In this design, the Cisco ASA is used as a VPN gateway for establishing an SSL VPN session to the remote endpoints. The ASA authenticates the user's digital certificate. Cisco ISE then authenticates the user via an RSA SecurID token. The combination of both allows the device onto the network. Figure 247 shows the network components involved in remote device access.

Figure 247 Remote Device Network Components



This design assumes the following for providing remote access capability:

- Devices that want to connect to the network remotely must be corporate approved devices. The corporate approved devices are the ones that have been provisioned with a digital certificate by the IT organization. To understand more about corporate approved devices, see Limited BYOD Access.
- Devices must be provisioned at the campus. The provisioning process consists of:
  - Installing the AnyConnect Client
  - Configuring the VPN gateway IP address
  - Setting up one-time-password scheme for the user.

  These steps must be completed at the campus location before it can be used remotely. This design does not allow remote provisioning of the devices.
- Devices connecting remotely are subjected to two factor authentication, which means the user should provide two forms of credentials.

Solution Components

The following components play a role in providing connectivity to remote clients:

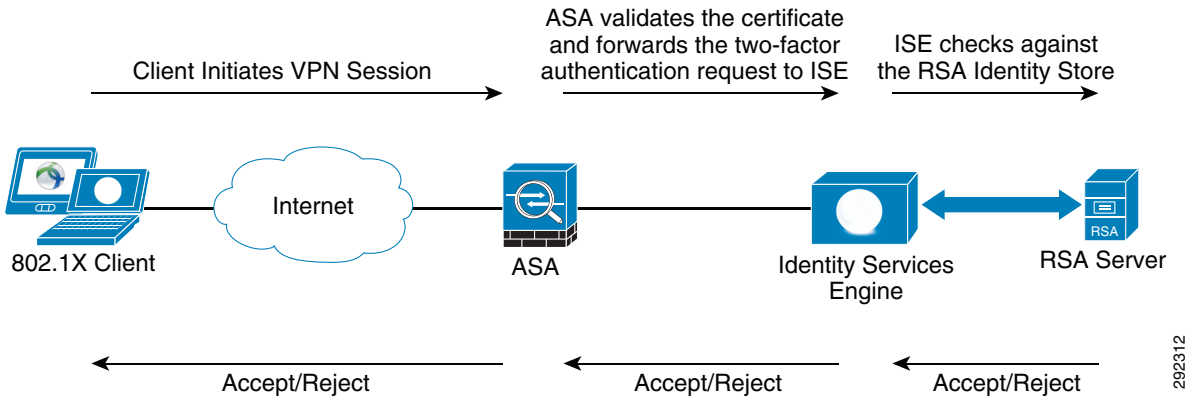
- Cisco Adaptive Security Appliance (ASA)—Functions as an SSL VPN concentrator for terminating VPN sessions.
- Cisco AnyConnect—Acts as a VPN client installed on the remote device.
- Cisco Identity Services Engine (ISE)—Acts as an intermediary to an external identity source for authentication between remote endpoints and the RSA Server. The token gets forwarded from the client to the ASA, from the ASA to the ISE, and then from the ISE to the RSA.
- RSA SecurID—Acts as the authentication server for tokens generated by the client.

RSA SecurID

VPN security is only as strong as the methods used to authenticate users (and device end points) at the remote end of the VPN connection. Simple authentication methods based on static passwords are subject to password "cracking" attacks, eavesdropping, or even social engineering attacks. Two-factor authentication, which consists of "something you know" and "something you have" is a minimum requirement for providing secure remote access to the corporate network. For more details, see: http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html.

This design includes the RSA SecurID Authentication Server 7.1, along with RSA SecurID hardware tokens, to provide two-factor authentication. The passcode that the user presents is a combination of their secret PIN and the one time password (OTP) code that is displayed on their token at that moment in time. This design utilizes both RSA SecurID (two-factor authentication) in conjunction with the deployment and use of x.509 client digital certificates. Figure 248 shows how RSA is used for two-factor authentication.

Figure 248 RSA Used for Two-Factor Authentication

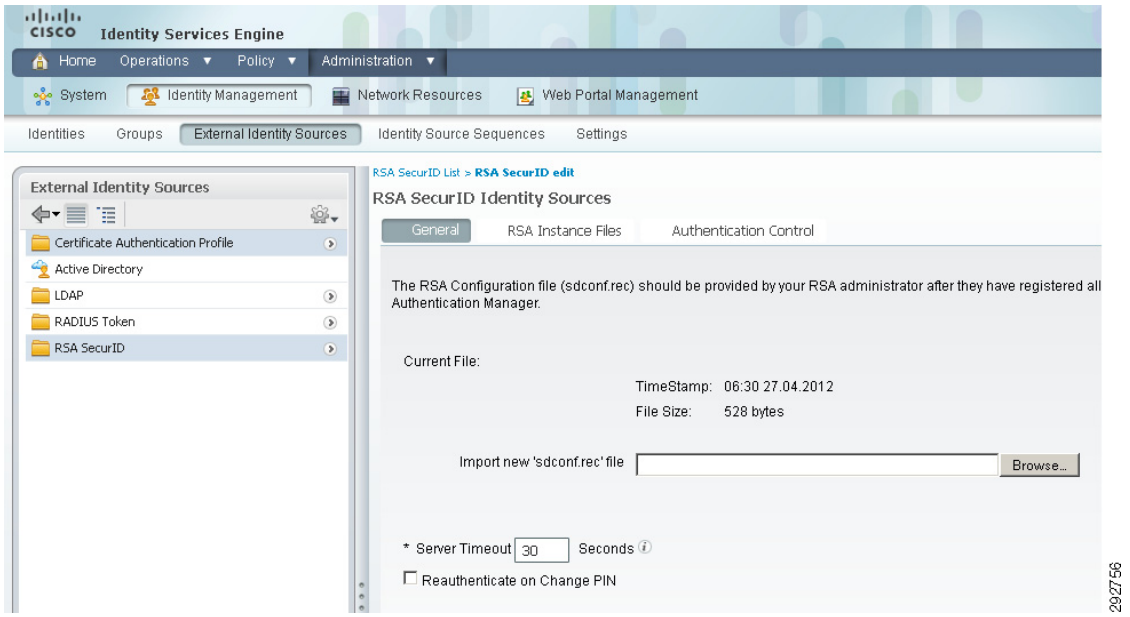


For information on configuring the RSA Secure Authentication Manager, see: http://www.emc.com/security/rsa-securid.htm.

ISE Integration with RSA

The RSA Identity Store is used primarily to authenticate remote users. The remote users are authenticated initially by their digital certificates and then they must provide a one-time password using a RSA SecurID token. To configure the RSA as an identity store, click **Administration > External Identity Sources > RSA SecurID > Add**, as shown in Figure 249.

Figure 249 RSA Server as an Identity Store for ISE



VPN Design Considerations

This section discusses the primary role of the ASA for this design, which is to terminate SSL VPN connections. The following are some of the many design considerations when implementing the SSL VPN:

- How do remote users trust the VPN gateway?
- How does the VPN gateway identify remote users?
- How to organize different types of users in groups so that different kinds of services can be provided?
- What kind of mobility client solution is needed for a particular client?
- Once the right kind of VPN solution is identified, how will the mobility client be installed on the remote device?
- How to centralize the policy settings for VPN users? It is not always easy or convenient for remote users to configure a mobile device for VPN functionality.

The Cisco ASA coupled with the Cisco AnyConnect client addresses the considerations mentioned above. The Cisco AnyConnect client 3.0 is used to meet the needs of wired, wireless, and remote users. The Cisco AnyConnect Secure Mobility client is the next-generation VPN client, providing remote users with secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA). AnyConnect provides end users with a connectivity experience that is intelligent, seamless, and always-on, with secure mobility across today's proliferating managed and unmanaged mobile devices.

The Cisco AnyConnect Secure Mobility client integrates new modules into the AnyConnect client package:

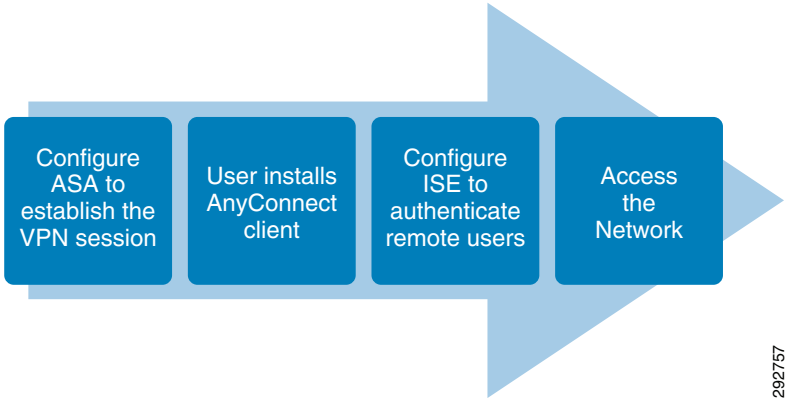
- Network Access Manager (NAM)—Formerly called the Cisco Secure Services Client, this module provides Layer 2 device management and authentication for access to both wired and wireless networks.

- Posture Assessment—The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client with the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host prior to creating a remote access connection to the ASA. Based on this pre-login evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance. The Host Scan application is delivered with the posture module and is the application that gathers this information.
- Telemetry—Sends information about the origin of malicious content detected by the antivirus software to the Web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA), which uses this data to provide better URL filtering rules.
- Web Security—Routes HTTP and HTTPS traffic to the ScanSafe Web Security scanning proxy server for content analysis, detection of malware, and administration of acceptable use policies.
- Diagnostic and Reporting Tool (DART)—Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
- Start Before Logon (SBL)—Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.

For more information on the Cisco AnyConnect 3.0 client, see: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac01intro.html.

Figure 250 shows the steps to provide VPN connectivity.

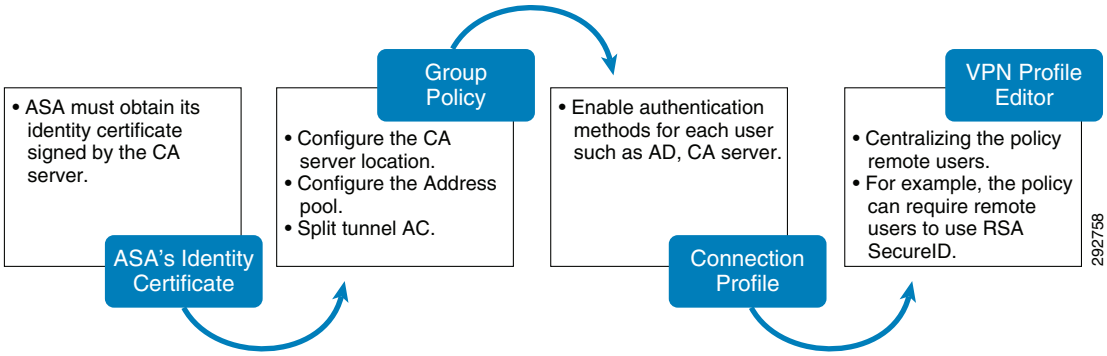
Figure 250 High Level Steps for Providing VPN Connectivity



ASA Configuration

The configuration of the ASA involves many steps. Figure 251 shows, at a high level, the steps required to configure the ASA.

Figure 251 Configuration of ASA

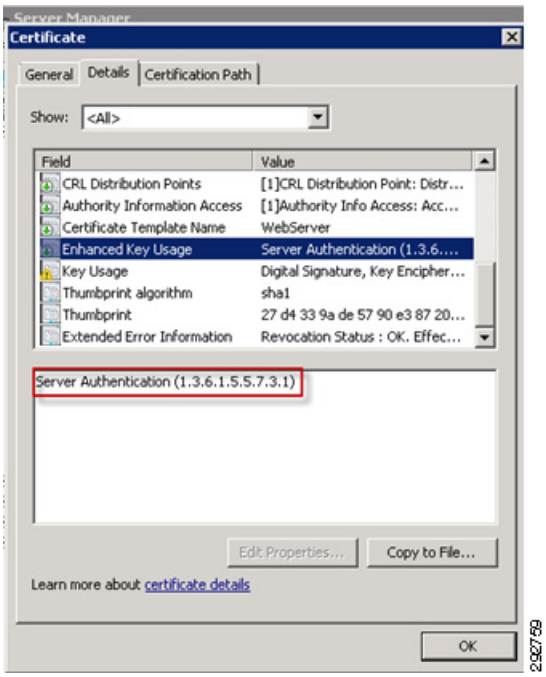


ASA's Identity Certificate

The ASA needs to present a digital certificate as means of authenticating itself to the clients. The remote clients validate the digital certificate and if the validation is successful, then they proceed to the next steps of establishing a VPN connection.

The digital certificate provided by the ASA must be issued by a trusted third-party like VeriSign or it could be also issued by an internal CA, which is signed by a trusted third-party. Instead, if the ASA presents a self-signed certificate, then the clients cannot validate the certificate because the signing authority (ASA for self-signed) is not in the list of trusted CAs in the client browser. Hence for greater security, it is recommended that the ASA's digital certificate is either issued by a trusted third-party or by an internal CA which is signed by a trusted third-party. When using a Microsoft CA as internal CA, it is important to verify that the certificate properties support Server Authentication. Figure 252 shows the certificate that can be used for server authentication. The certificate should contain EKU of Server Authentication, as indicated in Figure 252.

Figure 252 Certificate for Server Authentication



The ASA can obtain the certificate from the CA server by using SCEP or by a manual cut-and-paste method. To obtain more information on deploying certificates on the ASA, see: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html.

The following example shows the ASA configuration for certificate enrollment:

```
crypto ca trustpoint WIN2K-CA
 enrollment terminal
 subject-name CN=ASA-remote1
 serial-number
 ip-address 172.26.185.195
 keypair ssl
 no client-types
 crl configure
```

The above trust is used by ASA to obtain its own Identity Certificate from the CA server. In this design the enrollment method is terminal.

The following command shows the digital certificate issued by the CA server to the ASA:

```
ASA-remote1(config)# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 1594b5d9000000000213
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=secbn1-WIN-MRL23B7NQO6-CA
    dc=secbn1
    dc=com
  Subject Name:
    cn=ASA-remote1
    hostname=ASA-remote1.secbn1.com
    ipaddress=172.26.185.195
    serialNumber=JMX1215L1KF
```

```
  CRL Distribution Points:
    [1]  ldap:///CN=secbn1-WIN-MRL23B7NQO6-CA,CN=WIN-MRL23B7NQO6,CN=CDP,CN=Publi
c%20Key%20Services,CN=Services,CN=Configuration,DC=secbn1,DC=com?certificateRevo
cationList?base?objectClass=cRLDistributionPoint
    [2]  http://win-mrl23b7nqo6.secbn1.com/CertEnroll/secbn1-WIN-MRL23B7NQO6-CA.
crl
  Validity Date:
    start date: 09:29:35 EST May 30 2012
    end   date: 09:29:35 EST May 30 2014
  Associated Trustpoints: WIN2K-CA
```

Note The client must have network connectivity to the CRL distribution point as provided in the certificate.

ASA Trust Point to Authenticate Remote Users

ASA also needs a trust point to authenticate remote users' identity certificates. The following is the configuration of the trust point:

```
crypto ca trustpoint Validate
 enrollment terminal
 crl configure
```

The above trust point "Validate" is used to copy the root CA certificate. To understand more about how to cut-and-paste certificates using terminal method, see: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html.

Creating Groups for Different Types of Users

Group policy is an important building block for designing an effective access mechanism for users. The needs of specific users can differ. For example, one user might like to have a domain value of xyz.com and have 1.1.1.1 and 2.2.2.2 as their DNS servers. Another user might have similar requirements, but in addition might need a proxy server configured for their user name. If you have to attach all these attributes to each individual user, the configuration might become very large and complex. To solve this problem, multiple groups can be created, each with its set of individual attributes. In this case you can simply associate a user with a group name, rather than the large number of attributes, thus minimizing the configuration complexity when you have multiple users.

By default, the Cisco ASA creates DftGrpPolicy and the other group polices that inherit most of the common attributes. Only very specific attributes need to be configured explicitly for each group.

For more information about configuring tunnel groups, group policies, and users, see: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/vpngrp.html.

In the group policy definition for this design guide, the main attributes needed are vpn-tunnel-protocol, split-tunnel-network-list, and address pool location. The following example shows how this group policy was defined:

```
group-policy SSLClientPolicy internal     !This group policy is defined internally not
downloaded from radius.
group-policy SSLClientPolicy attributes
 wins-server value 10.1.6.100          ! WINS server IP address
 dns-server value 10.1.6.100          ! DNS server IP address
 vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split_ACL  ! split_ACL prevents some local network
traffic from getting into VPN traffic.
 default-domain value secbn1.com
 address-pools value testpool        ! The IP address pool value.
```

Connection Profile Configuration

While group policies define the attributes for a group, the connection profile specifies the attributes specific to a connection. For example, a connection profile for AnyConnect specifies if the users belonging to this connection are authenticated by a RADIUS server or locally. The connection profile also points to the group profile to which it belongs. If no connection profile is defined on the system, the ASA points to a default connection profile, but to make administration simple it is better to define a specific group and connection profiles. The following example shows the ASA configuration for the AnyConnect connection profile:

```
tunnel-group SSLClientProfile type remote-access
tunnel-group SSLClientProfile general-attributes
 authentication-server-group ISE    ! The remote sessions are authenticated with ISE.
 default-group-policy SSLClientPolicy ! The parent group policy used by this connection
profile.

tunnel-group SSLClientProfile webvpn-attributes
 authentication aaa certificate        ! The remote users are authenticated by AAA and
Digital Certificate.
 group-alias SSLVPNClient enable  ! The remote users are presented with this alias name
during the session.
 group-url https://172.26.185.195/SSLVPNClient enable
 group-url https://192.168.167.225/SSLVPNClient disable
!
```

The above configuration steps illustrate how to configure SSLVPN sessions with AnyConnect. The same configuration can also be done using ASDM editor or by another management tool. To obtain more information about the configuration using other tools, refer to ASA configuration editor at: http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_anyconnect.html#wp1090443.

Enabling AnyConnect VPN on the ASA

After defining the group-policy and connection profile on the ASA, the last step is to enable the AnyConnect VPN feature on the ASA. After enabling AnyConnect, the administrator can also configure additional features, such as pointing to the AnyConnect image software, NAM profile, and VPN Profile. The following example shows the configuration commands to enable AnyConnect modules:

```
webvpn
 enable outside
 anyconnect keep-installer installed ! This forces the anyconnect to remain installed on
the endpoint device, after the session is terminated.
 anyconnect modules none
```

A Provisioned Windows Device Connecting to the Network Remotely

For a corporate approved device to obtain remote access capability, the user must perform the following steps at the campus location:

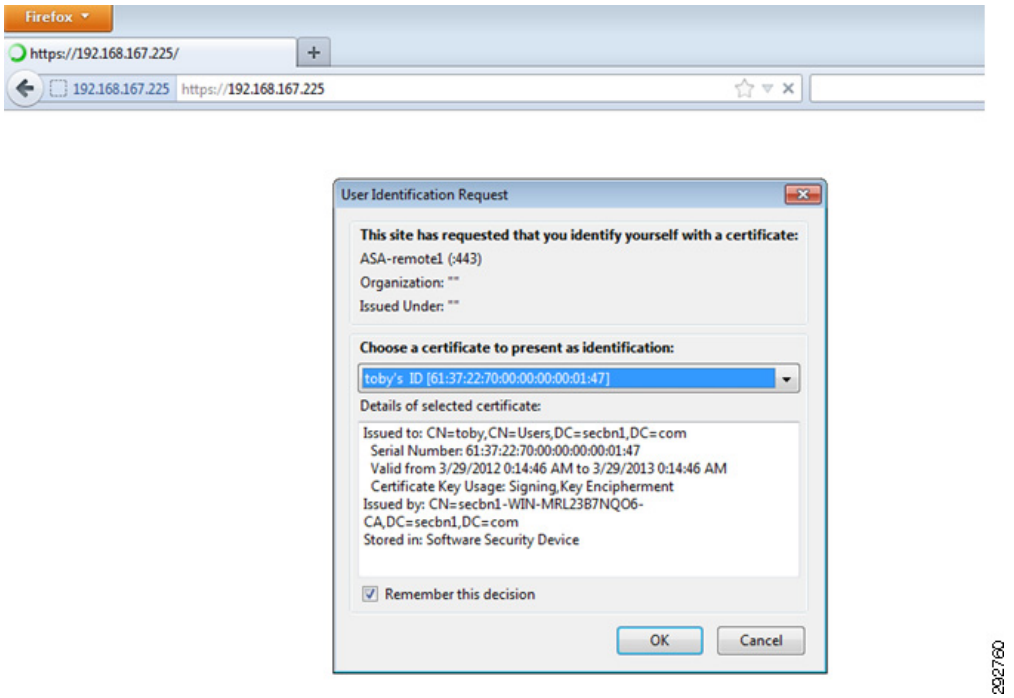
Step 1 Install the RSA SecurID application on the remote device and, with IT support, provision the software on the device.

Step 2 It is assumed that before the AnyConnect installation begins, the workstation has successfully completed the enrollment and provisioning process, which implies that the workstation has a valid digital certificate issued by the CA server.

The steps shown below are for one time installation. After the installation is completed, the user is never prompted for these steps.

Step 3 Initiate an SSL VPN session using a Web browser to the ASA VPN gateway IP address, which is shown in Figure 253.

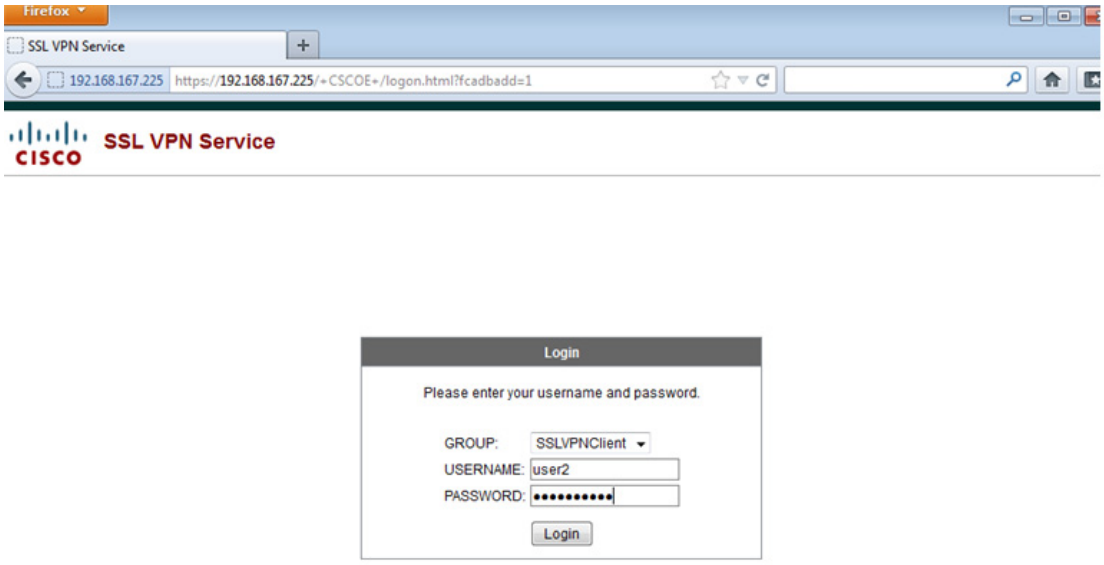
Figure 253 SSL VPN Session to ASA VPN Gateway IP Address



Note The certificates presented by the ASA remote end points and the identity certificate of the ASA must be signed by the same root CA server.

Step 4 The user is presented with login screen and the user needs to select the Group to which they belong. The user is expected to select the group-policy name and the valid credentials, as shown in Figure 254.

Figure 254 Selecting Group



Step 5 After the user credentials are validated, Cisco AnyConnect installation begins, which is depicted in Figure 255.

Figure 255 Cisco AnyConnect Installation

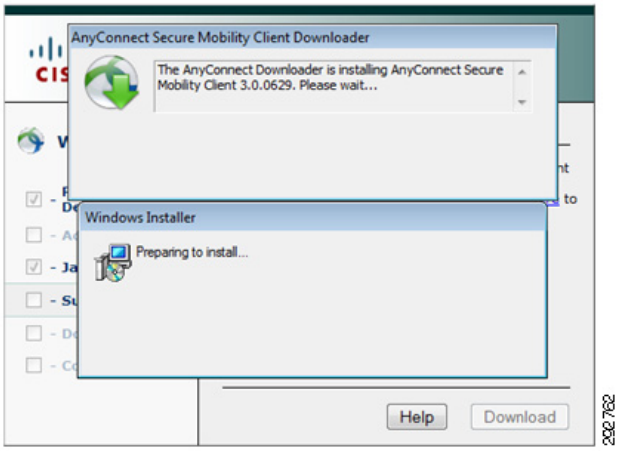


Figure 256 depicts successful installation of Cisco AnyConnect on the workstation:

Figure 256 Successful Installation of Cisco AnyConnect

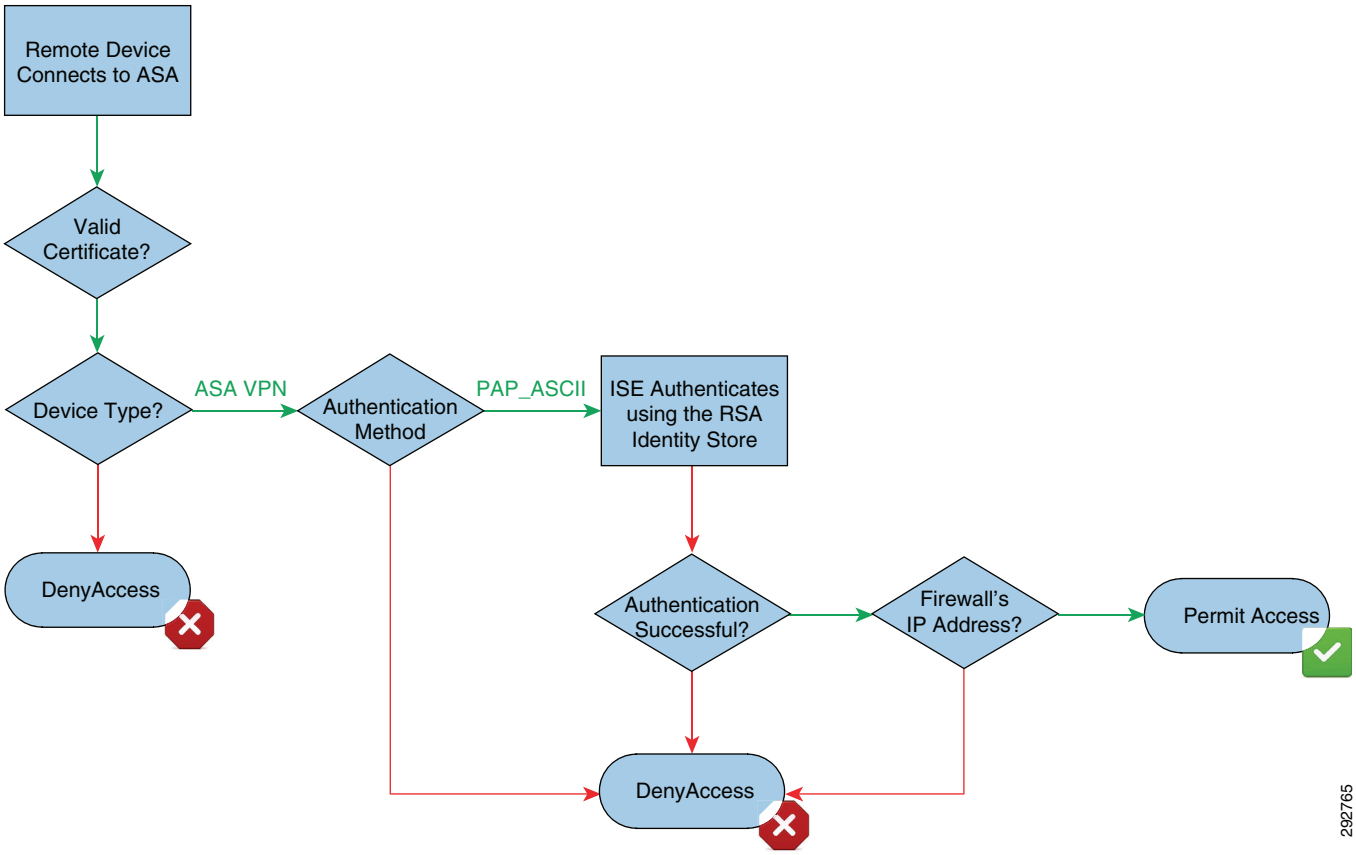
Figure 257 shows the Windows workstation establishing a session.

Figure 257 AnyConnect Initiates VPN Connection

As explained in the Connection Profile Configuration, when a remote worker connects to the network both ISE and the ASA authenticate the device. ASA initially validates the digital certificate of the remote user. If the certificate is valid, then the next step of authentication happens, which is through the RSA SecurID token. The remote worker is allowed to access the network if both authentications are valid.

The logic flow in Figure 258 shows what happens when a remote device accesses the network.

Figure 258 Logic Flow for a Remote Worker Accessing the Network



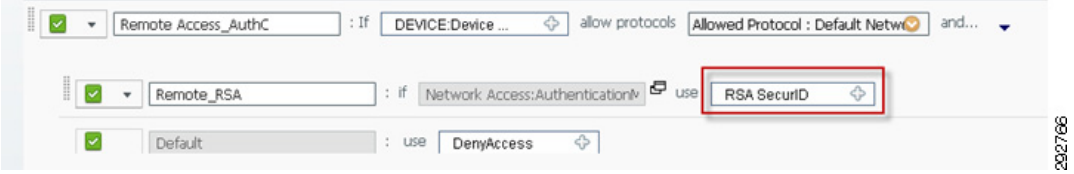
Verifying What ISE Policy Rules Are Applied

As shown in Figure 258, ISE validates the remote user in the following sequence:

1. Validate if the Device Type Equals ASA VPN. This is to ensure that only devices that are configured as VPN Type can initiate the communication with ISE.
2. Validate if the authentication protocol is PAP_ASCII. This is the protocol used by ASA to send the RSA Secure ID token passwords to the ISE, which the ISE sends to RSA Secure ID server for authentication.
3. In the authorization Rule, ISE validates the Source IP address of the ASA as a means to authorize the connection. In this design remote VPN users are only authenticated by ASA and ISE, and there is no authorization taking place. Figure 259 and Figure 260 detail the authentication and authorization rules in ISE.

The ISE rule shown in Figure 259 uses the RSA SecurID identity store for authentication.

Figure 259 Authentication Rule

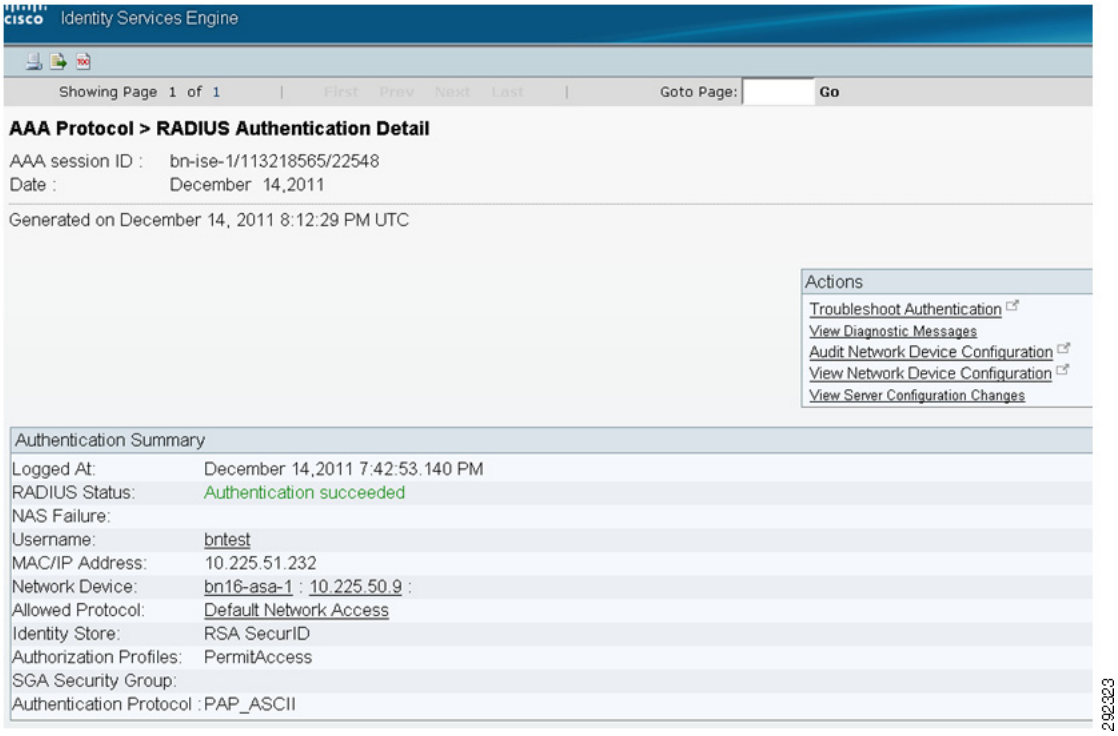


The ISE authorization rule shown in Figure 260 matched since a remote device connected and the Network Access: Device IP Address matches the ASA firewall's address.

Figure 260 Authorization Rule

To verify what rules were applied on the ISE, click **Monitor > Authentication**, as shown in Figure 261.

Figure 261 Log Information on ISE for Successful Remote Worker Authentication



A Provisioned iOS Device Connecting to Network Remotely

Similar to workstations, an iOS device that was provisioned at the campus can establish an SSL VPN connection to the campus network using Cisco AnyConnect. The following steps must be completed by the user before establishing SSL VPN connectivity:

Step 1 The iOS device should already have a digital certificate installed. Figure 262 shows an example of a provisioned device.

Figure 262 Provisioned Device

Step 2 The user should install the Cisco AnyConnect from Apple's App Store.

Step 3 Configure the profile on AnyConnect and select the certificate which is already installed in the device (Certificate Provisioning must happen before initiation remote VPN communication), as shown in Figure 263.

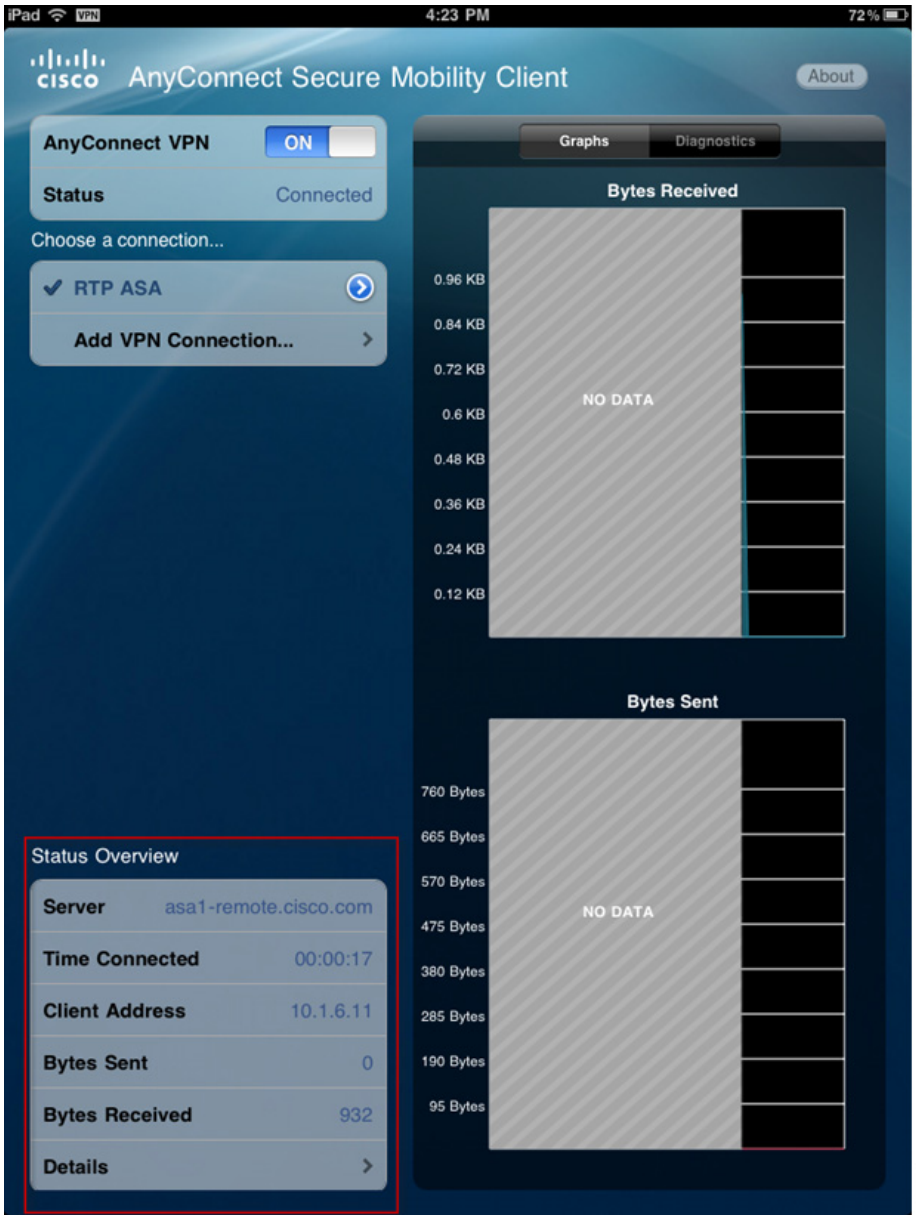
Figure 263 Configure Profile and Select Certificate

Step 4 Select the VPN Group which the Network Administrator must inform the user about the right group to select, and enter the user credentials. ASA VPN authentication requires the user certificate and the user credentials. Hence the user credentials have to be entered, as shown in Figure 264.

Figure 264 User Credentials

Figure 265 shows a successfully connected SSL VPN session

Figure 265 Connected SSL VPN Session



Managing a Lost or Stolen Device

When a previously provisioned device is reported lost or stolen, the device must be denied access to prevent unauthorized access to the network.

A first level of defense to protect against a lost or stolen device is to enforce the use of a passcode to access the device and lock the device automatically after a short period of inactivity (typically five to ten minutes). This can also be enhanced by erasing all data on the mobile device after a number of failed passcode attempts or performing a remote wipe. This and other rules may be enforced by a Mobile Device Manager.

The Cisco ISE offers different ways to prevent a lost or stolen device from connecting to the network. The My Devices Portal allows the employee to mark a device as lost and prevent others from gaining unauthorized access with that device. In addition, if the device is connected to the network when the device is marked as lost, the ISE issues a Change of Authorization (CoA) and forces the endpoint off the network.

The administrator is also able to blacklist a device and force the endpoint off the network. In addition, the administrator is able to use Endpoint Protection Services (EPS) to prevent the endpoint from further connecting to the network. The employee and administrator have different capabilities to block lost or stolen devices:

Employee:

- Report devices as “Lost” from the My Devices Portal.
- Reinstate a device and regain access without registering the device again.

Administrator:

- Add the endpoint to the Blacklist Identity Group.
- If the endpoint is connected, force it off the network by using the RADIUS Active Sessions.
- Quarantine the endpoint using the ISE’s Endpoint Protection Services (EPS) feature. Employees are not able to reinstate endpoints quarantined by the administrator.

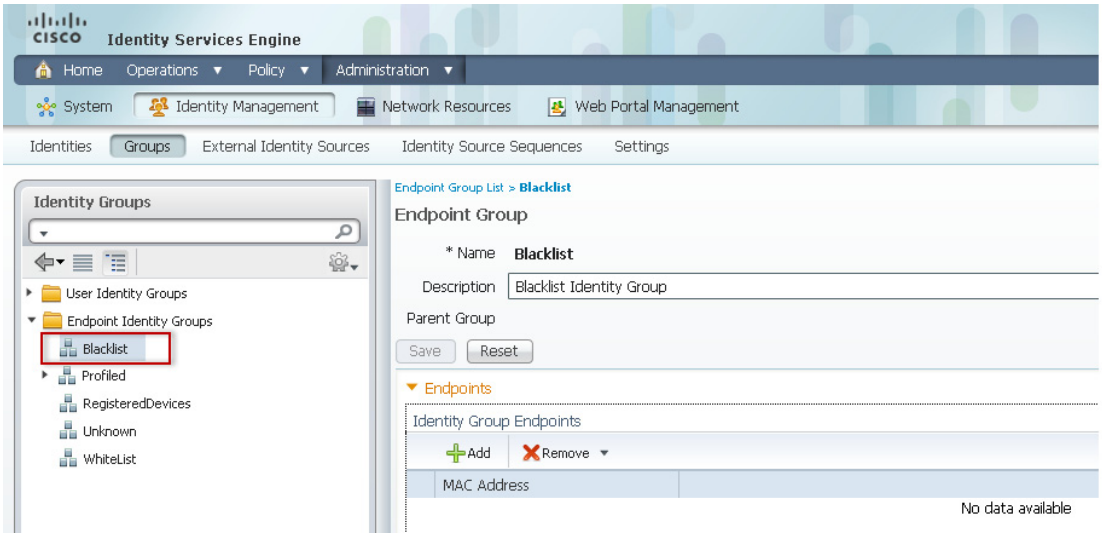
Blacklist Identity Group

The Blacklist is a system-generated endpoint identity group maintained by ISE to prevent access to lost or stolen devices. For this design guide, two authorization profiles are used to enforce the permissions for wireless and wired devices within the Blacklist:

- Blackhole_Wireless_Access
- Blackhole_Wired_Access

The Blacklist Identity Group is displayed by clicking **Administration > Identity Management > Groups > Endpoint Identity Groups**. Figure 266 shows an empty Blacklist identity group.

Figure 266 Blacklist Identity Group



Devices that have been blacklisted are assigned to the Blacklist identity group. Both wired and wireless devices can be placed into the Blacklist identity group. An authorization profile is used to define the access granted to the blacklisted devices. Blacklisted device connection requests are accepted and the device is redirected to a Web page that informs the user that the device is blacklisted.

Blacklisting Wireless Devices

The Blackhole_Wireless_Access authorization profile is configured under **Policy > Policy > Elements > Results > Authorization Profiles**, as shown in Figure 267. The Access Type is defined as ACCESS_ACCEPT and the following cisco-av-pairs are defined:

- cisco-av-pair: url-redirect=https://ip:port/mydevices/blackhole.jsp. The user gets redirected to this page.
- cisco-av-pair: url-redirect-acl=BLACKHOLE. The Wireless LAN Controller must have an ACL named BLACKHOLE configured for the redirection to work at the campus and a FlexConnect ACL at the branch also named BLACKHOLE.

Figure 267 Blacklist Authorization Profile

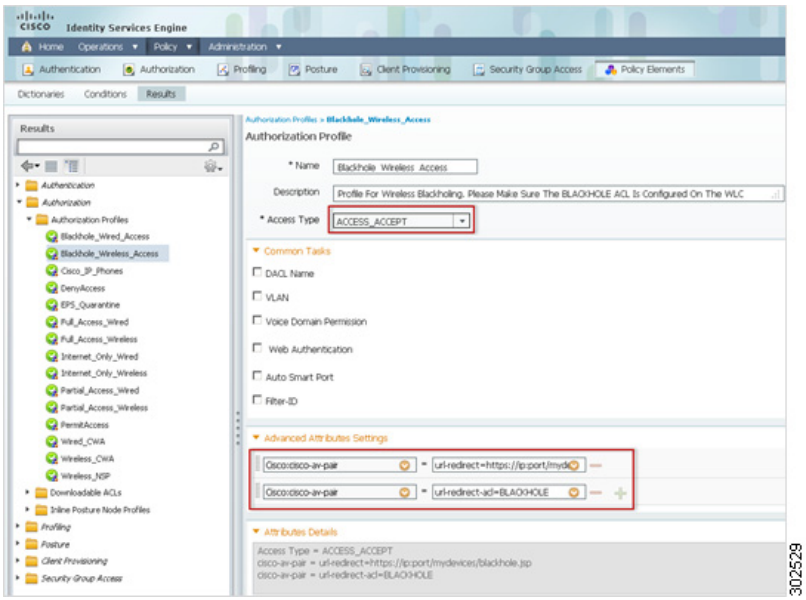
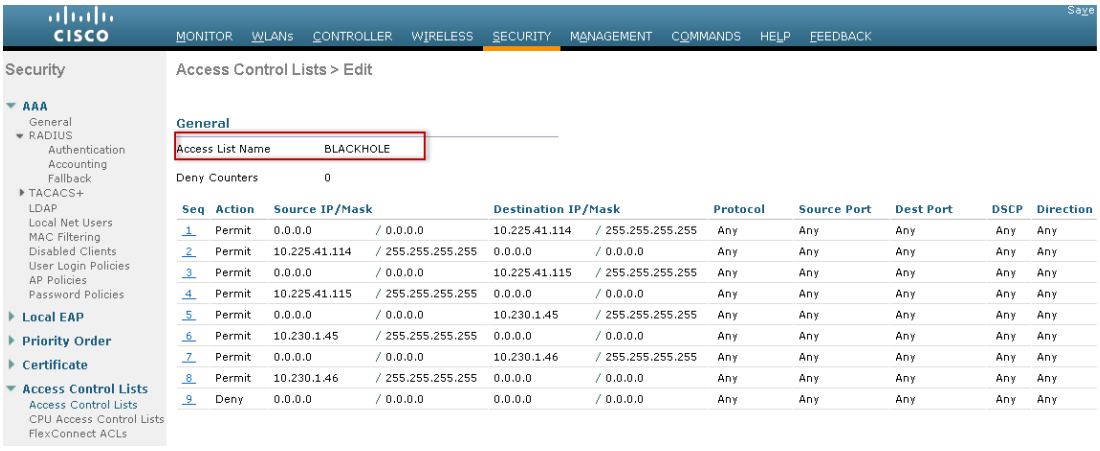


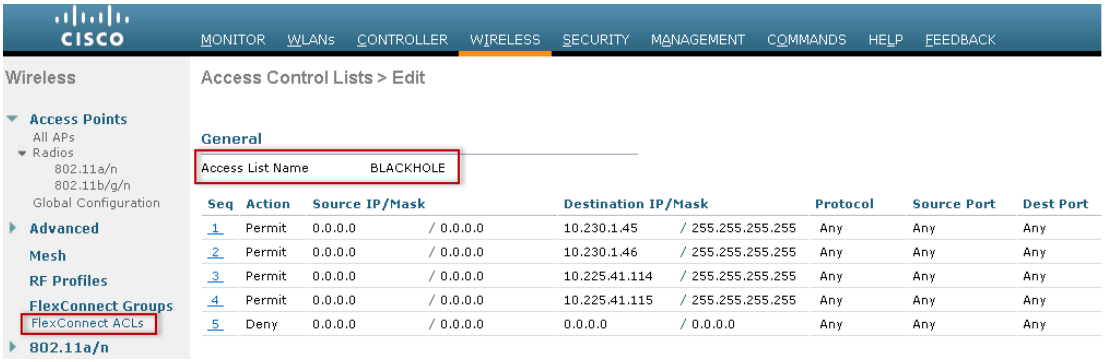
Figure 268 shows how the BLACKHOLE access list is defined in the WLC to only allow access to the ISE and DNS server. By granting access to DNS and ISE, the endpoint is able to reach the blackhole.jsp Web page.

Figure 268 BLACKHOLE ACL



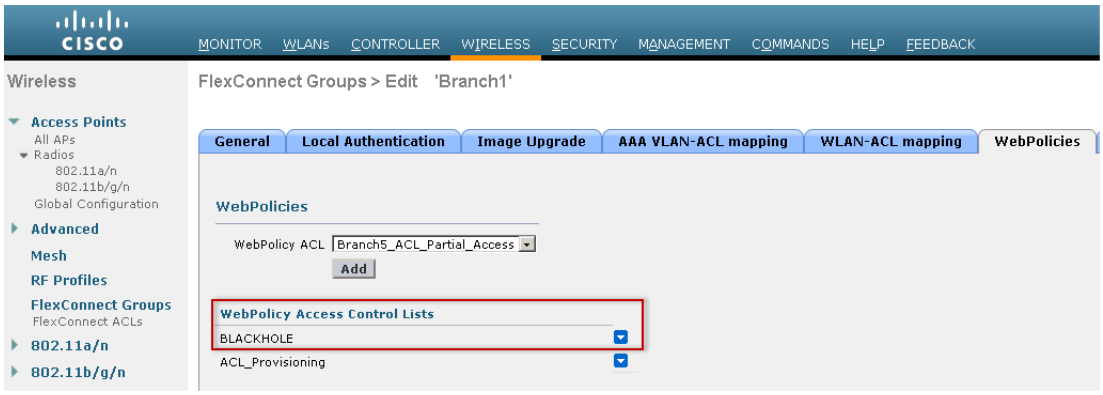
For endpoints connecting to the branch, a similar FlexConnect ACL is defined and applied to the FlexConnect Group. Figure 269 shows the BLACKHOLE FlexConnect ACL. This ACL is similar to the one shown above, which is used for campus devices.

Figure 269 BLACKHOLE FlexConnect ACL



To apply this FlexConnect to the branch, select the appropriate FlexConnect Group and click the **WebPolicies** tab. Add the BLACKHOLE ACL, as shown in Figure 270.

Figure 270 WebPolicies for Branch1



To enforce the blacklist permissions, an authorization rule is defined under **Policy > Authorization**. Figure 271 shows the Black List_Wireless_AuthZ rule enforcing the Blackhole_Wireless_Access permissions.

Figure 271 Black List_Wireless__AuthZ Authorization Rule

Once the device is in the Blacklist identity group, future attempts to connect to the network are denied. When a user opens a Web browser on a blacklisted device, the session is redirected to the page shown in Figure 272.

Figure 272 Unauthorized Network Access

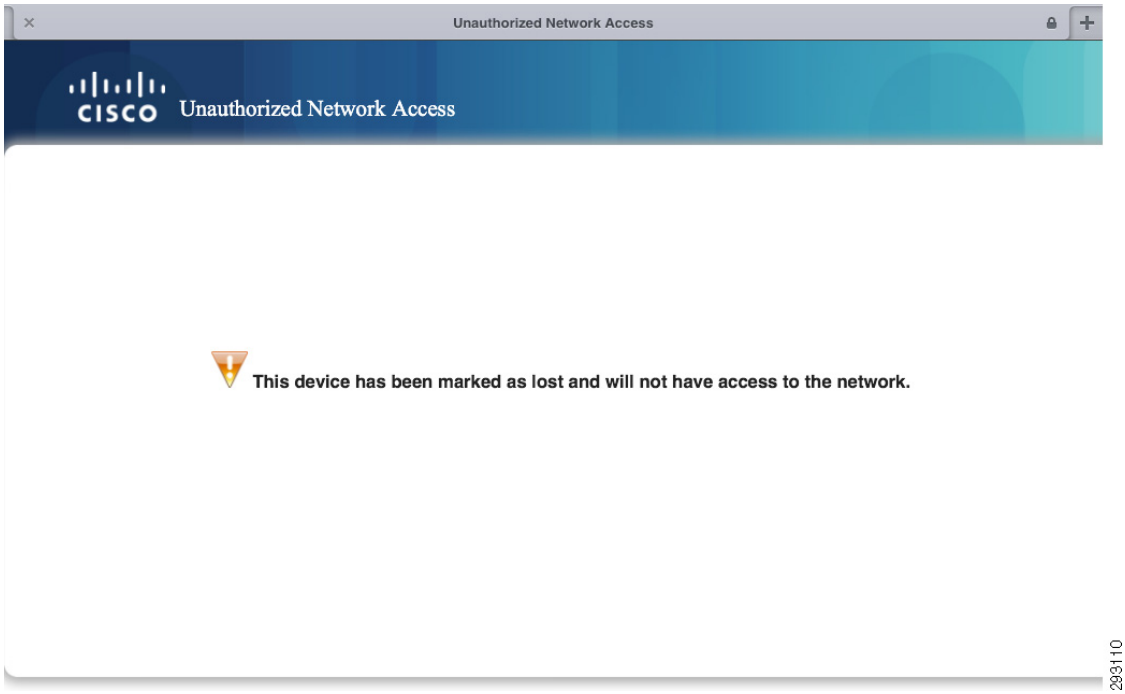
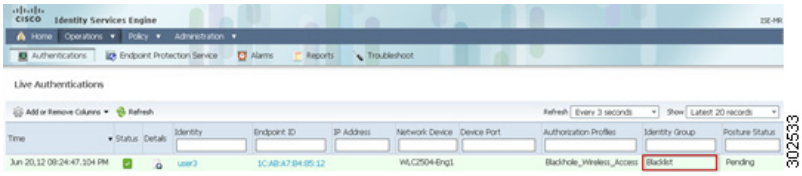


Figure 273 shows how a device in the Blacklist attempts to connect to the network and the Blackhole_Wireless_Access authorization profile is executed.

Figure 273 Device in Blacklist



Blacklisting Wired Devices

The user experience when a wired device is blacklisted is similar to a wireless device that has been black listed. When a device is blacklisted and the user attempts to access any Web page, the device is re-directed to a portal that displays “This device is marked as lost and will not have access to the network”. The following steps show how to implement this behavior:

Step 1 Create a dACL on the ISE, which is referred to in this guide as “BLACKHOLE_ACL”, that provides end user access to ISE only.

Step 2 Create a URL Redirect ACL called “BLACKHOLE” on the accesss layer switch that matches any http or https traffic.

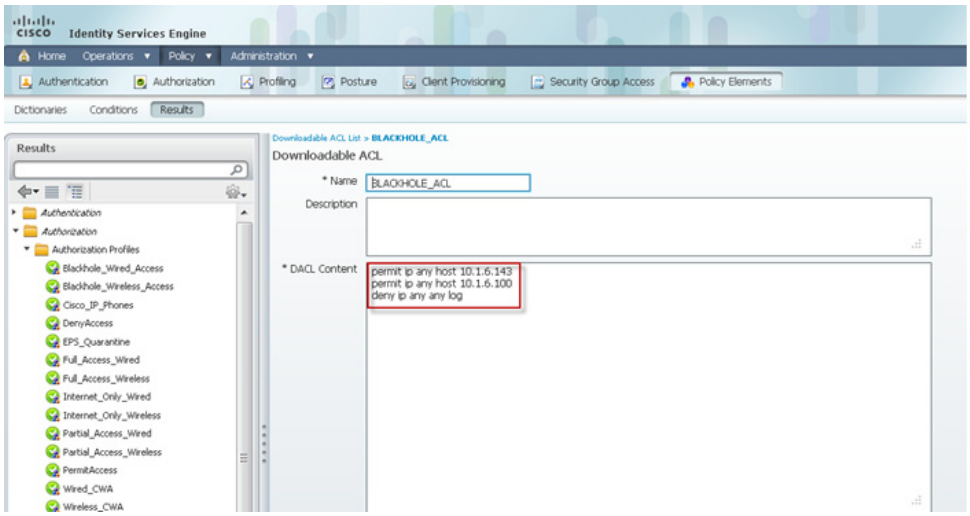
Step 3 Create an authZ profile, which is referred to in this gude as “BLACKHOLE_WIRED_ACCESS”, that pushes the dACL(BLACKHOLE_ACL, url-redirect-acl (BLACKHOLE)), and redirect-link to the switch.

Step 4 Define a new rule in the AuthZ policy that matches on the blacklisted devices and assigns the authorization profile “Blackhole_Wired_Access”.

Creating dACL on ISE

The BLACK_HOLE_ACL dACL is created under **Policy > Policy Elements > Results > Downloadable ACLs**, which is shown in Figure 274.

Figure 274 Creating dACL on ISE



Creating URL REDIRECT ACL on the Switch

Figure 275 shows the configuration for the BLACKHOLE redirect ACL on the wired switch:

Figure 275 Configuration for BLACKHOLE Redirect ACL

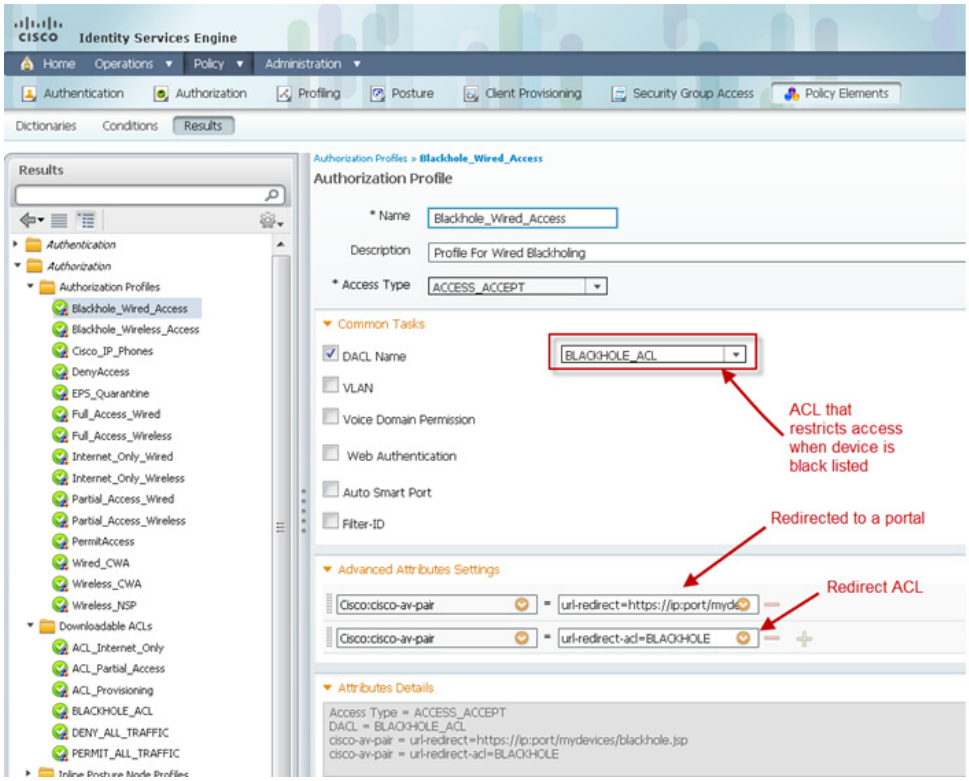
```
ACT#show ip access-lists | begin BLACKHOLE
    10 deny udp any any eq domain (465 matches)
    20 permit tcp any any eq www (2642 matches)
    30 permit tcp any any eq 443 (324 matches)
```

302541

Configuring AuthZ Policy

Define an authorization profile called "Blackhole_Wired_Access" under **Policy > Policy > Elements > Results > Authorization Profiles**, as shown in Figure 276.

Figure 276 Blackhole_Wired_Access Authorization Profile



302535

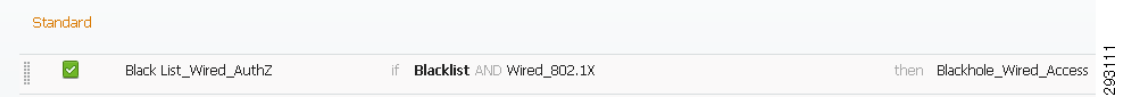
The following cisco-av-pairs are defined:

- cisco-av-pair: url-redirect=https://ip:port/mydevices/blackhole.jsp. The user gets redirected to this page.
- cisco-av-pair: url-redirect-acl=BLACKHOLE. The access layer switch must have an ACL named BLACKHOLE configured for the redirection to work.

Creating a Rule in the Authorization Policy

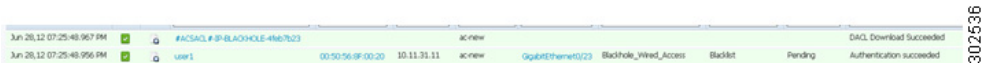
The last configuration step is to create a new rule in the authZ policy that uses the authZ profile "Blackhole_Wired_Access" (created above) when it matches a dot1x wired device which is blacklisted. Figure 277 displays the rule.

Figure 277 Black List_Wired_AuthZ



Once the rules are defined, a blacklisted device will be denied access to the network. Figure 278 shows the log information on the ISE.

Figure 278 ISE Log Information



Notice the following two items:

- user1 belongs to “Blacklist” identity group, so an authorization profile “Blackhole_Wired_Access” was implemented.
- A Dynamic ACL called “BLACKHOLE_ACL” is applied to the switch.

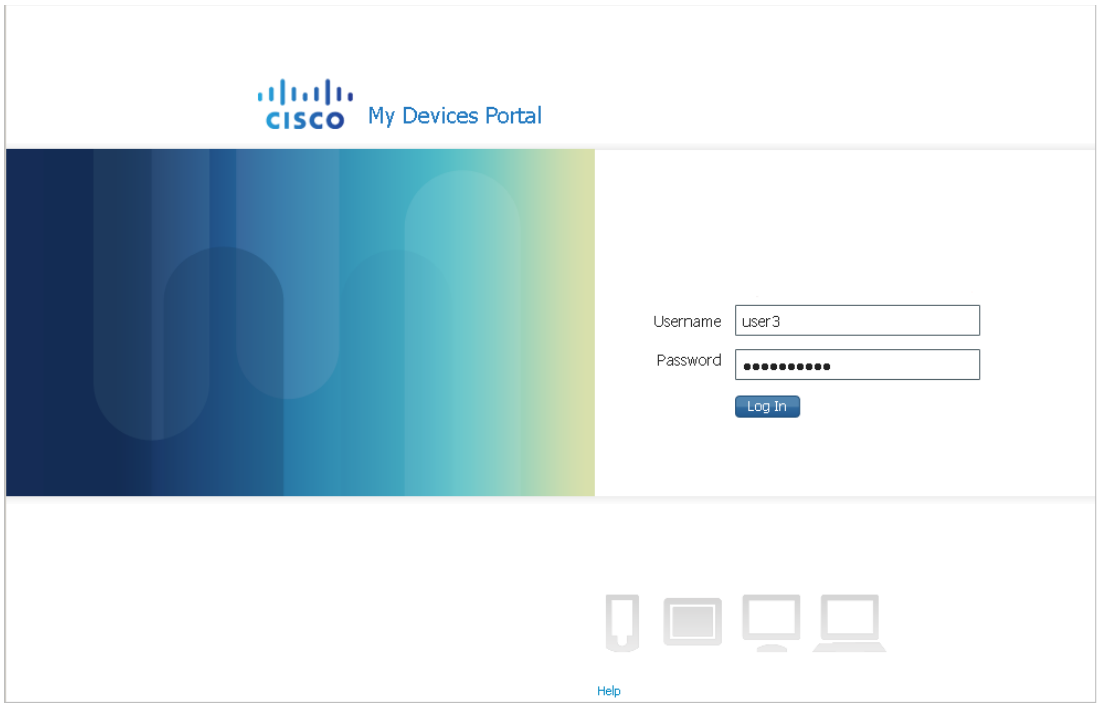
My Devices Portal

Using the My Devices Portal, employees are able to mark any lost or stolen device as blacklisted to prevent further network access. The portal requires user authentication and displays the devices that have been added or registered by the employee. The My Devices Portal may be accessed from the following URL:

https://<ISE_IP_Address>:8443/mydevices/LoginCheck.action

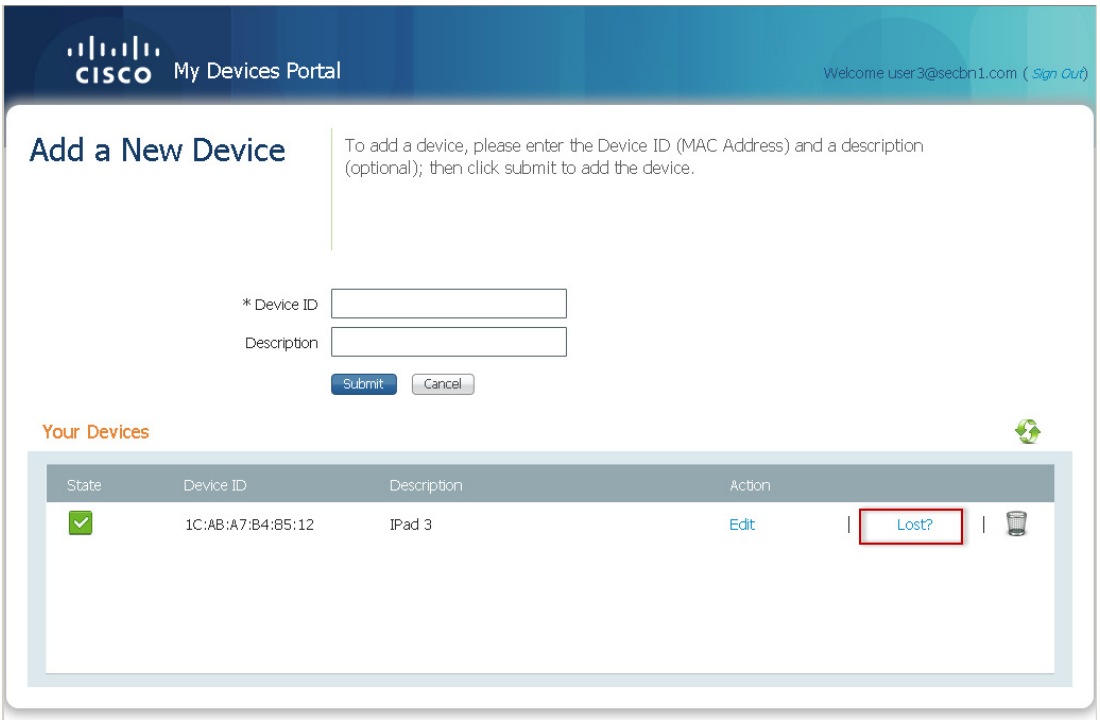
In addition to being able to report a device lost or stolen, the portal is used to add new devices or make changes to existing devices assigned to the employee. Figure 279 shows the main portal page.

Figure 279 My Devices Portal



The portal displays devices assigned to the employee or previously registered using the self-registration portal. The employee is able to edit the device's description and report a device as lost, as shown in Figure 280.

Figure 280 Lost Device

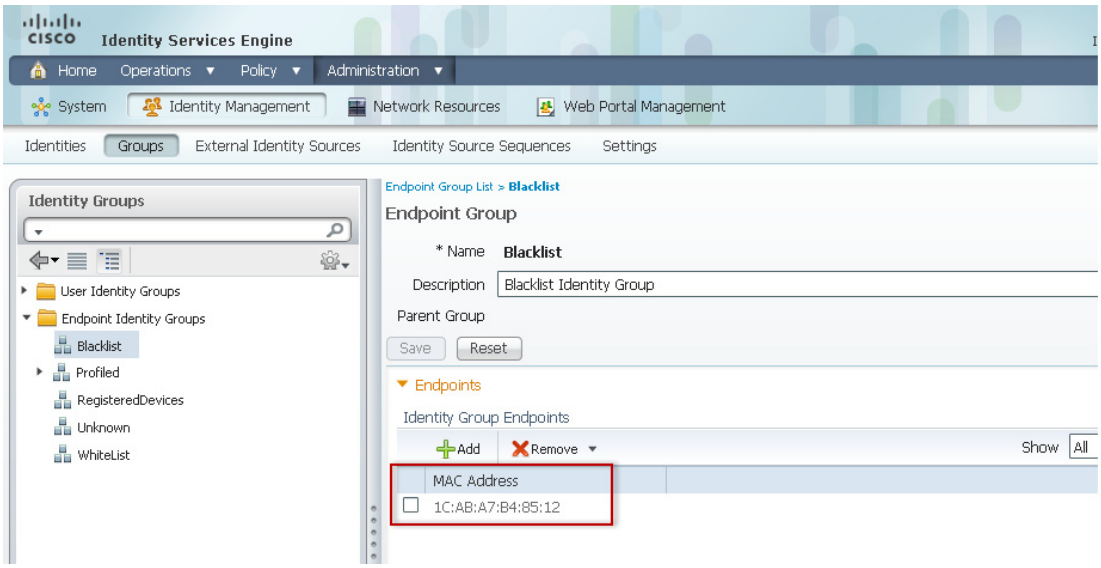


Before blacklisting a device, ISE displays the warning shown in Figure 281.

Figure 281 Blacklist Warning

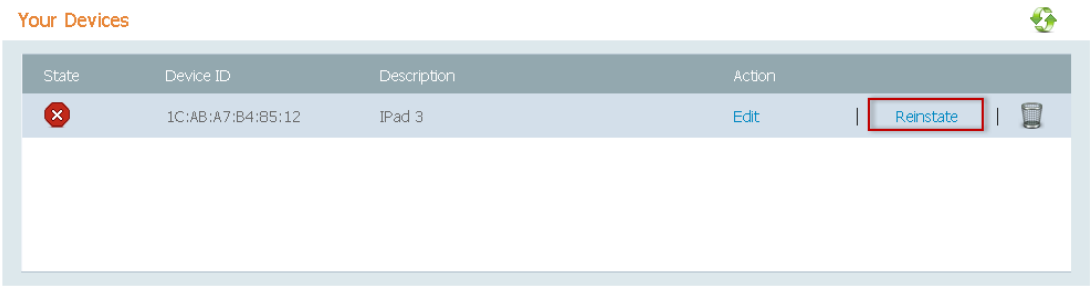
Once the device is marked as lost, the device is added to the Blacklist Identity Group. If the device is connected to the network at that time, ISE issues a Change of Authorization (CoA) and forces the device off the network. To verify that the device has been added to the Blacklist Identity group, click **Administration > Identity Management > Groups > Endpoint Identity Groups** and review the Blacklist. Figure 282 shows the MAC address added to the Blacklist.

Figure 282 Blacklist Identity Group



The My Devices Portal also gives the user the option to reinstate a blacklisted device to allow the device access to the network. Figure 283 shows the Reinstate option.

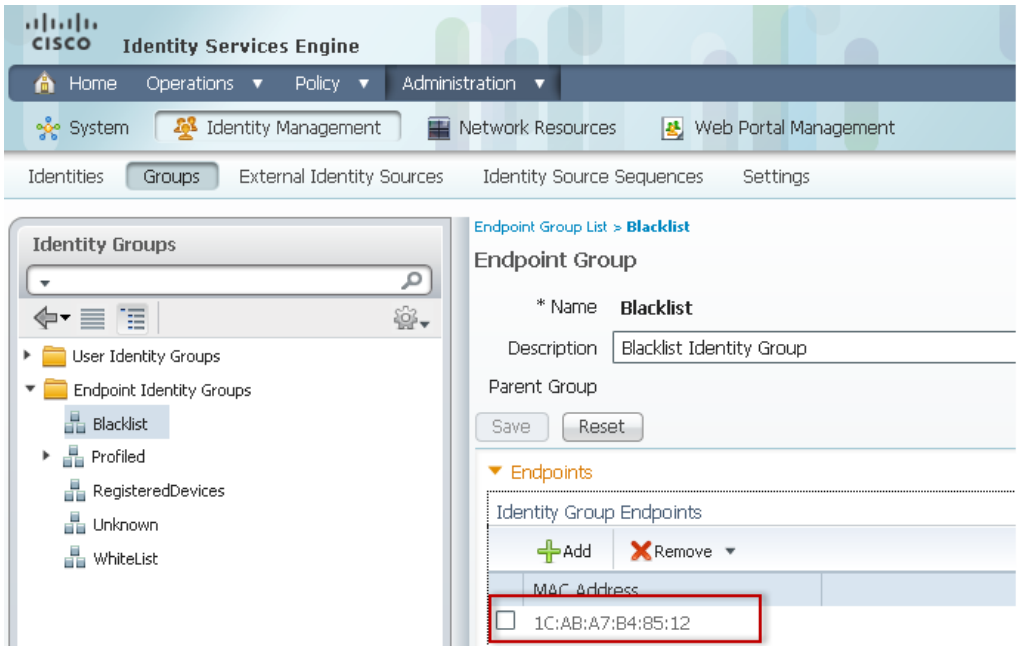
Figure 283 Reinstate a Device



Blacklisting a Device Manually

Administrators are able to blacklist a device by adding it manually to the BlackList Identity Group. Click **Administration > Groups > Endpoint Identity Groups > Blacklist** and add the MAC address of the device to be blacklisted. Figure 284 shows the MAC address added to the identity group.

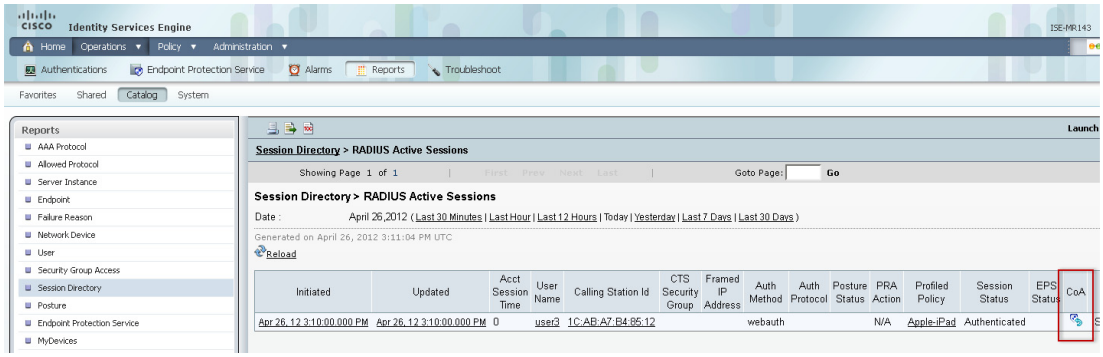
Figure 284 Device to be Blacklisted



Note that by adding the device to the Blacklist Identity Group, ISE prevents future attempts to connect to the network, but if the user is currently connected to the network, an additional step needs to take place to force the endpoint off the network.

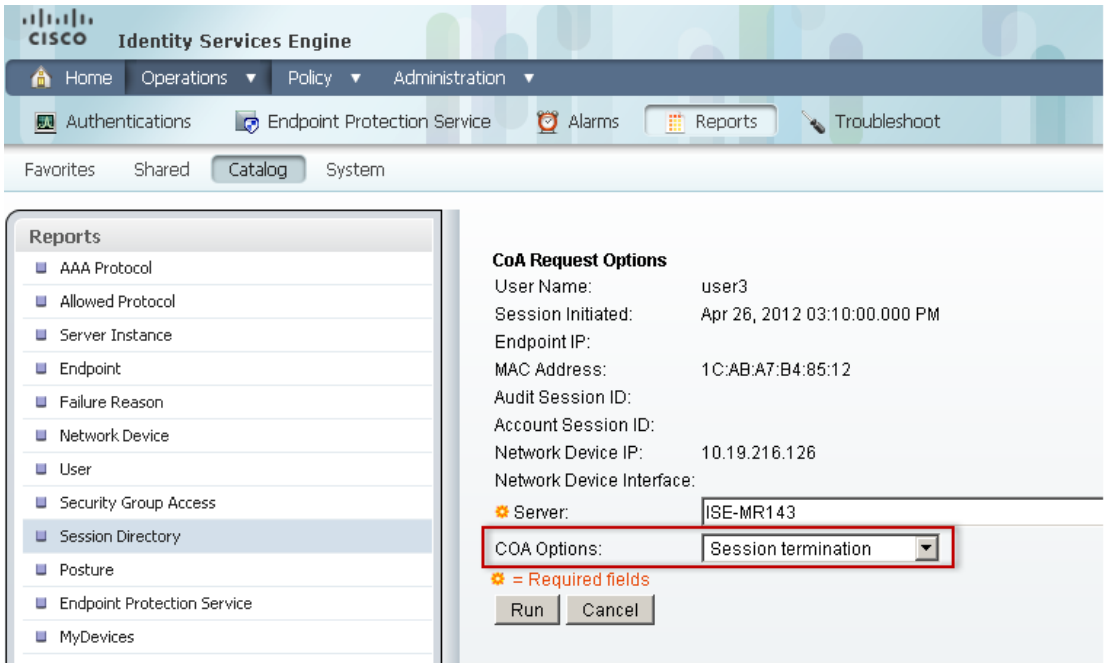
The RADIUS Active Sessions report provides details on what devices have authenticated and are active. To force a device off the network, click **Reports > Catalog > Session Directory > RADIUS Active Sessions** and select the active session for the blacklisted device. Figure 285 shows the active session for the blacklisted device. Click **CoA** to display the CoA options for that device.

Figure 285 RADIUS Active Sessions



As shown in Figure 286, under the CoA options, select **Session termination** to terminate the session and disconnect the device.

Figure 286 Session Termination



Note The employee still has the option to reinstate a device that was blacklisted by the administrator.

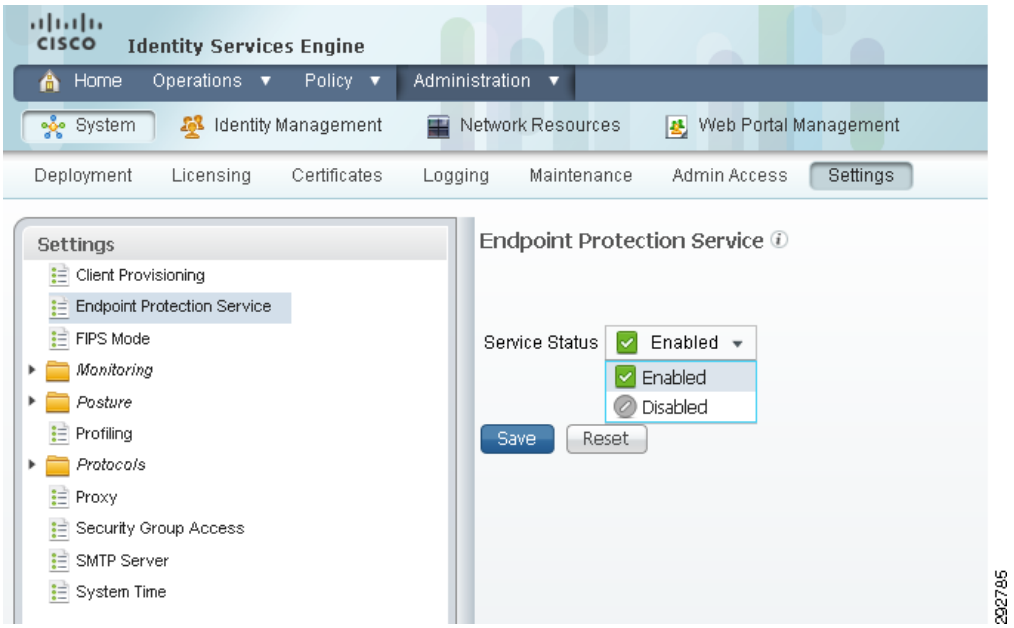
Endpoint Protection Services (EPS)

Endpoint Protection Services is a service provided by the ISE to extend the monitoring and controlling capabilities of endpoints. EPS also monitors and changes the authorization state of endpoints. EPS can be used to change the authorization state of an endpoint without having to modify the overall authorization policy. EPS allows the administrator to quarantine or limit access to a device and unquarantine a device or allow full access to the network to reverse the quarantine status.

Note EPS requires an ISE Advanced license.

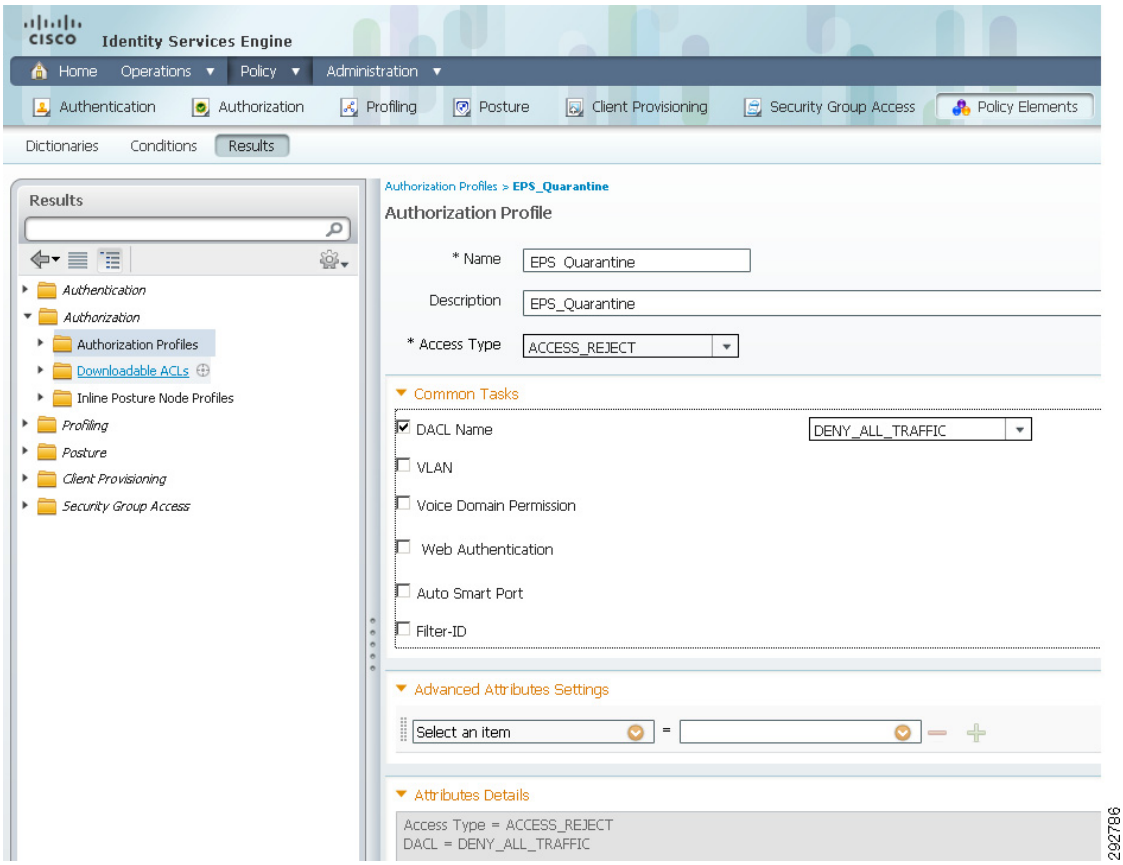
To enable EPS, click **Administration > System > Settings > Endpoint Protection Services** and select **Enabled**, as shown in Figure 287.

Figure 287 Enable EPS



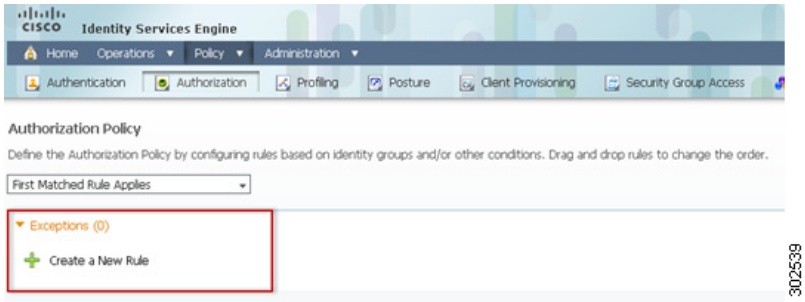
Create an authorization profile to define the permissions to specified network services. Click **Policy > Policy Elements > Results > Authorization > Authorization Profiles** and define a new authorization profile, as shown in Figure 288.

Figure 288 EPS_Quarantine Authorization Profile



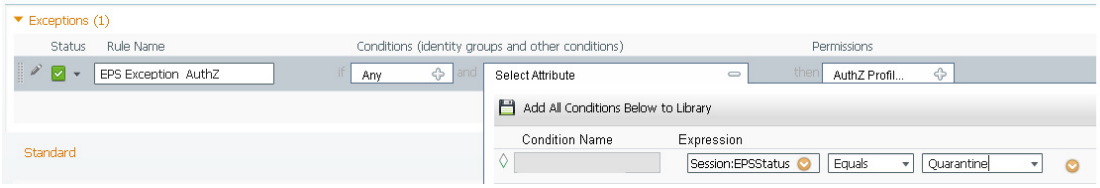
Create an EPS Exception policy and rule to be processed before the standard policies are processed. Click **Policy > Authorization > Exceptions > Create a New Rule**, as shown in Figure 289.

Figure 289 EPS Exception Policy



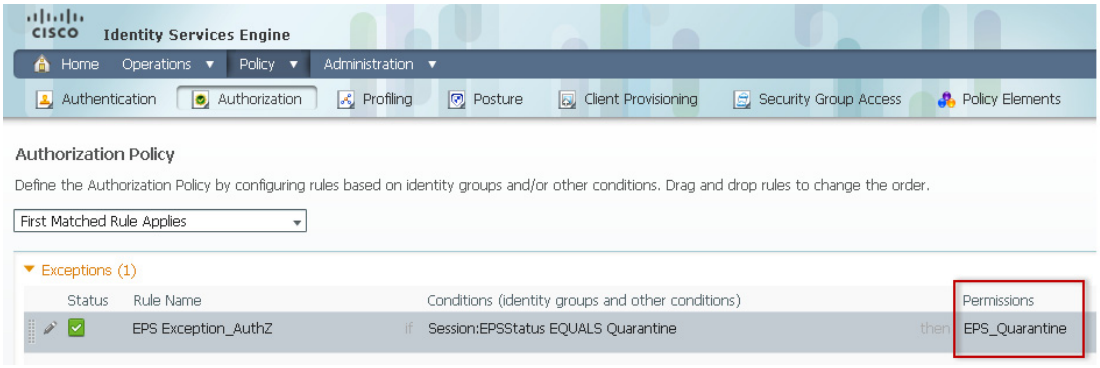
Enter a Rule Name and under Conditions create a new condition (**Advanced Option**). Under Expression click **Select Attribute** and select **EPSStatus Equals Quarantine**, as shown in Figure 290.

Figure 290 EPS Exception Policy



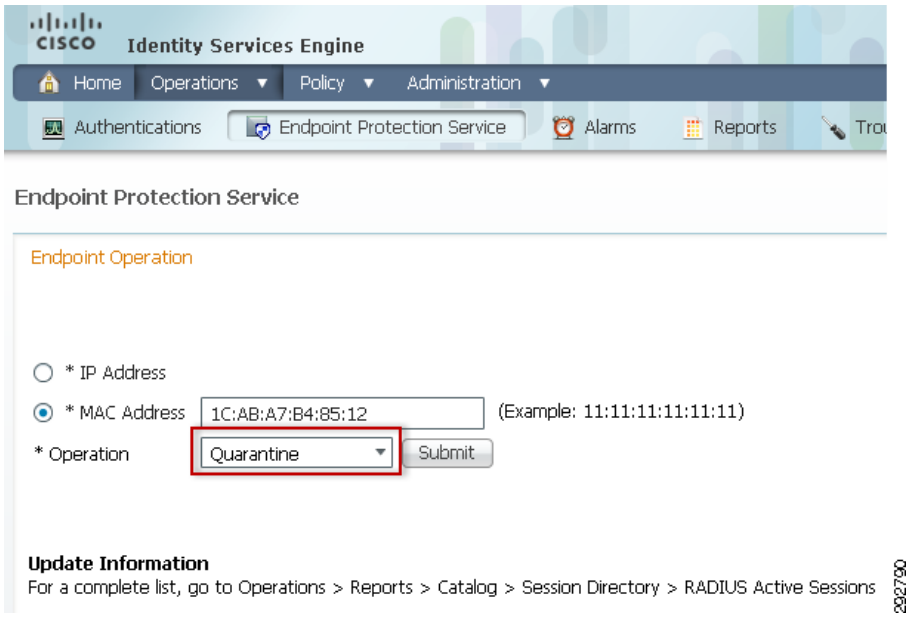
Under Permissions, select the previously defined **EPS_Quarantine** Authorization Profile. Figure 291 shows the complete Exception policy.

Figure 291 EPS Quarantine Permissions



To quarantine a device, click **Operations > Endpoint Protection Service** and enter the endpoint's MAC Address to be quarantined. Under Operation select **Quarantine**, as shown in Figure 292.

Figure 292 EPS



As soon as the administrator clicks **Submit**, the device is forced off the network and future attempts to connect are rejected. Figure 293 shows the EPS_Quarantine authorization profile being applied and the device is denied access.

Figure 293 Quarantined Endpoints

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Apr 26,12 04:26:24.274 PM			1C:AB:A7:B4:85:12	1C:AB:A7:B4:85:12		WLC2504-Eng1		EPS_Quarantine	RegisteredDevices
Apr 26,12 04:26:24.015 PM			1C:AB:A7:B4:85:12	1C:AB:A7:B4:85:12		WLC2504-Eng1		EPS_Quarantine	RegisteredDevices

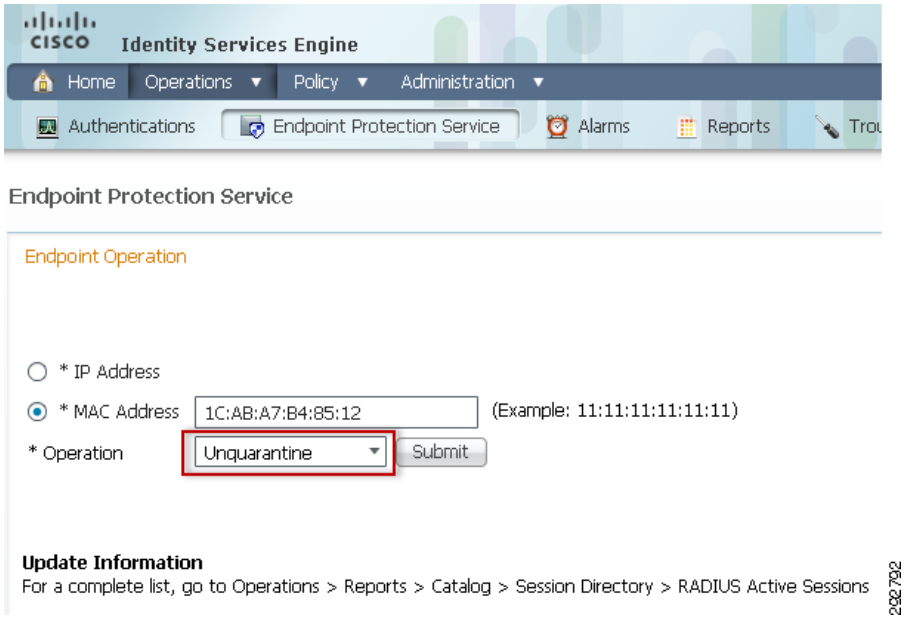
292791

EPS provides an extra layer of control to monitor and change the authorization state of endpoints.

Note Employees do not have the option to reinstate devices that have been quarantined by the administrator.

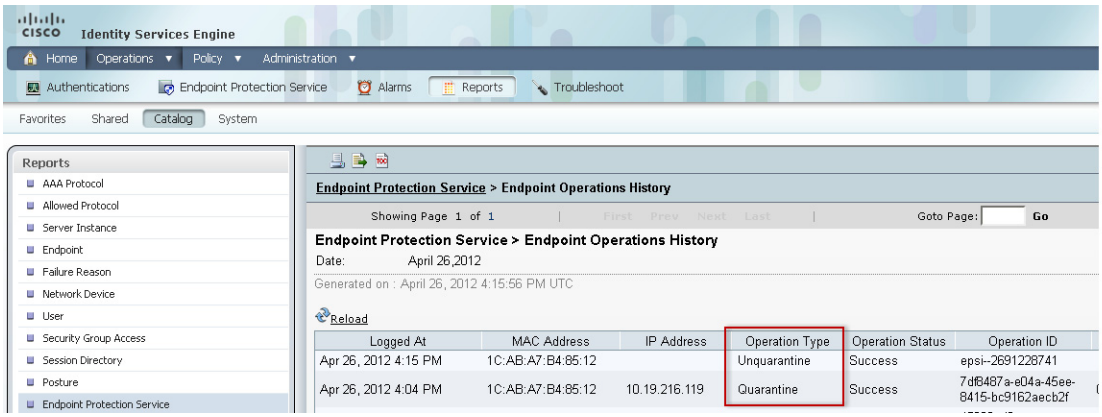
To unquarantine a device, enter the device's MAC address and select **Unquarantine** from the operation pull down menu, as shown in Figure 294.

Figure 294 Unquarantine a Device



The EPS activities are logged by ISE and can be reviewed by clicking **Operations > Reports > Catalog > Endpoint Protection Service**. Figure 295 shows quarantine and unquarantine events.

Figure 295 EPS Logs

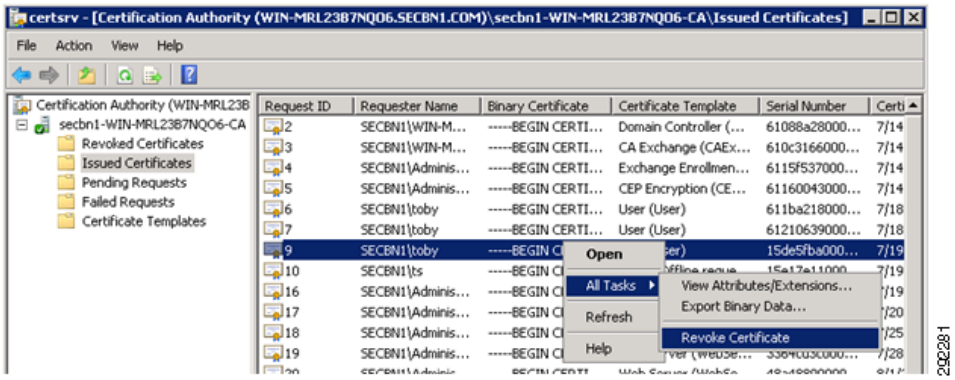


Revocation of Digital Certificate

Administrators also have the option of revoking an employee's digital certificate from the CA server to prevent further use by unauthorized devices. The CA server periodically publishes the Certificate Revocation List (CRL). ISE is configured to validate the certificate presented by the clients against the CRL list. If there is a match, then the ISE rejects the digital certificate presented by the client.

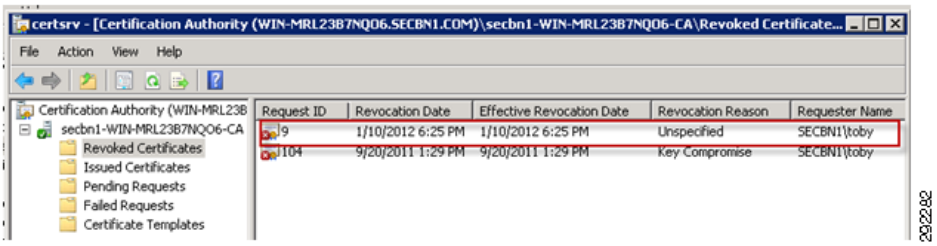
The first step is to revoke the digital certificate from the CA server. Figure 296 shows how to revoke the digital certificate for username "toby".

Figure 296 Revoking the Digital Certificate on the CA Server



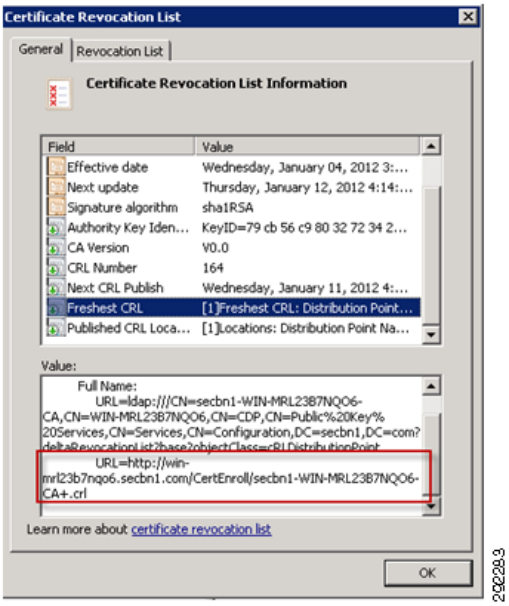
Once the above process is complete, the certificate serial number is added to the Certificate Revocation List (CRL). Figure 297 displays the CRL information.

Figure 297 Certificate Revocation List



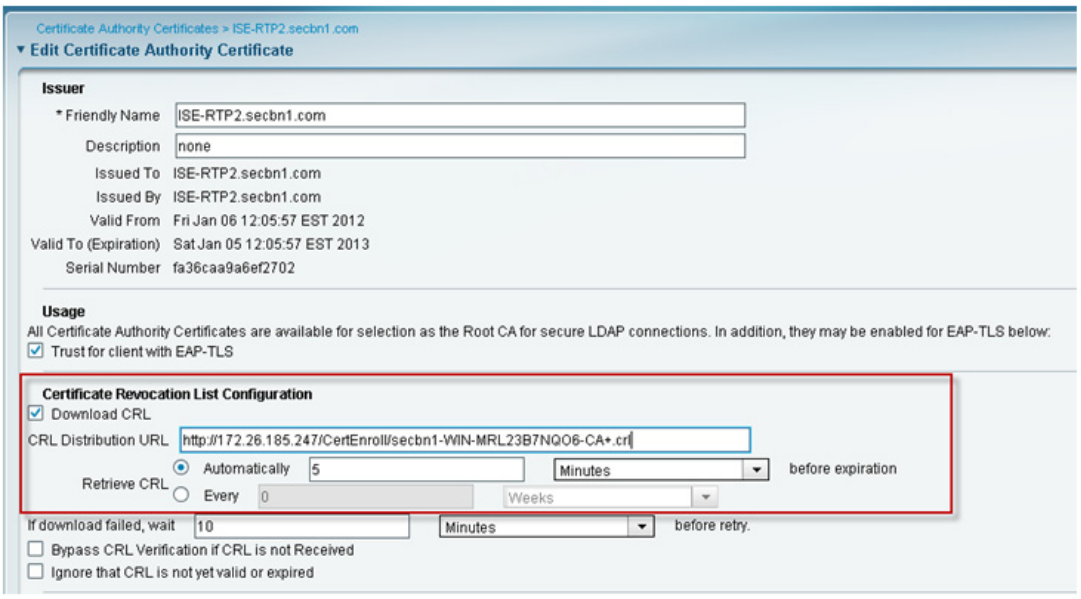
This information is periodically published by the CA server. Figure 298 shows the location of the CRL where the ISE can download the list.

Figure 298 CRL Distribution Point



The next step is for ISE to be configured with CRL distribution location so that it can periodically download the list and compare it with the certificates presented by the clients. Click **Administration > Certificates > Certificate Authority Certificates** and configure the CRL values, as shown in Figure 299.

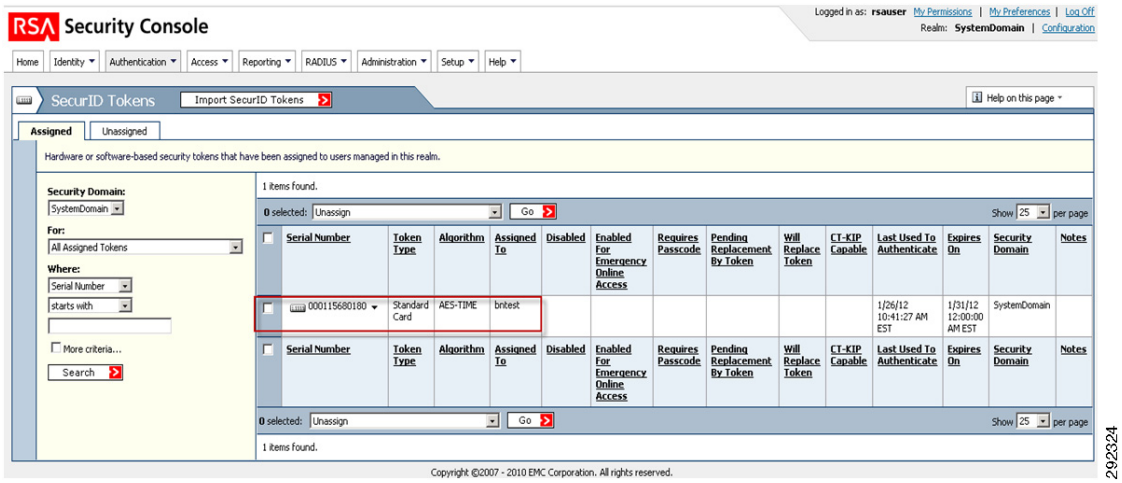
Figure 299 CRL Location Information on the ISE



Disable the RSA SecurID Token

When a device that has been previously provisioned is reported lost or stolen, the device must be denied access to prevent unauthorized access to the network. In addition, the remote user's RSA SecurID token must be disabled at the RSA Server so that the remote user cannot use the network. Figure 300 shows how to disable the RSA SecurID token at the RSA server.

Figure 300 Disabling the RSA SecurID Token



BYOD Network Management

Network Management for BYOD is separated into three sections:

- Cisco Prime Infrastructure Overview—A brief overview that covers the basic capabilities of Cisco Prime Infrastructure. The subsequent sections are focused on specific abilities of Prime Infrastructure directly related to BYOD. This overview describes the full capabilities of Prime Infrastructure.
- BYOD User and Device Tracking—Uses information from multiple components, consolidated by Cisco Prime Infrastructure, to identify and track end users and end devices on the network.
- BYOD Template-Based Configuration—Covers using Cisco Prime Infrastructure as a management tool for configuring and maintaining the BYOD wireless configurations across Cisco Wireless LAN Controllers (WLC).

This document does not cover the basic implementation of Prime Infrastructure and assumes the WLCs are already managed by Prime Infrastructure. For further information on Prime Infrastructure implementation, refer to the Prime Infrastructure Configuration Guide: http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html.

Key Acronyms and Terminology

Table 15 Acronyms and Terminology

Key Term	Explanation
Prime	Prime refers to Cisco Prime Infrastructure in this document. The Cisco Prime Family includes other products not covered in this document.
End Device	Also referred to as Endpoint. Both wired and wireless devices such as Android and Apple tablets and smartphones, wired IP phones, and laptops.
End User	Also referred to as User. Identified by “username” of one or more end devices.
WLC	Also referred to as Controller. Wireless LAN Controller
WLAN/SSID	WLAN (Wireless LAN) and SSID have a one-to-one relation and can be thought of as the same thing in this section.

Cisco Prime Infrastructure Overview

Cisco Prime Infrastructure is an exciting new offering from Cisco aimed at managing wireless and wired infrastructure while consolidating information from multiple components in one place. While allowing management of the infrastructure, Prime Infrastructure gives a single point to discover who is on the network, what devices they are using, where they are, and when. The capabilities of Prime Infrastructure and the other components featured go far beyond the focus of this document. A brief overview of Cisco Prime Infrastructure and supporting components follows.

Cisco Prime Infrastructure 1.2 is the evolution of Cisco Prime Network Control System 1.1 (NCS), adding additional infrastructure and wired device management and configuration capabilities while improving on existing capabilities in NCS 1.1.

Prime Infrastructure and Supporting Components

Cisco Prime Infrastructure interacts with many other components to be a central management and monitoring portal. Prime Infrastructure has integration directly with two other appliance-based Cisco products, the Cisco Mobility Services Engine and Identity Services Engine for information consolidation. Prime Infrastructure controls, configures, and monitors all Cisco Wireless LAN Controllers (WLCs), and by extension, all Cisco Access Points on the network. Prime Infrastructure also configures and monitors Cisco Catalyst switches and Cisco routers.

Figure 301 Prime Infrastructure Component Interaction Summary

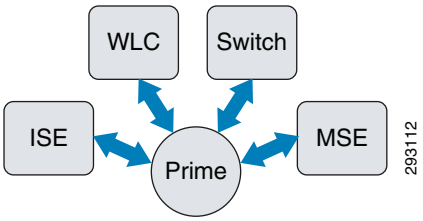


Table 17 Prime Infrastructure Components

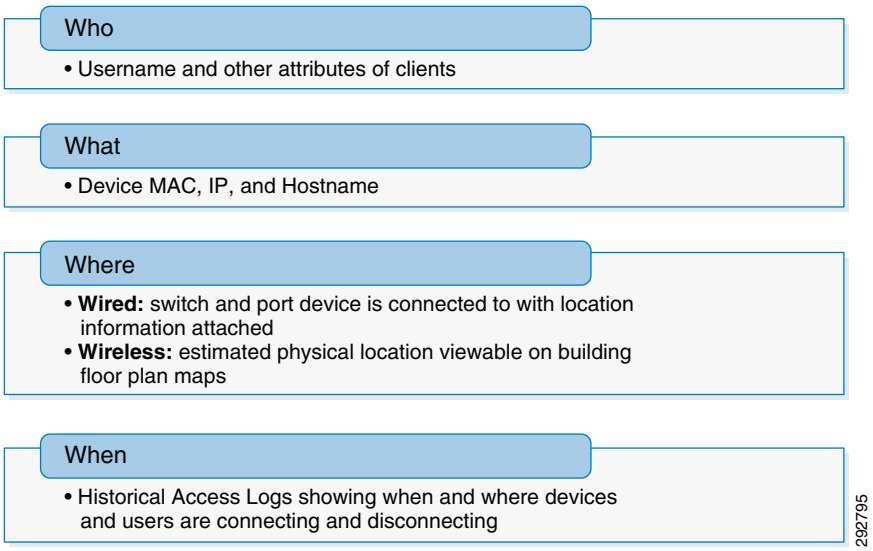
Prime Infrastructure	Cisco Prime Infrastructure is the core component that sends information to and consolidates information from the other four component types.
ISE	Cisco Identity Services Engine is the core component of BYOD for user and device authorization and access to the network. ISE provides user information to Prime Infrastructure.
WLC	Cisco Wireless LAN Controller is configured, controlled, and monitored by Prime Infrastructure. WLCs provide Prime Infrastructure with a wealth of real-time wireless environment and client device information.
Switch/Router	Cisco switches and routers are configured, controlled, and monitored by Prime Infrastructure. Wired device information is provided to Prime Infrastructure to be consolidated with wireless device information.
MSE	Cisco Mobility Services Engine complements Prime Infrastructure with current and historical location, usage, and other information for all devices Prime Infrastructure sees.

The following link has more information about Cisco Prime Infrastructure and the rest of the Cisco Prime family of products: http://www.cisco.com/go/prime.

BYOD User and Device Tracking

The ability to track users and devices on the wired and wireless networks is critical to knowing who is accessing the network, with what they are accessing it, where are they accessing it, and when they accessed it.

Figure 302 Who, What, Where, and When Summary



Understanding who is accessing the corporate network, what they are using, and where they are connected allows customers to better understand:

- Location and movement of employees and devices on the network
- Suspicious or unauthorized access of the network
- Location of missing or stolen assets, such as in a college campus
- Location of unknown devices on the network
- Current utilization of the network

Adding historical logging of when users and devices access the network allows:

- Persistent records of when users and devices accessed the network and their specific locations
- Searchable historical data of user and device access for tracking and troubleshooting issues
- Historical port utilization data

Components

Cisco Prime Infrastructure is the central portal for user and device tracking. Prime Infrastructure uses information from multiple places to give a single, consolidated view of current and historical user and device access to the network. The five main components needed for User and Device tracking of both wired and wireless users are listed below with brief summaries of each. Figure 303 adds to Figure 301

showing how the components cover the Who, What, Where, and When aspects of user and device tracking.

Figure 303 Prime Infrastructure Component Interaction Summary for User and Device Tracking

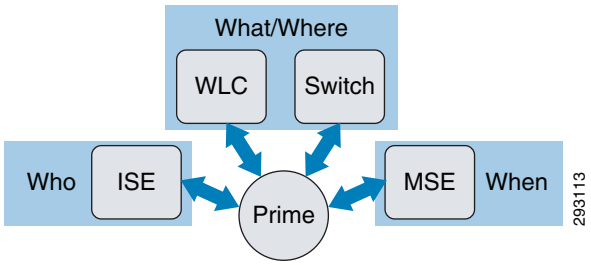


Figure 304 shows a more detailed view of how Prime Infrastructure interacts with the rest of the architecture.

Figure 304 Prime Infrastructure Interaction with Infrastructure Components

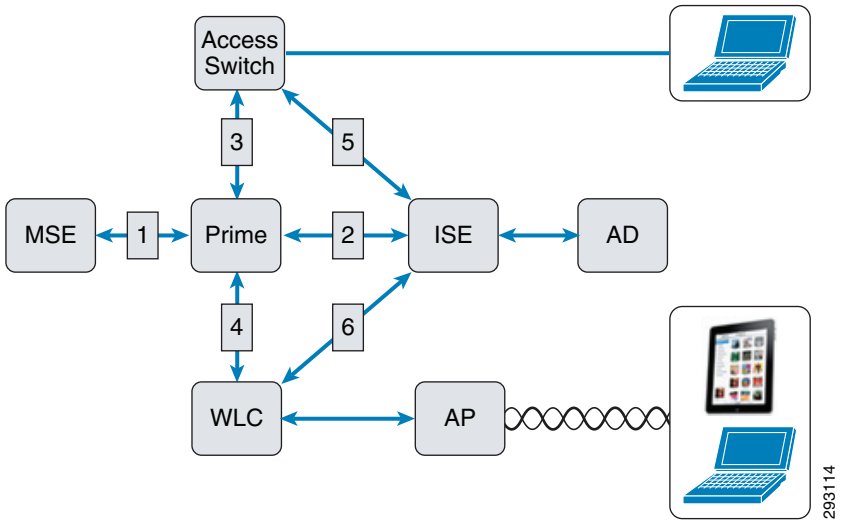


Table 18 Prime Infrastructure Interaction with Other Infrastructure Components

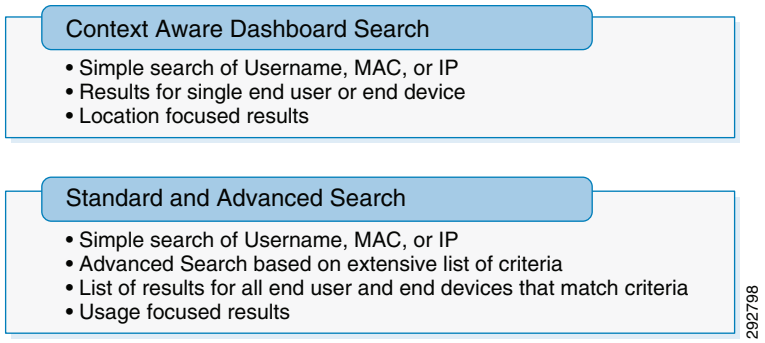
	Components	Communication
1	Prime—MSE	Prime receives urrent and historical location information for mobile devices
2	Prime—ISE	Prime receives user information including username and device MAC and authentication history
3	Prime—Switch/Router	Prime receives wired device information including port and MAC. Prime sends/receives component configuration.
4	Prime—WLC	Prime receives wireless user and extensive device information. Prime sends/receives component configuration.
5	Switch—ISE	RADIUS authentications
6	WLC—ISE	RADIUS authentications

To locate and track users and devices, Prime Infrastructure pulls information from all of these sources, consolidating it based mainly on common MAC. Prime Infrastructure is device focused and displays detailed reports based on a particular device. Prime Infrastructure also has the ability to show all devices with which a particular user accesses the network, giving the ability to track a particular user across multiple wireless and wired devices.

Locating Users and Devices

There are two basic ways to display information on users and devices. Both options are considered "Search" options, although the abilities to filter and display based on an extensive list of criteria goes far beyond what most would consider a simple search option.

Figure 305 Types of Search

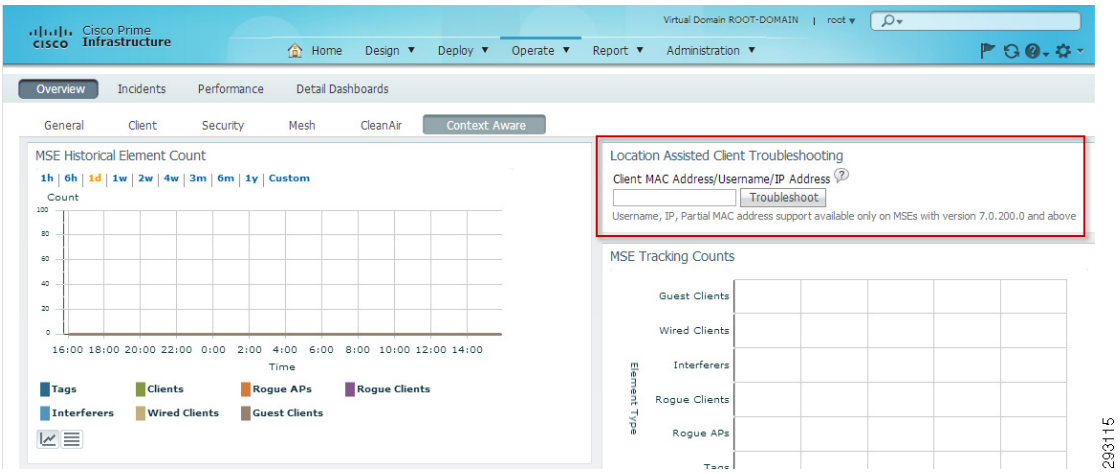


Context Aware Dashboard Search

Context Aware search is used to display information on a single device based on current MAC, IP, or Username of the end user of the device. While limited in how you can search and what is displayed, this option does give you a slightly different view of location information compared to the standard search.

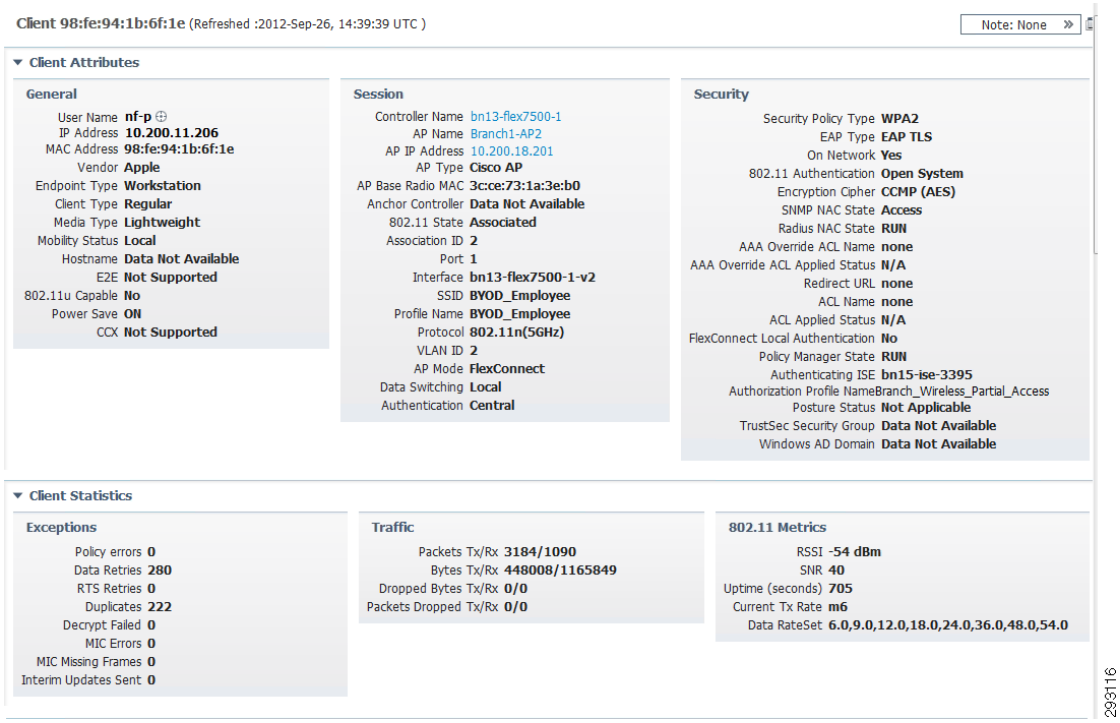
The Context Aware Dashboard in Figure 306 has a search box titled "Location Assisted Client Troubleshooting", which is where the search is executed. The search instantly resolves the MAC, IP, or Username to the device and display that device only.

Figure 306 Context Aware Dashboard



The results shown in Figure 307 are common to both types of search and give quite a bit of current information about the device and end user of it, if there is one.

Figure 307 Context Aware Search Standard Results

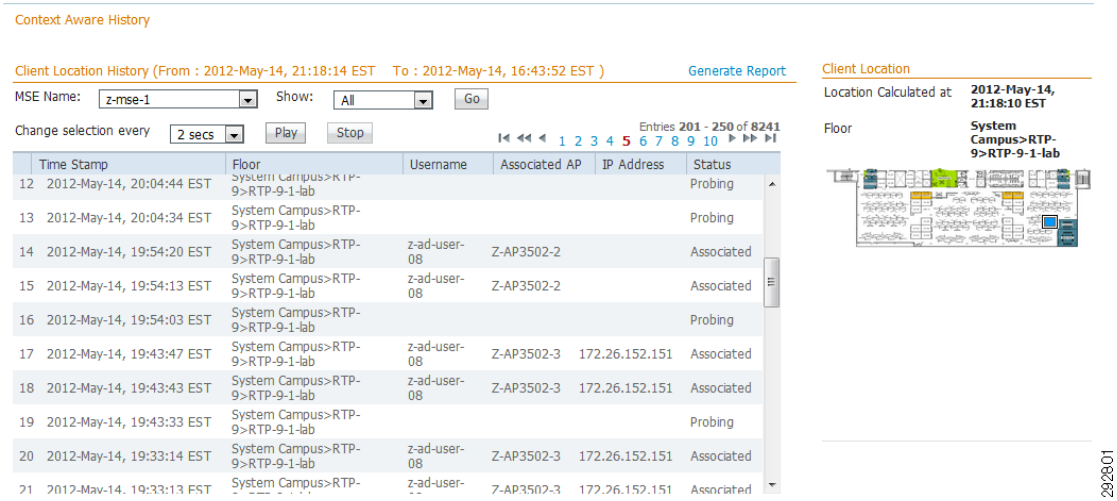


The information in the search results unique to the Context Aware Search is location based. Standard and Advanced Search show “Association History”, which includes location, but not in the same format.

Context Aware Search results give you the ability to easily see exactly where a device was at a given time as well as show historical motion of the device. Using the “Play” feature, the device location is shown being updated on a map for a visual representation of movement, which can be accurate down to several feet in a properly implemented wireless network.

Figure 308 shows the location results with a blue square showing current location on the floor plan map adjacent. Pressing “Play” would show the blue square moving as location references were cycled through.

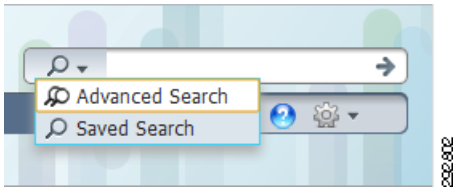
Figure 308 Context Aware Search Location Results



Standard and Advanced Search

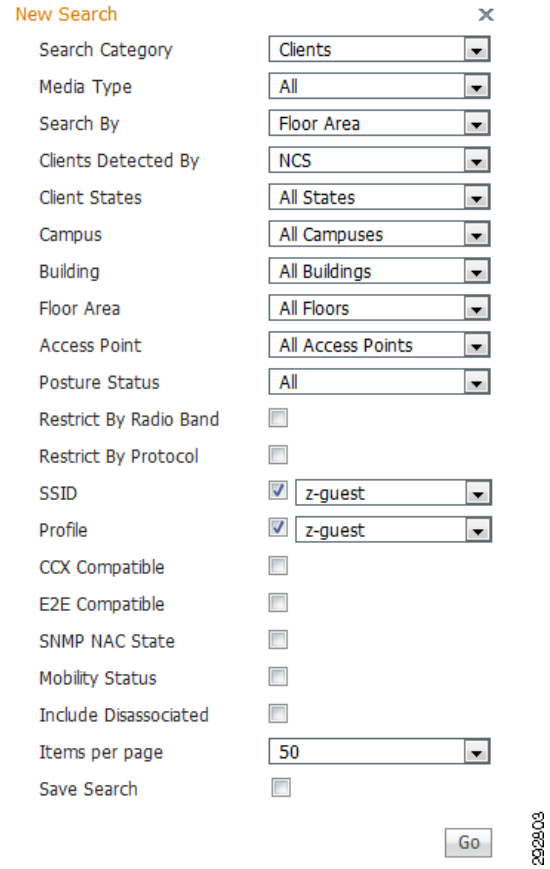
In addition to searching for clients or devices using the Context Aware Dashboard, Standard and Advanced Search may be performed in the top right corner of the Prime Infrastructure interface, visible at any time. Much more granular searches may be performed using the Advanced Search option shown in Figure 309. Search results are more device usage focused with the Standard and Advanced Search, but still contain location information.

Figure 309 Standard and Advanced Search Box



With Advanced Search, results for many end users or end devices that meet a particular set of criteria may be displayed instead of looking for one particular user or device. Parameters such as physical location, type of user, SSID, and even posture/authentication status may be used. Figure 310 shows a subset of criteria available.

Figure 310 Advanced Search Criteria

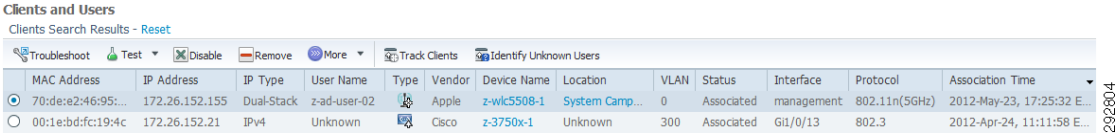


The form above is dynamic, changing as selections are made, which means this image shows only a subset of the criteria available for the "Clients" category, which in this case refers to both end devices and end users.

Additional search criteria and information may be found in the Cisco Prime Infrastructure Configuration Guide: http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html.

Figure 311 shows the search results list, which contains both wired and wireless users unless one type is filtered out. In this example two devices are shown, the first a wireless device and the second wired.

Figure 311 Standard and Advanced Search Results List



An extensive amount of information is available from just the search results screen. The result columns may be customized and results list sorted by any of those columns. Figure 312 shows a list of available columns.

Figure 312 Search Results Columns

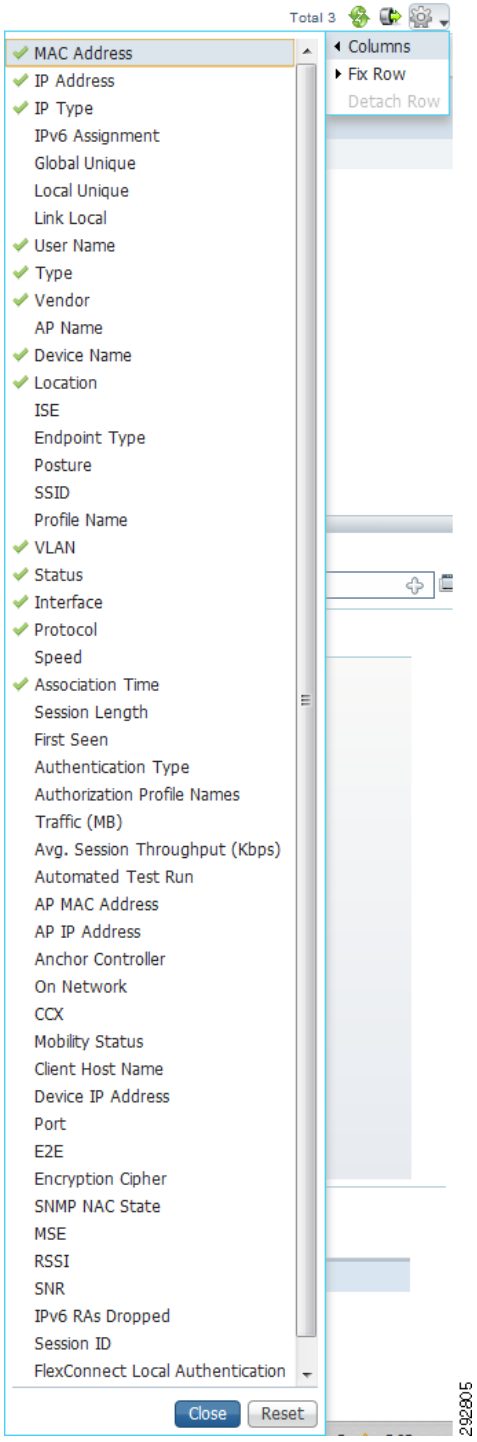


Figure 313 through Figure 318 show examples of basic and extended information shown for individual devices selected from the search list.

Figure 313 shows the same basic end user and end device information as the Context Aware Search discussed earlier.

Figure 313 General User and Device Details

Figure 314 shows association times, durations, and locations, which is similar but not the same as the location history with the Context Aware Search.

Figure 314 Device Association History

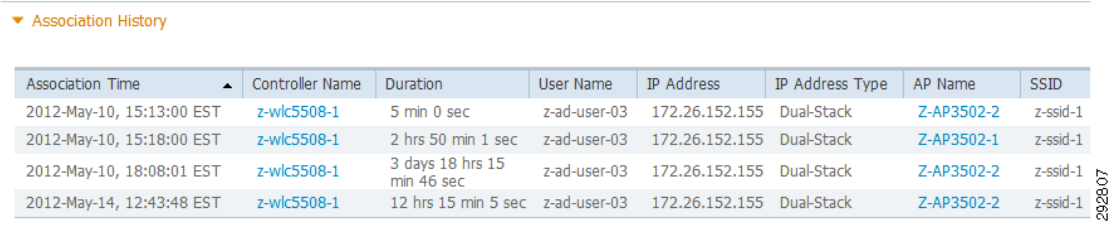


Figure 315 is pulled directly from ISE and shows recent authentication successes and failures.

Figure 315 Device Authentication History

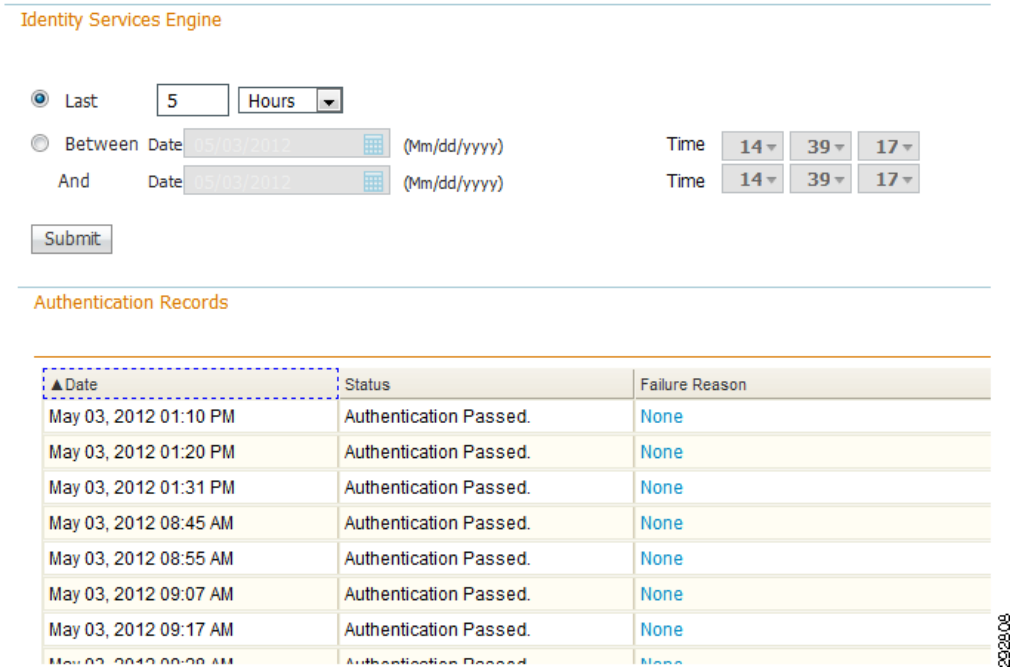


Figure 316 shows signal quality for various, changeable time frames in graph format.

Figure 316 Device Signal Quality and Usage History

Figure 317 shows the device in its current location, along with any additional information chosen. In this example, only heat map and AP location is selected, but many other items are available for display, such as interfering devices and other clients.

Figure 317 Floor Plan Heat Map with APs and Client Device

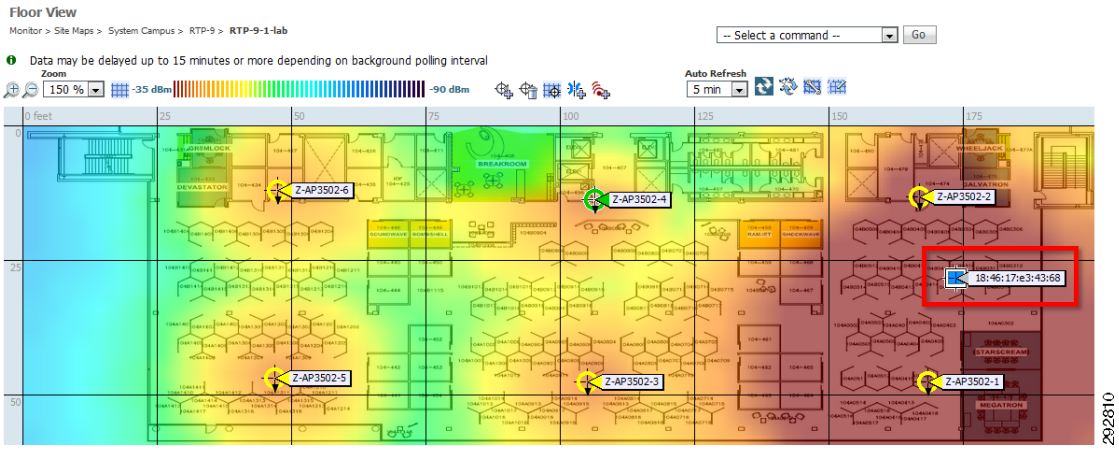
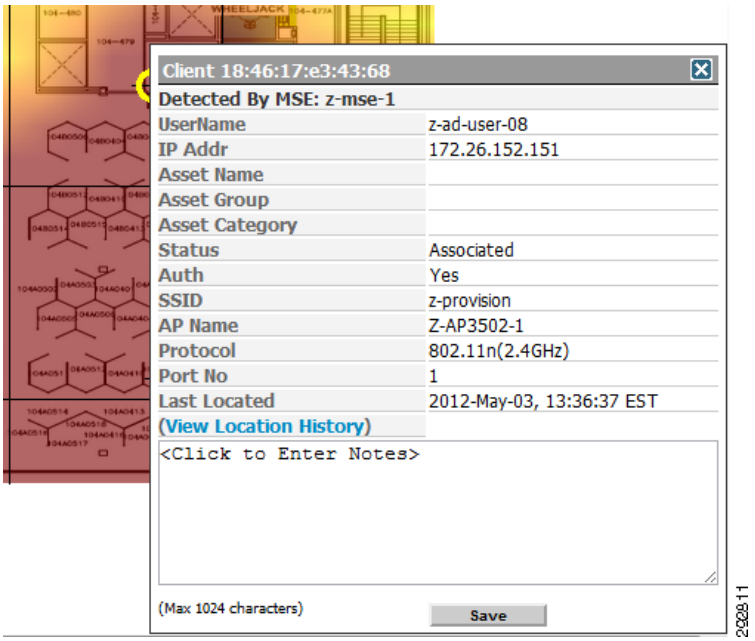


Figure 318 shows details of any device shown on the heat map.

Figure 318 Device Detail Pop-up from Heat Map



BYOD Template-Based Configuration

This section covers the use of Cisco Prime Infrastructure to deploy and maintain configurations to Cisco Wireless LAN Controllers (WLCs) matching the BYOD configurations referenced in this document.

Cisco Prime Infrastructure has the ability to control configuration of Cisco Wireless LAN Controllers (WLCs) directly or through the use of templates. One template will not configure the entire controller. Templates are separated out to granularly cover each feature of the controller. Templates exist for just about every small feature that can be implemented on the controllers and many portions of the templates can be modified during deployment to accommodate unique settings in WLCs. Templates can be configured for a common configuration across all WLCs as well as be implemented across a sub-set of WLCs or individual WLCs.

Note Each WLAN has exactly one SSID and the two terms may be thought of as being the same thing for simplicity in understanding this content: **WLAN = SSID**.

Template-based configuration has a number of advantages compared to individual configuration of WLCs:

- Consistent Configuration of WLCs
- Multiple Templates for Variations of Deployment
- Rapid Deployment of New or Replacement Components
- Staged Rollout of Configuration Changes with Rapid Rollback

Consistent Configuration of WLCs

Inconsistencies in configuration can easily occur when configuring multiple WLCs through their local Web-based administrative interfaces. Inconsistencies can have far reaching negative impact on WLAN functionality, security, and performance.

Inconsistencies in even the order of configuration can sometimes have serious impacts. For example, configuring multiple WLANs in different orders on different controllers will cause the WLAN IDs (an integer that uniquely identifies each WLAN) to be inconsistent. WLAN IDs are used by ISE to determine how the client should be treated. Inconsistent WLAN IDs may result in a client attaching to a particular SSID and being assigned access as if they were attached to a different SSID.

One important note here, however, is that Prime Infrastructure will have the controller auto-assign the WLAN ID. If the base configuration of the controllers starts in an inconsistent state, such as a WLAN existing on one controller that does not exist on another, the WLAN IDs will be set inconsistently when applied from Prime Infrastructure. Checks should be done to ensure the WLAN IDs are consistent across all controllers. See the WLAN ID Implementation Notes in Configuring the Infrastructure for more information.

Multiple Templates for Variations of Deployment

Variations in deployment may be required for some features of WLCs based on model or location in the network. If a WLC is being used for dedicated guest access, its configuration for certain features would differ from other WLCs on the network, requiring some variation of templates.

Prime Infrastructure supports multiple templates for the same feature, allowing templates to be created with variation for WLCs. Templates may be applied to all WLCs or individually selected WLCs at the time of application.

Rapid Deployment of New or Replacement Components

By creating templates for WLC configuration, new and replacement WLCs may be rapidly configured from the latest templates, reducing time to deploy and eliminating errors from misconfigurations.

Staged Rollout of Configuration Changes with Rapid Rollback

Multiple templates for a specific feature can be created allowing an altered configuration to co-exist with the current configuration in template form. The new configuration template can then be tested on one or more WLCs with ease of rollback to the previous configuration template should issues arise.

Note The acronym WLC (Wireless LAN Controller) is frequently used in this document while some of the interfaces shown use the common term "Controller". In this document "WLC" and "Controller" refer to the same thing: **WLC = Controller**.

Template Creation and Implementation

Template creation and implementation is a fairly straightforward process in Prime Infrastructure with a few caveats. The templates and configurations that follow are specific to the BYOD solution in this document and are but a tiny subset of the many settings and features that are needed for implementing an enterprise wireless network.

This section assumes the WLCs are already managed by Prime Infrastructure. For further information on Prime Infrastructure implementation, refer to the Prime Infrastructure Configuration Guide: http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html.

Template Creation

Template creation for WLC configuration may be handled in one of three ways:

1. Create new templates directly in Prime Infrastructure.
2. Configure a WLC through Prime Infrastructure and then create templates from that configuration.
3. Configure a WLC through the local WLC web interface and then create templates from that configuration.

The following material focuses on option 2, configuring a WLC through Prime Infrastructure followed by creation of templates to configure additional WLCs and make changes to the original WLC. This approach would seem the most logical since it incorporates option 3 as well if the WLC were already configured, as shown in Configuring the Infrastructure.

This approach would also be appealing to someone wanting to learn the interface and operation of Prime Infrastructure and the WLC at the same time, using a separate WLC to create the configurations and templates to be deployed in production at a future date. For base template creation, functional trials, and understanding of the solution, most of the features covered in this document may be deployed using a relatively inexpensive Cisco 2504 with the base license and a single AP. Two key features the 2504 lacks as part of the BYOD solution are the ability to act as a DMZ Guest WLC and the ability to rate limit traffic. Both of those features are covered in BYOD Guest Wireless Access. All other features and abilities in the BYOD solution are supported on this platform.

Due to the extensiveness of configuration for a FlexConnect environment, not every step is shown for the initial configuration. Following the steps in Configuring the Infrastructure using the Prime Infrastructure interface instead of the WLC interface directly should be fairly straightforward. Minor differences in location of options and features in the Prime Infrastructure interface are shown.

Using option 2 from above (Configure a WLC through Prime Infrastructure and then create templates from that configuration) the following steps are used. If beginning with a WLC that was directly configured from the material inConfiguring the Infrastructure, just skip steps 1 and 3.

- Step 1—Configure Base Network Connectivity on the New WLC
- Step 2—Add the WLC as a Managed Device to Prime Infrastructure
- Step 3—Using Prime Infrastructure, Directly Configure the WLC
- Step 4—Create Templates from the Configured WLC
- Step 5—Deploy Templates on One or More WLCs

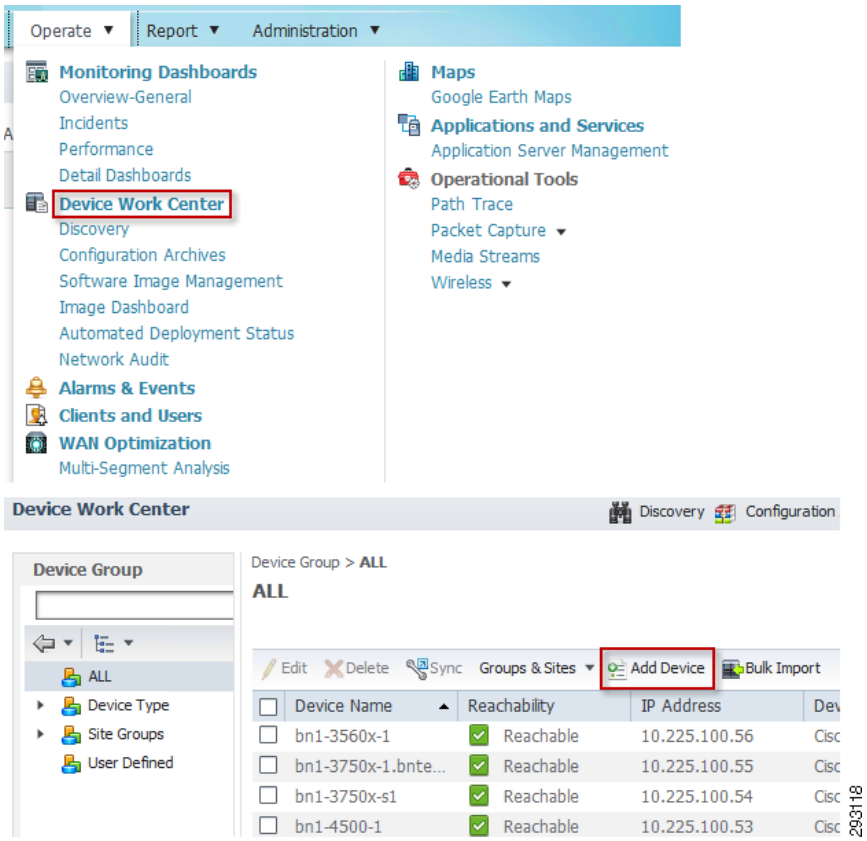
Step 1—Configure Base Network Connectivity on the New WLC

This step should be completed with documentation for the WLC you are implementing. Documentation for all Cisco WLCs can be found at:
http://www.cisco.com/web/tsweb/redirects/mm/support/wireless.html.

Step 2—Add the WLC as a Managed Device to Prime Infrastructure

In Prime Infrastructure, use the Device Work Center and manually add the device, as shown in Figure 319.

Figure 319 Device Work Center—Add a Device



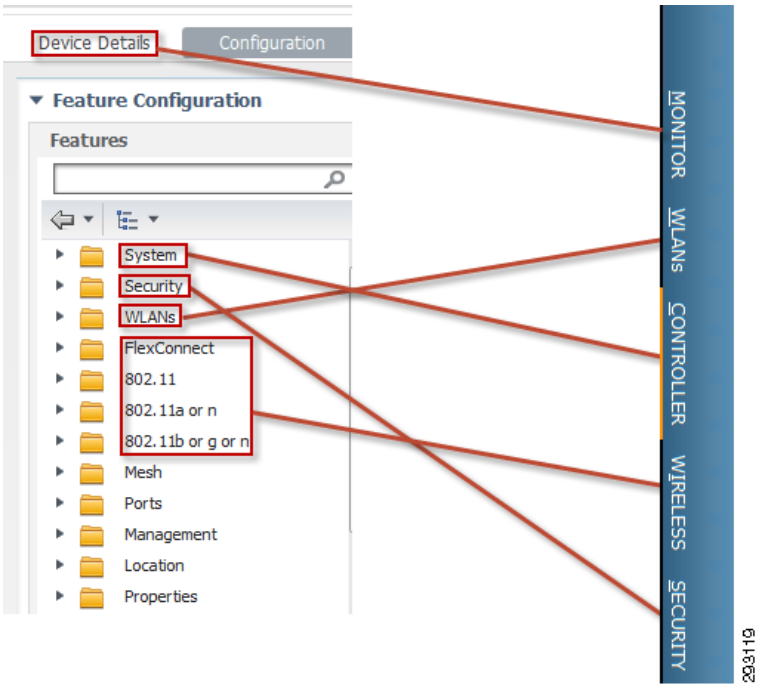
You do not need to specify the WLC type as Prime Infrastructure will determine it during the synchronization process. Alternatively, the WLC may be added through the discovery process, which is not shown.

After the WLC is added it will synchronize any existing configuration with Prime Infrastructure. This process should take only a couple of minutes and show a Device Status of "Managed" in the Device Work Center. It will also be placed in the appropriate Device Type folder, which can be expanded on the left side of the Device Work Center screen shown in Figure 319.

Step 3—Using Prime Infrastructure, Directly Configure the WLC

The WLC may now be directly configured in the Device Work Center, similar to being on the Web-based interface of the WLC itself, by selecting the WLC and then the Configuration tab in the section below. The configuration interface is very similar, but not exactly the same. Figure 320 shows how the WLC interface main categories map to the Prime Infrastructure categories.

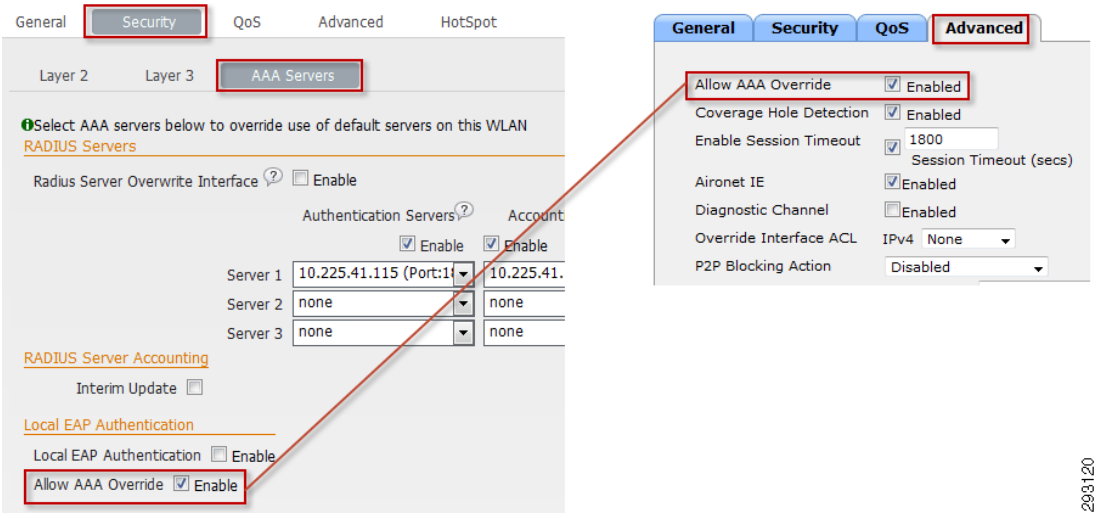
Figure 320 Mapping of WLC Interface Categories to Prime Infrastructure Categories



Following the steps in Configuring the Infrastructure, the WLC may be configured. Be aware that one significant feature, AAA Override, is in a different location.

The feature AAA Override is shown in the Advanced tab of the WLAN settings when configuring through the WLC interface. This same feature is in the Security tab of the WLAN settings when configuring through Prime Infrastructure, as shown in Figure 321.

Figure 321 AAA Override on Advanced Tab of WLAN Settings

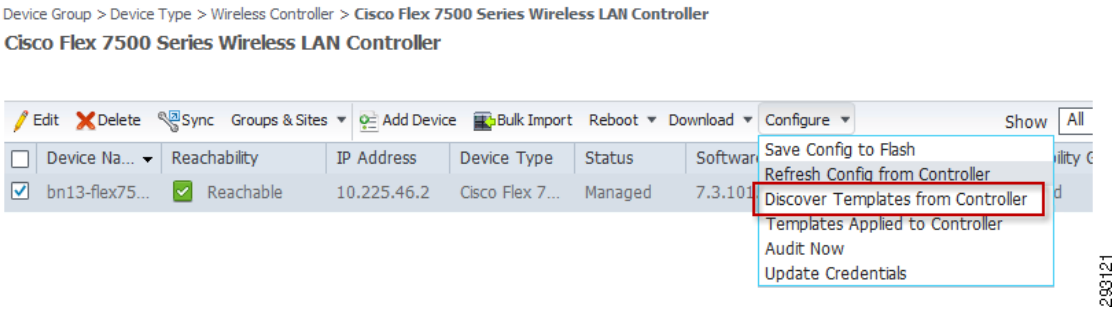


Take note of the WLAN ID caveat at the end of this section as it is important to both the creation of WLANs initially as well as template-based deployment of WLANs.

Step 4—Create Templates from the Configured WLC

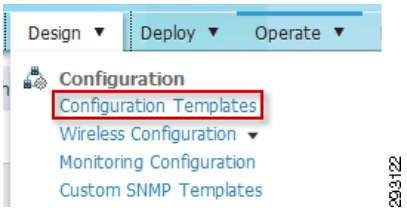
Creating templates from a configured WLC is a fairly simple process. An automated process creates templates of everything in the WLC that can have a template created. To accomplish this, go to the device in Device Work Center, the same place as the last step. Select the configured WLC and choose Configure and then Discover Templates from Controller, as shown in Figure 322.

Figure 322 Discover Templates from Controller



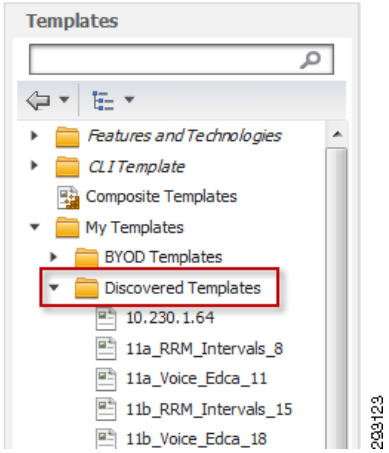
After the template discovery process completes, the templates are found in the Configuration Templates section in the Design section from the top menu, as shown in Figure 323.

Figure 323 Configuration Templates



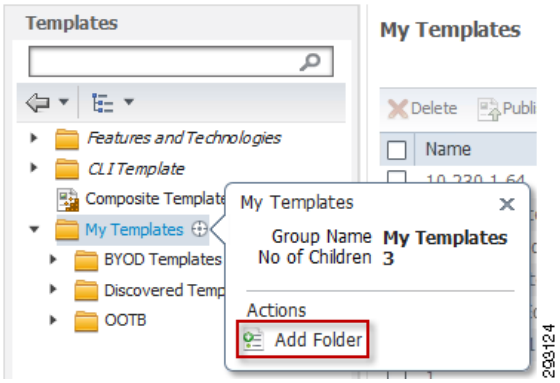
The newly discovered templates will be shown under My Templates, then Discovered Templates as shown in Figure 324.

Figure 324 Discovered Templates



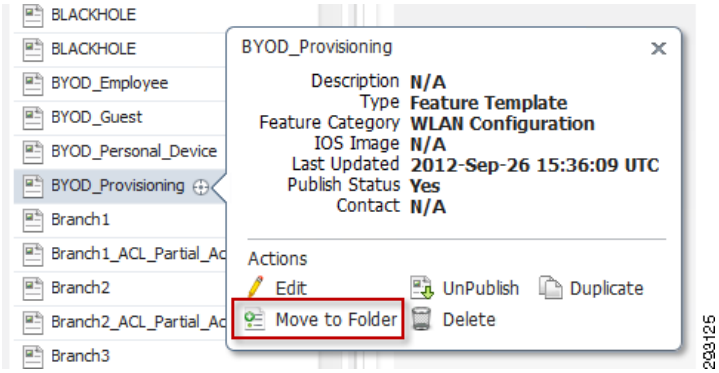
There will be many templates shown in this section, but only a small number of them are really needed. Before any customization or deployment of templates occurs, it is highly recommended to organize the needed templates into a custom folder. First, create a new folder by placing the mouse pointer next to My Templates, which will pop up a box. Click **Add Folder**, as shown in Figure 325.

Figure 325 Add Folder



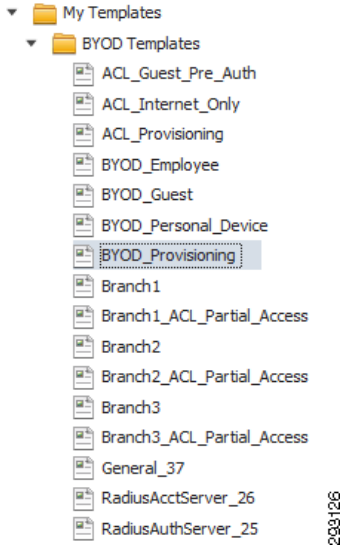
After creating the folder, in this case named BYOD Templates, place the pointer next to each of the desired templates, one at a time, and click **Move to Folder**, moving them to the newly created folder, as shown in .

Figure 326 Moving Templates



Once complete, all the desired templates will show up in the new folder, ready for editing and deployment, as shown in Figure 327.

Figure 327 BYOD Templates



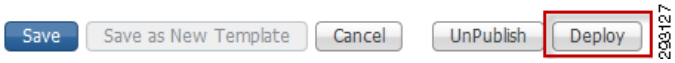
Step 5—Deploy Templates on One or More WLCs

It is fairly straightforward to deploy standard templates with no unique settings. Deploying templates that require unique configurations, such as FlexConnect Groups, is more involved.

A FlexConnect Group has specific APs associated with it, which will be different from WLC to WLC. A simple static template would not be particularly useful and the deployment must accommodate customization. The following template deployment is of a FlexConnect Group, showing the most complex type of deployment as an example.

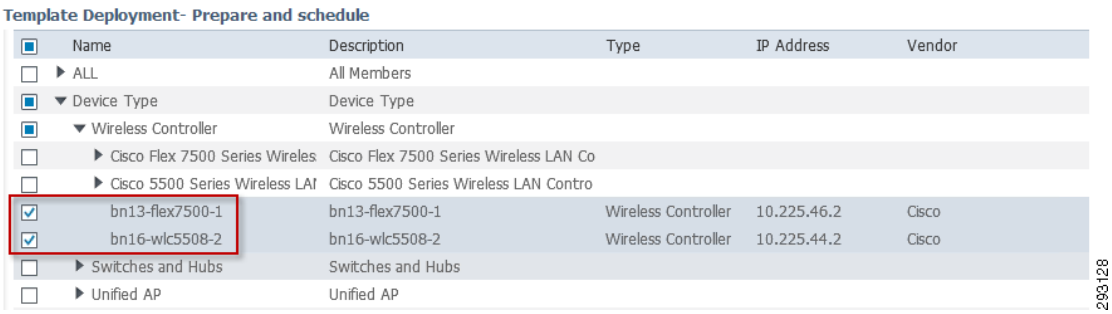
At the bottom of every template is a button to deploy it, shown in Figure 328, which when clicked shows the deployment screen.

Figure 328 Deploy Button



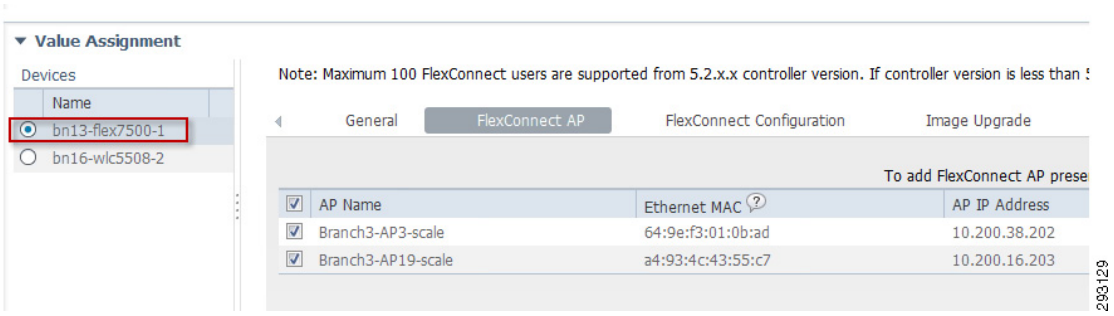
When a FlexConnect Group template is launched, the target WLCs must be chosen. In this example two WLCs of different types are selected, as shown in Figure 329.

Figure 329 Deployment Screen



When selected, you see the Value Assignment screen, shown in Figure 330. This section allows you to assign values and resources to each WLC independently. In this example APs may be added to the FlexConnect Group separately for each WLC. The APs are added by clicking **Add AP** on the far right of the screen (not shown) which will bring up a list of all APs that are visible to Prime Infrastructure.

Figure 330 Value Assignment



After completion of customization, the template can be deployed immediately or scheduled.

Caveat 1—WLAN ID

WLAN ID is used by ISE in determining what SSID (WLAN) clients are using to connect to the network. This ID is unique to each WLAN on each controller, so ensuring each WLAN has the same WLAN ID on each controller is essential for proper operation and security.

Ensuring this can become complex for large enterprise customers with multiple WLCs. Take note of the following:

- Prime Infrastructure cannot set the WLAN ID and lets the WLC assign the WLAN ID.
- WLCs with existing WLANs increment to the next available integer.
- Creating a WLAN using the WLC web interface directly allows the WLAN ID to be chosen.
- WLAN IDs cannot be changed once the WLAN is created.

The following simple example shows the issue:

- WLC A has no WLANs defined.
- WLC B has WLAN “Special-SSID” with WLAN ID 1.

Using Prime Infrastructure to create a new WLAN, “Employee-SSID”, across all WLCs results in it being assigned WLAN ID 1 on WLC A and WLAN ID 2 on WLC B.

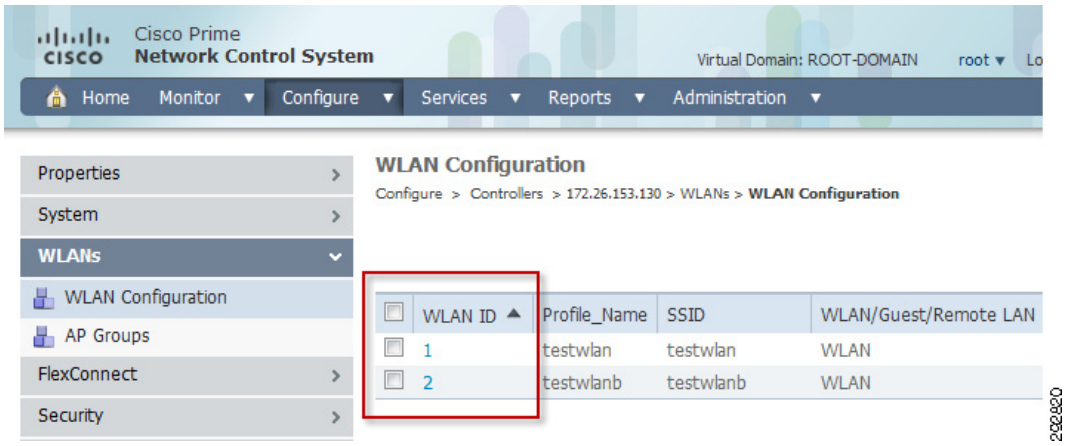
- WLC A
  - WLAN “Employee-SSID” WLAN ID 1
- WLC B
  - WLAN “Special-SSID” WLAN ID 1
  - WLAN “Employee-SSID” WLAN ID 2

To avoid this potentially serious mismatch, it is essential to audit existing WLCs for WLANs and prepare the WLCs for template-based WLAN configuration. Using only Prime Infrastructure and not the WLC interface, the following summarized steps (followed by detailed steps) prevent WLAN ID inconsistencies.

Detailed Steps for Ensuring WLAN ID Consistency

1. Add all WLCs to Prime Infrastructure and synchronize their configurations.
2. Using Prime Infrastructure, look at the WLANs on each WLC to determine the highest WLAN ID in existence, as shown in the example in Figure 331. In this example, two WLANs exist on a particular WLC.

Figure 331 WLAN ID List



3. Create disabled dummy WLAN templates and apply to WLCs to bring them all up to the same highest WLAN ID.

   The dummy WLAN settings are irrelevant as long as they are created in the "disabled" state. In this example, two dummy WLAN templates must be created and applied to all WLCs with no WLANs.

   As an alternative to creating the dummy WLANs, the existing WLANs may be deleted and re-created with higher WLAN IDs manually set directly on the WLC. Deletion and re-creation is the only method currently available for changing the WLAN ID. Changing the WLAN ID on an existing WLAN is not possible.
4. Create the new WLAN templates for BYOD configurations and apply to all WLCs.
5. Check WLCs to ensure WLAN IDs are consistently assigned across all WLCs.
6. After WLAN templates are applied, dummy WLANs may be deleted if desired.

Note When adding a new WLC to the network, dummy WLAN templates must be applied to them before applying BYOD WLAN templates. Since the WLAN ID is assigned sequentially, BYOD WLAN templates must always be applied in the same order.

Scalability Considerations

This section explores several design elements that are important to consider when expanding BYOD deployments to include a large number of users. Distributing ISE functionality across multiple hosts enables increased scalability, availability, and performance. With any distributed system it is important to consider the topic of load balancing to ensure the most efficient use of the individual nodes. With larger deployments it is also important to understand how to enforce policy without impacting network performance. This section provides design considerations and guidelines.

Distributed ISE Deployment

Cisco ISE provides a highly scalable architecture that supports both standalone and distributed deployments. Distributed mode of operation is used to support a large number of endpoints and also for increased availability and performance.

The following document provides guidelines on sizing based on the number of endpoints required: http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_deploy.html.

The ISE functionality can be distributed across multiple nodes, allowing for increased availability and scalability. Distributed deployments support three different ISE personas:

- Administration (PAN)—The Administration node handles all system level configurations. There can be one primary and one secondary Administration node in a distributed deployment.
- Monitoring (MNT)—The Monitoring node handles log collection and provides monitoring and troubleshooting tools. There can be one primary and one secondary Monitoring node in a distributed deployment.
- Policy Service (PSN)—The Policy Service node provides authentication, authorization, guest access, client provisioning, and profiling services. There can be multiple Policy Service nodes in a distributed deployment. To support a medium size BYOD deployment, both Administration and Monitoring personas can be deployed on a single node while dedicated Policy Service nodes can handle AAA functions. For large BYOD deployments, the Monitoring persona can be implemented on a dedicated node providing centralized logging functions.

Virtual ISE Specifications

Table 19 outlines the hardware specifications for ISE appliances. These specifications may be used to guide virtual machine (VM) sizing when deploying VMware-based ISE.

Further details about VM requirements can be found at: http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_vmware.html#wp1110217.

Table 19 Appliance Hardware Specifications

Platform	ISE-3315(small)	ISE-3355(Medium)	ISE-3395(Large)
Processor	1 x Quad Core Intel Core 2 CPU Q9400 @ 2.66 GHz (4 total cores)	1 x Quad Core Intel Xeon CPU E5504 @ 2.00 GHz (4 total cores)	2 x Quad Core Intel Xeon CPU E5504 @ 2.00 GHz (8 total cores)
Memory	4Gb	4Gb	4Gb
Hard Disk	2 x 250-GB SATA HDD (500 GB total disk space)	2 x 300-GB SAS drives (600 GB total disk space)	4 x 300-GB SFF SAS drives (600 GB total disk space) *
Ethernet NICs	4x Integrated Gigabit NICs	4x Integrated Gigabit NIC	4x Integrated Gigabit NICs

Consider the following when sizing the VMs against the hardware appliance specifications:

- VM resources need to be dedicated, not shared or oversubscribed across multiple VMs.
- PSNs on a VM can be deployed with less disk space than the PAN or MNT nodes.
  - Recommended minimum storage for PSN is 100Gb.
- VMs can be configured with 1-4 NICs.

- Recommended to allow for 2 or more NICs.

Table 20 shows the validated deployment of eight VM ISE nodes, which are based on the ISE-3395 appliance.

Table 20 ISE VM Details

Hostname	IP Address	Node Persona	HD
ise-vm-adm-pri	10.230.113.201	PAN	600Gb
ise-vm-adm-sec	10.230.113.202	PAN	600Gb
ise-vm-mon-pri	10.230.113.203	MNT	600Gb
ise-vm-mon-sec	10.230.113.204	MNT	600Gb
ise-vm-psn-1	10.230.113.205	PSN	250Gb
ise-vm-psn-2	10.230.113.206	PSN	250Gb
ise-vm-psn-3	10.230.113.207	PSN	250Gb
ise-vm-psn-4	10.230.113.208	PSN	250Gb

Virtual ISE Configuration

The section covers the installation of ISE on a virtual machine.

Create VMware Server

Create the VMware servers that will be used to install the Cisco ISE software. The detailed guide for this can found be at:
http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_vmware.html#wp1053064.

Installing ISE on VMware System

To install the Cisco ISE software on the newly created VMware servers, view the procedure documented at:
http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_vmware.html#wp1053177.

Configuring the Distributed Deployment

To configure the Cisco ISE distributed environment, refer to:

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_dis_deploy.html#wpxref26216.

ISE and Load Balancing

When distributing ISE functionality across multiple nodes, it is important to be able to load balance the workload across the PSN nodes. This results in optimal usage of resources and faster responses to the end users. Load balancing also provides advantages for servicing individual nodes without service disruption to users.

This section provides two different design options to load balance traffic across a distributed ISE deployment.

Load Balancing Design Considerations

The following are two methods that can be used to load balance RADIUS requests from clients across multiple Policy Service nodes:

- IOS-based RADIUS SLB
- Application Control Engine (ACE)-based RADIUS SLB

Both options provide the capability for load balancing RADIUS sessions across PSNs. The ACE offers additional capabilities to load balance HTTP/S that is used for device onboarding and guest access. A well-designed load balanced implementation simplifies the operation and deployment of all access devices. Considerations for certificate management and address translation are discussed to ensure a successful load balanced deployment.

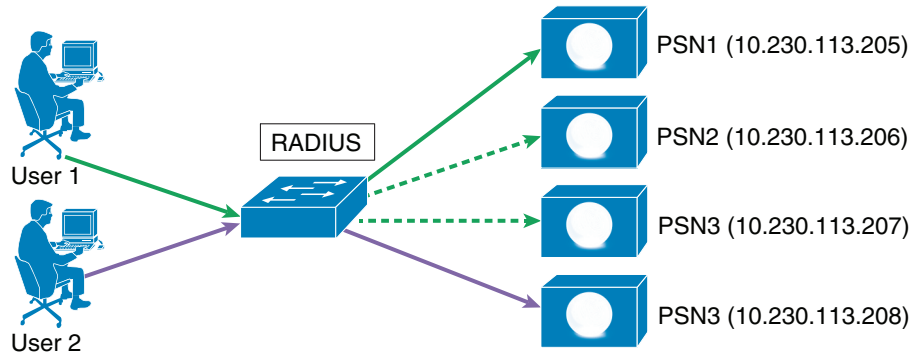
IOS-based RADIUS SLB

A simple method of load balancing RADIUS requests to the PSN is to configure each Network Access Device (NAD), in this case an access switch, with multiple RADIUS servers. The switch controls the load distribution of AAA requests to all PSNs without a dedicated Load Balancer.

There are four Policy Service nodes in this deployment, so we would configure the radius-server hosts on one switch as shown in Figure 332.

The **radius-server load-balance method least-outstanding batch-size 5** command enables the switch to distribute batches of AAA transactions to the server with the least number of outstanding transactions.

Figure 332 IOS-based RADIUS SLB



Application Control Engine-based RADIUS SLB

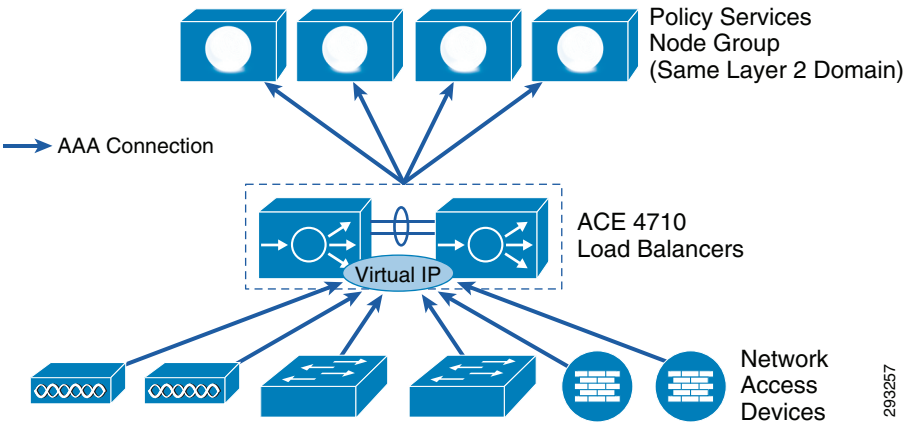
This guide uses the ACE 4710 appliance, but the following concepts apply to any load balancer.

The Cisco ACE 4710 appliance provides maximized application availability to help ensure business continuity and the best service to end users by taking advantage of availability through highly scalable Layer 4 load balancing and Layer 7 content switching and minimizes the effects of application, device, or Web site failure.

When an ACE appliance or module is deployed inline with ISE, it enables RADIUS server load balancing across multiple ISE Policy Service nodes. This allows the servers to share the transaction load, resulting in faster responses to incoming requests by optimally using available servers.

The Network Access Devices direct RADIUS sessions towards a Virtual IP Address (VIP), which is configured on the ACE 4710. The ACE appliance then uses the configured predictor to decide the real server (PSN) to which to direct the session.

Figure 333 PSN Load Balancing Topology

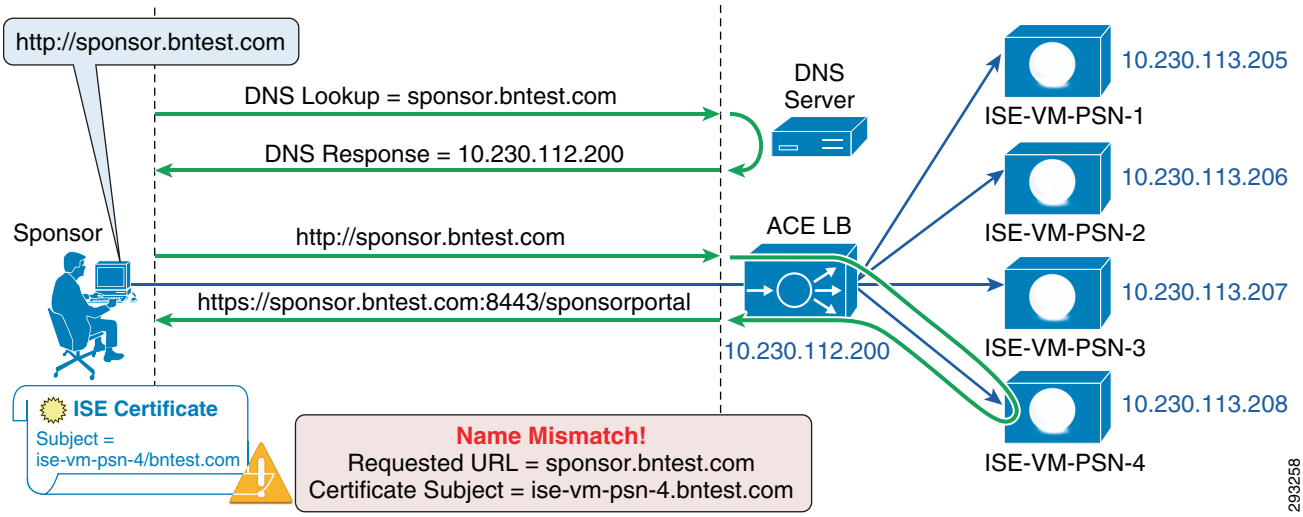


ISE PSN Certificates

ISE only permits a single certificate to be installed for management purposes. This certificate is used for all HTTPS sessions terminating on ISE, including guest and sponsor sessions. The Subject Name of the certificate must contain the Fully Qualified Domain Name (FQDN) of the ISE node; all guest sessions will need to be redirected to the FQDN of the PSN.

In a load balanced, locally distributed ISE deployment, one needs to create a certificate for ISE that maps to multiple DNS names. Otherwise, a certificate error will occur, as illustrated in Figure 334. The user requests a connection to the sponsor.bntest.com portal and gets sent to the ACE Virtual IP Address VIP @10.230.112.200. The ACE then chooses the PSN that will be used. The selected PSN replies with a Subject CN name that differs from the one requested in the URL by the client's browser, resulting in a Name Mismatch certificate error.

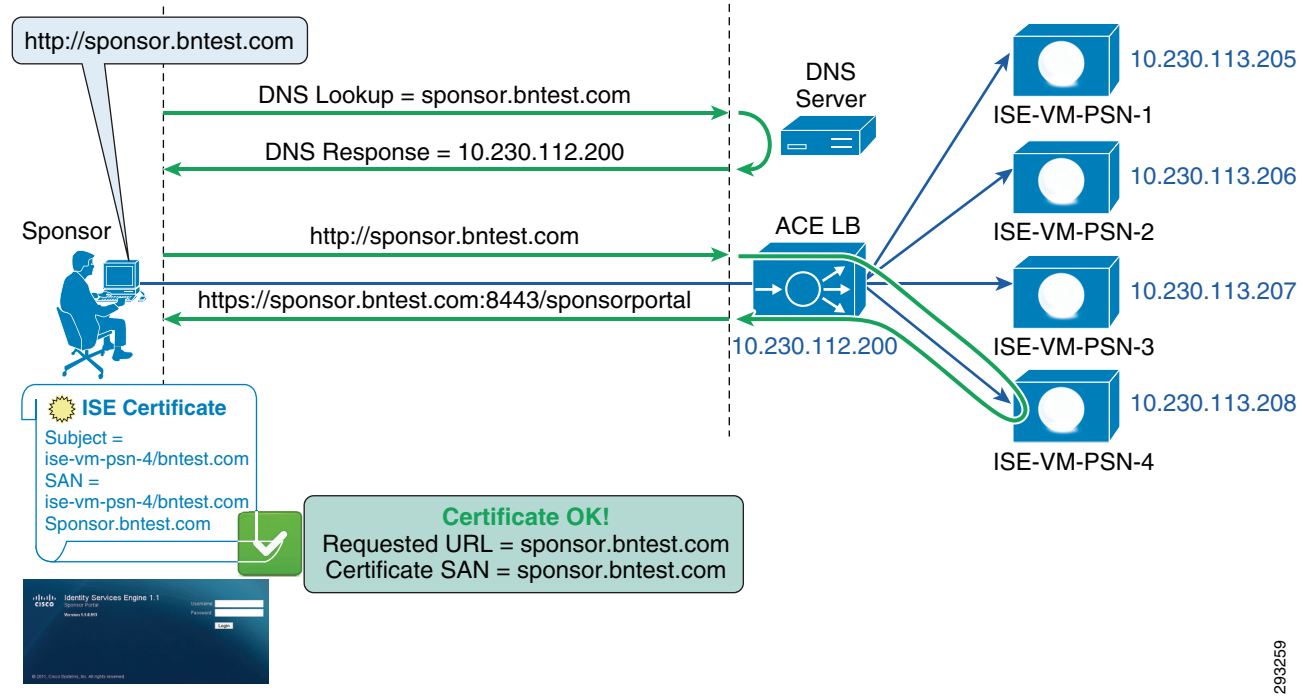
Figure 334 ISE Certificate—No SAN



Creating a certificate with multiple Subject Alternative Name (SAN) fields enables mapping to multiple DNS names. A browser reaching the PSN using any of the listed SAN names will accept the certificate without any error as long as it trusts the CA that signed the certificate.

This is shown in Figure 335, where previously we had a mismatch, now we have a Certificate SAN also including the DNS name sponsor.bntest.com, which ensures the user successfully can open the sponsor portal without error.

Figure 335 ISE Certificate with SAN



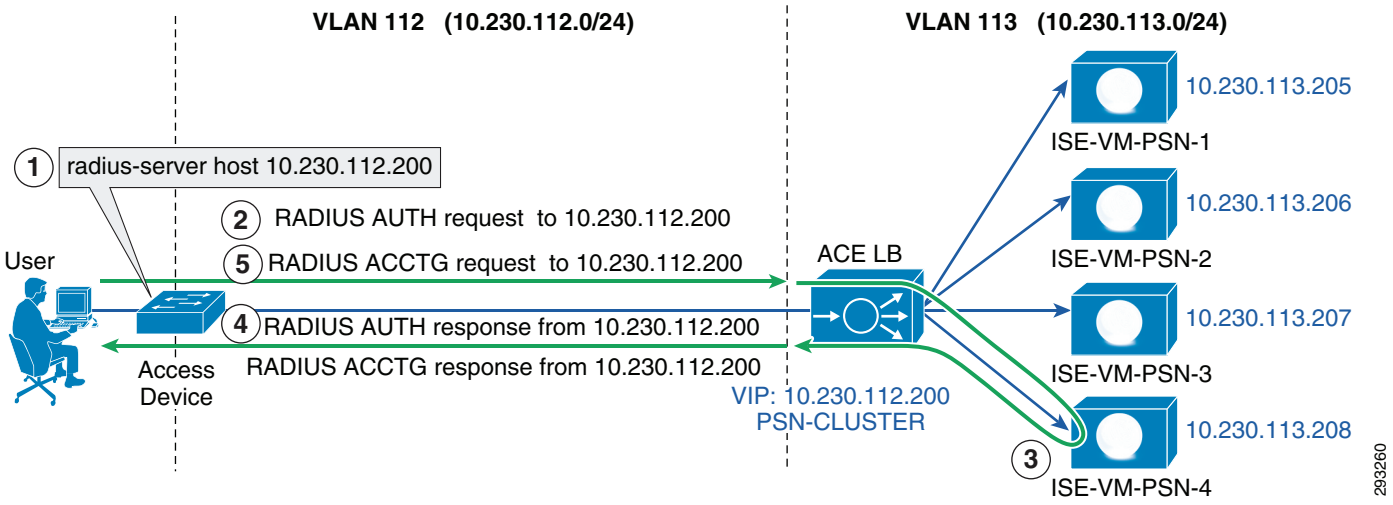
To view the procedure to create the Certificate SAN for each ISE PSN, see Configure Certificates for PSN with SAN.

Load Balancing RADIUS Using ACE

RADIUS packets sent to the ACE virtual IP (VIP) are load-balanced to a real PSN based on the configured algorithm. Cisco ACE supports sticky based on source IP, Framed-IP-Address, and Calling-Station-ID to ensure the same Policy Service node services RADIUS requests from the same endpoint.

A Load Balanced RADIUS flow through the ACE is shown in Figure 336.

Figure 336 PSN Load Balancing RADIUS



1. The Network Access Device (NAD) has a single RADIUS Server defined; this is the ACE Virtual IP (VIP) 10.230.112.200.
2. RADIUS Authentication requests are sent to the VIP Address @ 10.230.112.200.
3. Requests for the same endpoint are load balanced to the same Policy Service Node (PSN) via Sticky based on RADIUS Calling-Station-ID, Framed-IP-address, and source IP.
4. RADIUS Response received from real server, ise-vm-psn-4 (10.230.113.208).
5. RADIUS Accounting is sent to and from the same PSN based on RADIUS Attribute Stickiness.

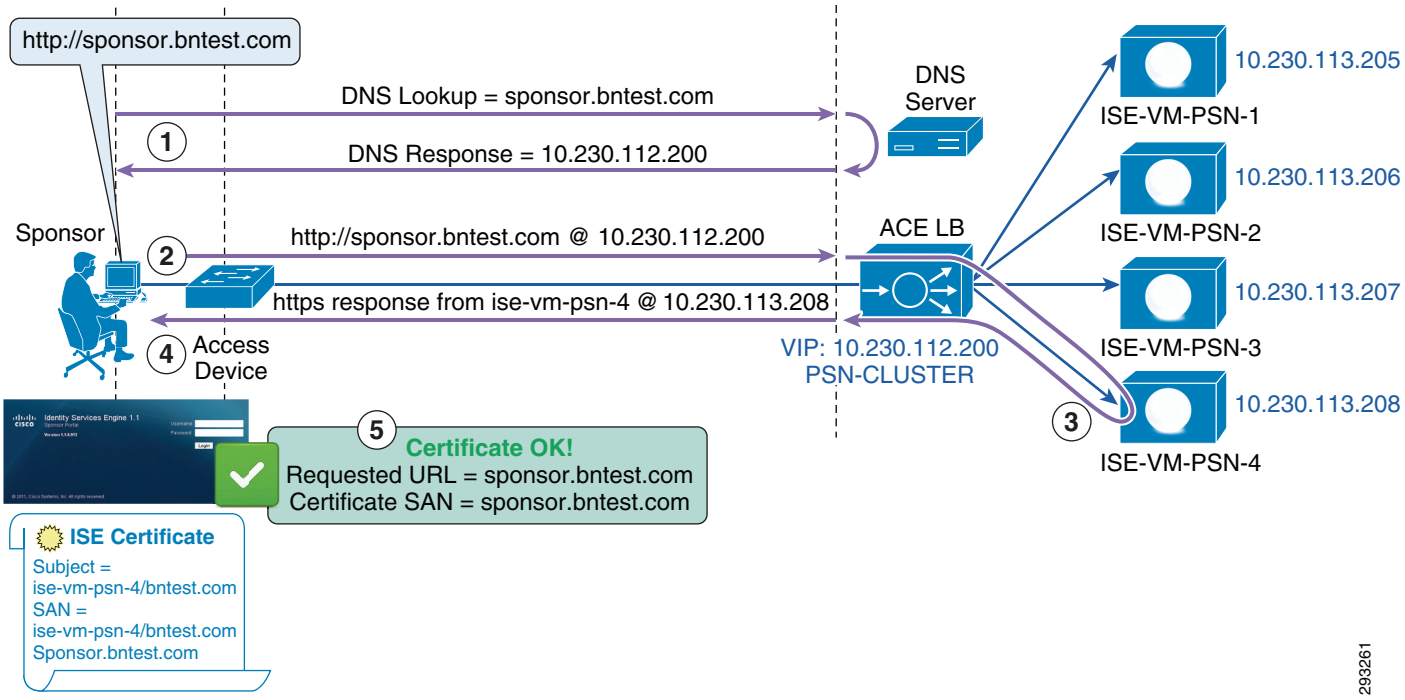
ISE PSN Load Balancing Non-redirected Web Services

Direct HTTP/S Services such as Local Web Authentication (LWA), Sponsor Portal, and MyDevices portal can be classified as non-redirected Web services.

A single Web portal Fully Qualified Domain Name (FQDN) should resolve to the ACE VIP for http and https load balancing.

A sample flow of a user connecting to the Sponsor Portal is shown in Figure 337.

Figure 337 Load Balancing Non-redirected Web Services



1. Browser resolves sponsor.bntest.com to VIP @ 10.230.112.200.
2. Web request sent to https://sponsor.bntest.com @ 10.230.112.200.
3. ACE load balances request to PSN based on IP or HTTP sticky.
4. HTTPS response received from ise-vm-psn-4 @ 10.230.113.208.
5. Certificate SAN includes FQDN for both sponsor and ise-vm-psn-4.

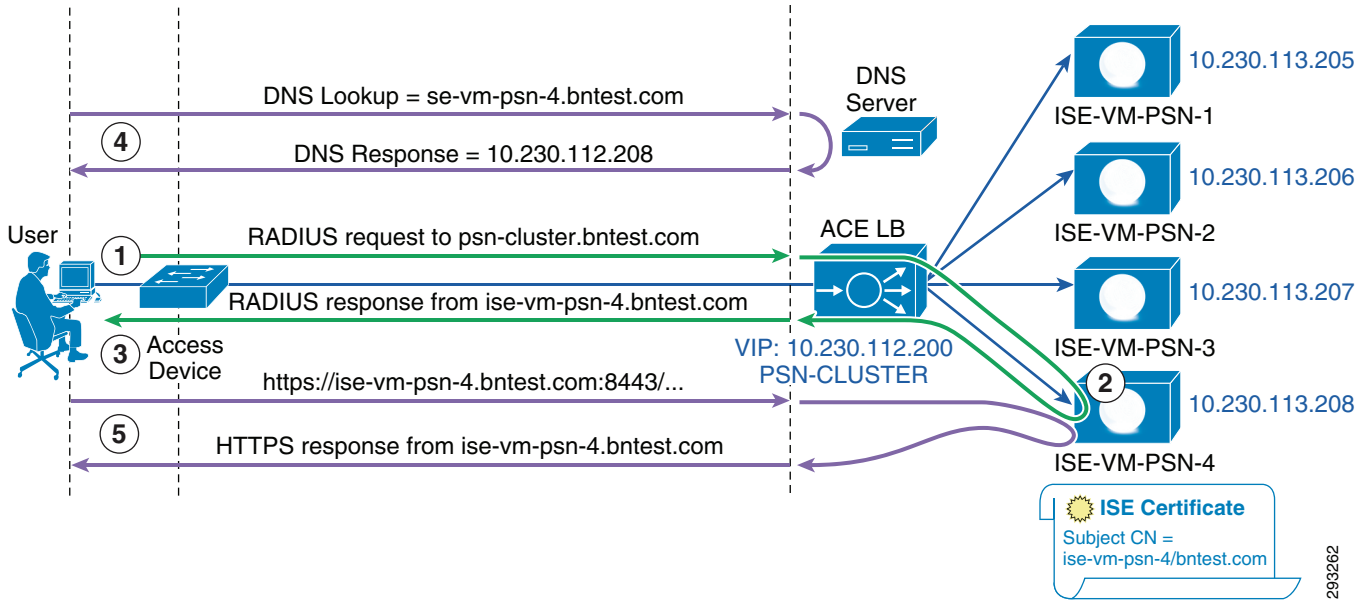
ISE PSN Load Balancing with URL-Redirection

Posture, Central Web Authentication (CWA), Native Supplicant Provisioning (NSP), and Device Registration Web Authentication (DRW) can all be classified as URL-Redirected Services.

A sample flow of URL-redirection is shown in Figure 338.

The PSN that terminates RADIUS and returns URL Redirect with its own certificate CN name substituted for ***ip*** variable in the URL.

Figure 338 PSN Load Balancing with URL-Redirection



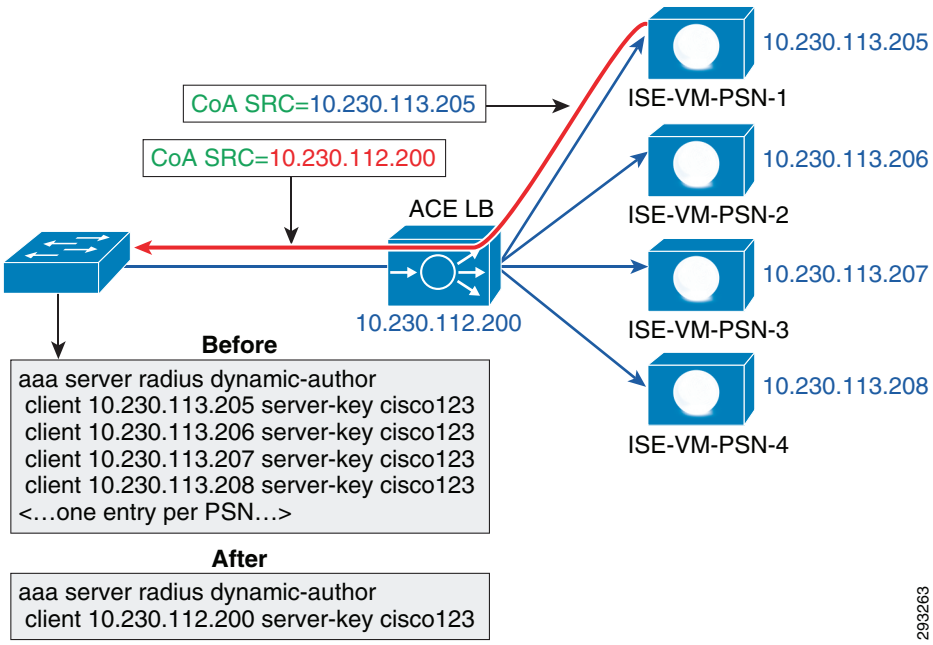
1. RADIUS Authentication requests are sent to the ACE Virtual IP (VIP) @10.230.112.200.
2. Requests for the same endpoint are load balanced to the same PSN via RADIUS sticky.
3. RADIUS Authorization received from ise-vm-psn-4 @ 10.230.113.208 with a URL Redirect to https://ise-vm-psn-4.bntest.com:8443/.
4. Client browser is redirected and resolves the FQDN in the URL to real server address.
5. User sends the Web request directly to the same PSN that serviced RADIUS request.

NAT PSN CoA Requests

We can simplify the configuration for wired and wireless by configuring NAT to translate only Change of Authorization (CoA) requests to a RADIUS server VIP address. Without NAT-CoA configured, every Network Access Device will have to point to each PSN; with NAT-CoA, the Network Access Device will only require the ACE VIP to be listed. This simplifies configuration where users need to add or remove ISE PSN, as no configuration would be required on the Network Access Device. An example of this is shown in Figure 339, showing the configuration before and after NAT-CoA is configured.

NAT CoA will match the traffic from Policy Service nodes to UDP/1700 (RADIUS CoA) and translate to the VIP. This is shown in Figure 339. This allows us to configure only the VIP as the RADIUS server, rather than each PSN.

Figure 339 NAT CoA



PSN and ACE Load Balance Configuration

Deployment Map

To implement load balancing with the ACE appliance and ISE, the following steps take place:

Step 1 Create DNS Entries for PSN.

Step 2 Configure Certificates for PSN with SAN.

Step 3 Configure ACE inline connectivity.

Step 4 Configure ACE contexts for Admin and load-balancing.

Step 5 Configure ISE.

Step 6 Configure Wireless LAN Controllers.

Step 7 Configure Wired Access Switch.

ACE Deployment Guidelines

There are some guidelines that the user must be aware of before deploying the ACE load balancers, including:

- The ACE must be deployed in Inline Routed mode.
- ISE uses the Layer 3 address to identify the Network Access Device (NAD), not the NAS-IP-Address in the RADIUS packet. Therefore we cannot use Source NAT for traffic sent to the ACE VIP.

- Each Policy Service node must be reachable by the PAN and MNT directly.
- Each Policy Service node must be reachable directly from the client network for redirections.
- RADIUS Attribute Stickiness is to be based on Calling-Station-ID and Framed-IP-address.
- VIP for the Policy Service nodes is listed as the RADIUS server on each Network Access Device for all RADIUS AAA.
- Each Policy Service node gets listed individually in the Network Access CoA list by its real IP Address.
- When using NAT-CoA, only list the ACE VIP in the CoA list.
- Load Balancers get listed as Network Access Devices in ISE so the test Authentications (probes) may be answered.

Create DNS Entries for PSN

The DNS server needs to have entries for the Fully Qualified Domain Names (FQDNs) that are to be used by the Load Balancing VIP. In this case we need to add the entries shown in Table 21.

Table 21 ISE FQDN

FQDN	IP Address
psn-cluster.bntest.com	10.230.112.200
sponsor.bntest.com	10.230.112.200
guest.bntest.com	10.230.112.200
ise-vm-psn-1.bntest.com	10.230.113.205
ise-vm-psn-2.bntest.com	10.230.113.206
ise-vm-psn-3.bntest.com	10.230.113.207
ise-vm-psn-4.bntest.com	10.230.113.208

Configure Certificates for PSN with SAN

As detailed in ISE PSN Certificates, we need to configure the Subject Alternative Name on the ISE Policy Service nodes' certificates.

Install OpenSSL 0.9.8h

Download and install OpenSSL 0.9.8h from the Internet. This package is required to insert the Subject Alternative Names (SAN) in the ISE PSN certificates.

Customizing ISE PSN Certificate Subject Attributes

The following procedure uses ise-vm-psn-1.bntest.com as an example of populating the PSN Certificate Signing Request (CSR) with custom Subject Alternative Names (SANs):

Step 1 Access the local certificate store of the ISE Policy Service node (PSN). In this example, the PSN FQDN is http://ise-vm-psn-1.bntest.com.

Step 2 Login to the ISE appliance running the Policy Service persona. For example: http://ise-vm-psn-1.bntest.com:8443.

Step 3 ISE deployment is distributed with the PSN deployed on a dedicated appliance, then navigate to **Administration > System > Server Certificate**.

Step 4 Select **Add > Generate a new self-signed certificate**.

1. **Certificate Subject**: CN=bn-ise-vm-psn1.bntest.com
2. **key length**: 2048
3. **Digest to sign with**: SHA-256
4. **Expiration TTL**: 2 years
5. **Friendly Name**: psn1 self-signed cert
6. **Override Policy**: Select Replace Certificate

Step 5 Export the Certificate A**dministration>System>Server Certificate**.

1. Select Certificate and export.
2. Select option to **Export Certificate and Private Key** using password *********.
3. Save the certificate and private key on your local computer, e.g., bnisevmpsn1.zip.

Step 6 Uncompress the .zip file and rename the files to:

1. psn1.pem
2. psn1.pvk
3. Copy .pem and .pvk file to c:\Program Files <x86>\GnuWin23\bin.

Step 7 Create a customized configuration file for the OpenSSL CSR requests named **openssl.conf**. The touch points per PSN will be **commonName** and **DNS.#** entries.

```
##################################################################
# This is where we define how to generate CSRs
[ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name # where to get DN for reqs
req_extensions = v3_req # The extensions to add to req's
string_mask = nombstr
##################################################################
# Per "req" section, this is where we define DN info
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = US
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = California
localityName = Locality Name (eg, city)
localityName_default = San Jose
0.organizationName = Organization Name (eg, compaany)
0.organizationName_default = Cisco Sytems
organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = SAMPG
commonName = ise-vm-psn-1.bntest.com
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 64
##################################################################
# Extension for requests
[ v3_req ]
# Lets at least make our requests PKIX compliant
```

```
basicConstraints = CA:true
extendedKeyUsage = serverAuth, clientAuth
keyUsage = keyEncipherment, digitalSignature
subjectAltName = @alt_names
[alt_names]
DNS.1 = ise-vm-psn-1.bntest.com
DNS.2 = psn-cluster.bntest.com
DNS.3 = guest.bntest.com
DNS.4 = mydevices.bntest.com
DNS.5 = sponsorportal.bntest.com
####################################################################
```

Step 8 Use OpenSSL to create a custom CSR request using the following commands:

```
    openssl.exe req -key PVK_filename -new -out CSR_filename
C:\Program Files (x86)\GnuWin32\bin>openssl.exe req -new -key psn1.pvk -new -out
psn1csr.pem -config openssl.conf

Enter pass phrase for psn1.pvk:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

----
Country Name (2 letter code) [US]:
State or Province Name (full name) [California]:
Locality Name (eg, city) [San Jose]:
Organization Name (eg, compaany) [Cisco Sytems]:
Organizational Unit Name (eg, section) [SAMPG]:
ise-vm-psn-1.bntest.com \[\]:ise-vm-psn-1.bntest.com
Email Address \[\]:
```

Step 9 To validate CSR contents, use the following command:

```
    openssl req -text -noout -in CSR_filename
C:\Program Files (x86)\GnuWin32\bin>openssl.exe req -text -noout -in psn1csr.pem
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=US, ST=California, L=San Jose, O=Cisco Sytems, OU=SAMPG,
CN=ise-vm-psn-1.bntest.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:dc:e5:fb:a5:3b:7a:91:9a:36:52:85:37:64:a3:
5c:6a:3f:f7:3a:6f:c9:66:19:29:af:9b:c1:29:ac:
db:b2:9d:da:aa:20:60:a9:17:5d:65:a2:ea:b7:64:
46:bf:64:54:1e:1c:fc:67:be:e4:15:62:37:2a:37:
49:4b:41:bc:85:5c:84:86:4e:46:5e:f5:36:a6:be:
53:1b:06:80:c3:65:27:10:5e:01:f1:4c:ee:ff:7c:
28:8b:1a:00:9a:3f:6a:0a:42:a2:ac:56:9a:89:51:
68:ea:47:57:38:24:08:25:fc:0e:b7:c1:c7:0e:23:
78:c9:ad:bd:65:b6:21:c8:68:f4:c7:f9:25:08:c8:
ae:1c:89:1c:f8:00:34:e0:a8:81:97:2f:41:70:fc:
3c:2b:59:68:5c:dd:55:99:c7:d8:94:40:a3:3d:8c:
3c:28:97:d5:1b:a0:33:19:4e:cb:d2:44:0a:13:8c:
fe:60:8f:60:59:24:52:ec:e2:a9:69:3a:0e:23:c3:
e3:ff:11:3f:90:52:d0:95:da:7e:fe:89:63:9e:be:
6d:e4:45:e2:b6:cb:2e:c5:42:5f:d6:d4:ab:ac:7c:
```

```
06:cd:32:40:c3:eb:c5:5b:18:8d:40:f8:57:51:87:
37:0e:3e:3c:00:ae:31:8b:4f:69:11:fe:8d:a8:a5:
c0:81
Exponent: 65537 (0x10001)
Attributes:
Requested Extensions:
X509v3 Basic Constraints:
CA:TRUE
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment
X509v3 Subject Alternative Name:
DNS:ise-vm-psn-1.bntest.com, DNS:psn-cluster.bntest.com, DNS:guest.bntest.com,
DNS:mydevices.bntest.com, DNS:sponsorportal.bntest.com,
Signature Algorithm: sha1WithRSAEncryption
49:92:1c:04:8b:f0:c7:6b:fe:67:fe:04:8f:d0:cc:22:86:4c:
5a:8b:13:70:3b:90:31:e1:43:52:ee:d3:2f:69:47:22:41:06:
80:8f:f4:a5:e3:52:f7:17:de:72:36:18:a9:b4:9b:9d:e2:a7:
03:41:0b:3e:10:fa:d5:39:3a:0d:8c:93:3d:5a:69:9b:19:39:
d8:0d:74:a3:2f:2b:f7:55:b1:e7:b0:01:24:00:c8:72:dc:93:
00:58:f0:dd:a9:ac:12:7e:a5:ca:d1:b2:c3:a8:0d:60:49:05:
79:78:79:24:3a:97:99:76:96:0a:6e:8c:5c:ac:de:80:aa:3a:
01:2e:32:dd:60:56:61:da:3f:0d:00:dd:f1:11:27:4a:4a:54:
e9:06:1f:7c:8f:0e:e8:65:16:95:90:50:b2:8c:7d:b0:56:f0:
d4:f4:60:c4:bb:d4:33:b2:ef:5a:44:03:5e:73:0d:cf:c9:b8:
63:6c:bc:d7:f1:74:d8:ae:26:7a:88:01:6a:b2:a0:2e:08:b1:
34:8d:bf:43:12:4a:8b:8d:d2:ff:24:02:da:2b:4f:c8:ed:a0:
c8:f7:4d:a5:7d:a5:48:e9:c4:63:5d:bc:2f:a8:e6:78:06:59:
d4:c2:30:ef:82:98:93:5a:4b:73:93:7a:49:71:42:68:aa:85:
4a:46:5c:16
```

Step 10 Submit CSR (for example, psn1csr.pem) to a CA server for signing. Download the resulting ISE certificate in PEM format.

In this example, the newly signed certificate was saved using the name **psn1cert.cer**.

Step 11 To validate ISE CSR contents, use the command:

- Base64 (PEM) format: openssl x509 -text -noout -in Cert_filename

```
C:\Program Files (x86)\GnuWin32\bin>openssl x509 -text -noout -in psn1cert.cer
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            44:94:7e:2e:00:00:00:00:af:fb
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=bntest, CN=bntest-BN-W2K8-CA-1-CA
        Validity
            Not Before: Dec  5 19:55:49 2012 GMT
            Not After : Dec  5 20:05:49 2014 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Sytems, OU=SAMPG,
       CN=ise-vm-psn-1.bntest.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b7:6e:57:3c:1e:ca:aa:6f:8b:4c:8c:73:a4:1e:
                    27:63:cd:65:cf:6b:a0:65:f9:b5:ea:13:9e:e2:23:
                    81:82:91:07:f8:5d:5d:8a:95:26:86:13:ad:d7:fe:
                    55:7a:e8:98:41:f4:3a:a3:c9:9b:f0:8e:ab:c9:17:
                    a9:66:28:a7:af:d1:42:3d:56:62:b4:fb:5d:45:21:
                    ee:98:90:2e:8f:55:85:4f:4a:3d:15:23:ce:1f:cb:
                    41:e7:e3:84:f0:57:2c:0d:28:6a:10:c8:4d:dd:d4:
```

```
                    06:8b:14:52:ed:a1:cc:a9:f1:43:21:61:59:32:0c:
                    fb:e3:ec:11:c0:bd:11:7c:c9:10:55:9f:28:99:76:
                    fa:8b:76:2d:ec:1f:26:24:84:42:30:be:f6:2f:a9:
                    2a:fa:cb:d9:41:55:ac:b3:81:21:0c:56:56:b9:6f:
                    7c:0d:8a:a2:ea:09:ed:a8:4a:20:2f:98:5c:36:e1:
                    84:4b:34:69:0f:f3:a2:3b:3b:0f:43:d4:54:47:7f:
                    2a:72:5c:33:a6:ff:7a:2b:c0:d1:0b:fc:27:85:b5:
                    92:6a:63:8d:ed:0f:80:53:b5:3e:9b:15:aa:28:c6:
                    0c:8c:99:fb:44:65:2f:a9:f9:35:e2:19:9b:ff:e0:
                    c5:c5:65:70:63:59:67:e9:d7:5d:a0:73:ac:a4:16:
                    f4:bd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:ise-vm-psn-1.bntest.com, DNS:psn-cluster.bntest.com,
              DNS:guest.bntest.com, DNS:mydevices.bntest.com,
              DNS:sponsorportal.bntest.com
            X509v3 Subject Key Identifier:
                DE:5B:A3:CC:FD:06:0C:21:37:6D:2A:BE:F6:E7:A4:C0:F3:F0:9C:0C
            X509v3 Authority Key Identifier:
                keyid:22:D6:0A:D0:ED:1A:C3:D2:87:85:0E:5D:C5:E5:FD:62:1A:5D:DE:3C

            X509v3 CRL Distribution Points:

URI:ldap:///CN=bntest-BN-W2K8-CA-1-CA,CN=BN-W2K8-CA-1,CN=CDP,CN=Public%20Key%20Services,CN
=Services,CN=Configuration,DC=bntest,DC=com?
certificateRevocationList?base?objectClass=cRLDistributionPoint
                URI:http://bn-w2k8-ca-1.bntest.com/CertEnroll/bntest-BN-W2K8-CA-1-CA.crl

            Authority Information Access:
                CA Issuers -
URI:ldap:///CN=bntest-BN-W2K8-CA-1-CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Con
figuration,DC=bntest,DC=com?cAC
ertificate?base?objectClass=certificationAuthority

            1.3.6.1.4.1.311.21.7:
                0..&+.....7.....\..........%...Lr.......h..d...
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
    Signature Algorithm: sha1WithRSAEncryption
        32:e9:1e:a9:63:df:90:42:32:cf:b5:78:e1:d3:be:50:89:ab:
        dc:c4:4f:cd:fd:2d:99:2a:e5:79:de:71:e3:91:34:e4:1c:42:
        91:28:52:e9:7d:b0:c3:01:1f:ac:3e:4e:0b:9d:52:b4:b4:29:
        d1:74:ff:29:7c:0a:fa:31:be:7f:21:52:72:88:66:38:49:5c:
        98:44:81:3e:07:47:e5:dc:34:ae:25:b3:9b:57:a6:09:f2:62:
        4b:a1:27:11:c8:29:a7:f8:c4:e3:58:b1:7e:6b:56:5f:44:94:
        d6:f5:c7:84:32:fc:da:da:0c:24:cc:0e:7f:71:75:1e:6f:7c:
        7f:6e:d0:8b:6f:26:46:78:5b:1a:14:83:11:80:a1:d6:3b:a2:
        75:c3:1c:62:72:84:c2:da:64:92:e1:31:63:35:e8:fe:94:1e:
        a1:39:b2:fa:11:72:8c:35:3b:01:a4:77:84:be:f4:44:3f:b6:
        31:b6:3f:18:1e:2c:65:d5:1c:90:8e:83:d7:2a:b8:8b:c6:b3:
        09:f1:8b:2c:a7:58:c6:b9:3f:99:8e:ef:f0:d1:62:3b:f0:3f:
        ff:86:1e:80:1c:da:06:54:5a:99:72:4f:1e:fb:45:0b:0a:56:
        7e:86:ed:5d:7c:23:3f:c4:83:86:fa:6d:dc:b2:e9:2d:2c:b2:
        42:90:a2:3b
```

Step 12 If the signing CA is not already trusted by the ISE Policy Service node, import the CA certificate and certificate chain as applicable.

Step 13 From the Administration node, navigate to **Administration > System > Certificates > Certificate Authority Certificates** and select **Import**. Complete the form for importing a CA certificate:

1. Under Certificate File, browse to the location of the CA certificate file. For example: C:\Program Files\GnuWIn32\bin\cacert.cer.
2. Under Friendly Name, enter a descriptive name. For example: cts-ad-ca CA Certificate.
3. Optionally enable Trust for client authentication.
4. Click **Submit** when you have completed entering information on the form.
5. The CA certificate should now appear in the list.

Step 14 Import the CA signed certificate as a local server certificate into ISE. If ISE deployment is distributed with the PSN deployed on a dedicated appliance, then navigate to **Administration > System > Server Certificate**.

Step 15 From the Local Certificate section, click **Add** and then select **Import Local Server Certificate**.

1. Under Certificate File, browse to the location of the CA-signed certificate file, e.g., **C:\Program Files\GnuWIn32\bin\psn1cert.cer**.
2. Under Private Key File, browse to the location of the original self-signed certificate Private Key file, e.g., **C:\Program Files\GnuWIn32\bin\psn1.pvk**.
3. Under Password, enter the Private Key password.
4. Under Friendly Name, enter a descriptive name, e.g., **ise-vm-psn-1 CA-Signed Certificate**.
5. Under Protocol, enable EAP and Management Interface (HTTPS), as appropriate. This example shows how to leverage SAN fields for Web-based services, so HTTPS is selected.
6. Click **Submit** when you have completed entering information on the form.
7. Click **OK**. Upon submit, wait for the application server to return (including Web access to admin interface) before logging back into ISE.

Step 16 Repeat the process for each node that requires custom attributes. Be sure to update the OpenSSL.conf file according to requirements for each node.

Configure ACE Inline Connectivity

The Cisco ACE 4710 appliances need to be deployed in a routed inline mode. The following example shows the inline deployment.

We are connecting the ACE 4710 appliances running 5(1.2) code to the Cisco Nexus 7000 and Cisco Nexus 5000, as shown in Figure 340.

While the Nexus platforms provide a virtual port-channel (vPC) feature for a device to create a single logical link to two Cisco Nexus Switches, it is recommended not to leverage the vPC feature for Cisco ACE 4710 (http://www.cisco.com/en/US/prod/collateral/contnetw/ps5719/ps7027/ps8361/white_paper_c11-688039.html).

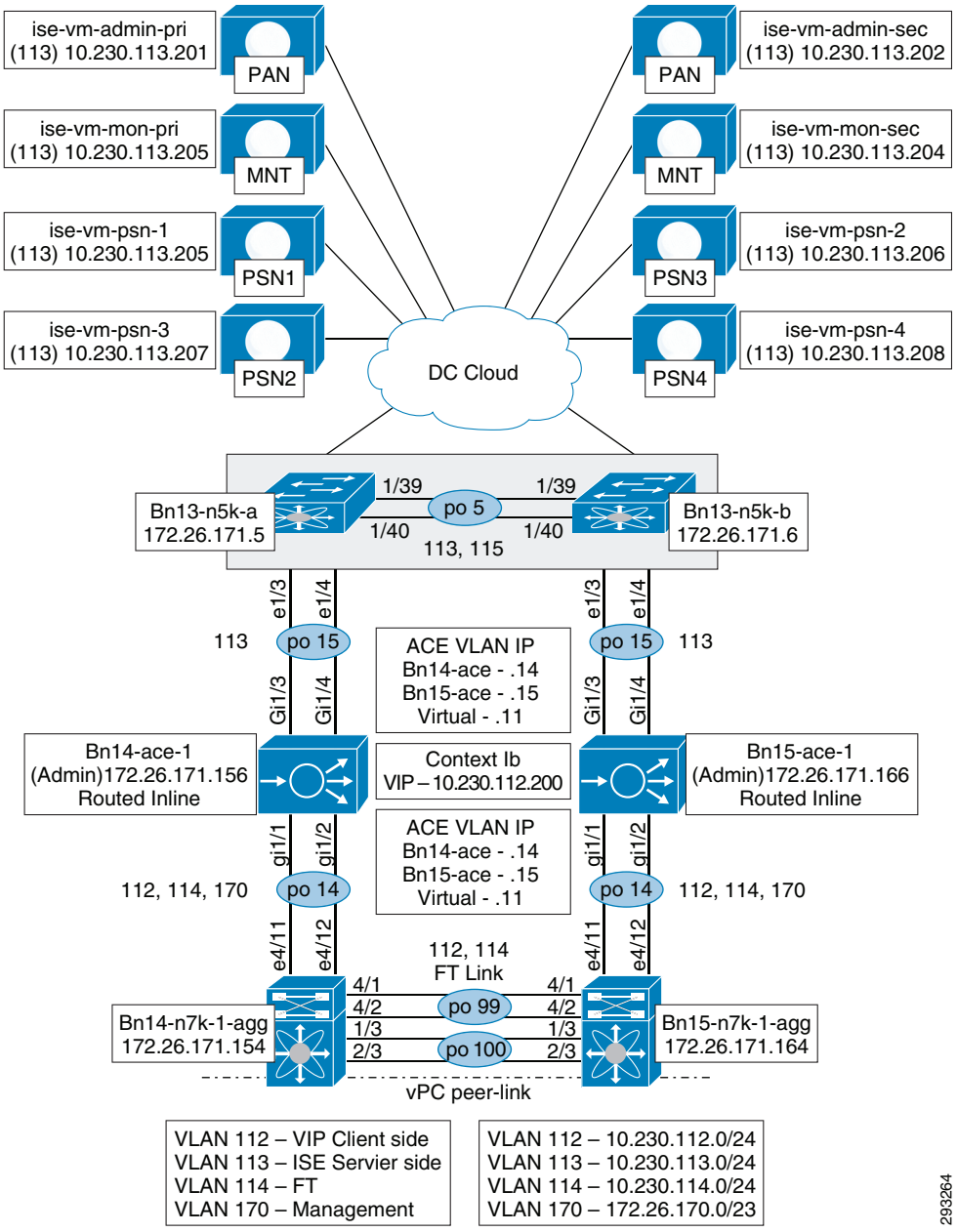
To add the ACE 4710 appliances inline, these steps take place:

Step 1 On each Cisco Nexus 5000, add the ISE-server VLAN and port-channel for the two links to the ACE.

Step 2 On each Cisco Nexus 7000, add the ISE-client VLAN and port-channel for the uplinks.

Step 3 On each Cisco Nexus 7000, create a static route to the ISE-server VLAN via the ISE-client and redistribute into EIGRP.

Figure 340 Physical Topology—ACE inline



ACE Configuration

This section describes on the configuration steps required on the ACE appliances.

ACE GUI and CLI

The ACE appliances can be configured via a GUI or using the command line; the entire ACE configuration in this guide is performed using the CLI.

ACE Contexts

This section addresses the ACE contexts. The ACE will be configured to use two contexts:

- The **Admin** context will be used for remote management and Fault Tolerant (FT) configuration.
- The **lb** context will used for load balancing.

ACE Admin Context

By default, the ACE initially provides you with an Admin context with the ability to define up to five user contexts. (With additional licenses, you can define up to 20 contexts.) As the system administrator, you have full system administrator access to configure and manage the Admin context and all user contexts. Each context can also have its own administrator and log-in mechanism that provides access only to the specific context. When you log in to the ACE using the console or Telnet, you are authenticated in the Admin context.

Initial configuration will be done via a serial connection.

Configure Hostname and Users

Step 1 Configure the hostnames:

```
switch/Admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch/Admin(config)# hostname bn14-ace-1
bn14-ace-1/Admin(config)#
```

Step 2 Configure the users:

```
username admin password 0 Nufc-5-1 role Admin domain default-domain
username www password 0 Nufc-5-1 role Admin domain default-domain
```

Configure Interfaces and VLANs

The Cisco ACE 4710 appliance does not support Port Aggregation Protocol (PAgP) or Link Aggregate Control Protocol (LACP). As a result, the port channel is configured using “mode on”.

Step 1 Configure the port-channels and interfaces:

```
interface port-channel 14
  description port-channel to bn14-n7k-1-agg
  switchport trunk native vlan 170
  switchport trunk allowed vlan 112,170
  port-channel load-balance src-dst-port
  no shutdown
!
interface port-channel 15
  description port-channel to bn13-n5k-a_e1/3-4
  switchport access vlan 113
  no shutdown
```

```
!
interface gigabitEthernet 1/1
  description link to bn14-n7k-1-agg_e4/11
  speed 1000M
  duplex FULL
  carrier-delay 30
  channel-group 14
  no shutdown
interface gigabitEthernet 1/2
  description link to bn14-n7k-1-agg_e4/12
  speed 1000M
  duplex FULL
  carrier-delay 30
  channel-group 14
  no shutdown
interface gigabitEthernet 1/3
  description Link to bn13-n5k-a_gi1/3
  speed 1000M
  duplex FULL
  channel-group 15
  no shutdown
interface gigabitEthernet 1/4
  description Link to bn13-n5k-a_gi1/4
  speed 1000M
  duplex FULL
  channel-group 15
  no shutdown
!
```

Step 2 Configure the VLAN used for remote access, in this case VLAN 170:

```
interface vlan 170
description Management VLAN
ip address 172.26.171.156 255.255.254.0
no shutdown
```

Step 3 Configure the default route for the ACE Admin context:

```
ip route 0.0.0.0 0.0.0.0 172.26.170.1
```

Configure Remote Management Access to the ACE

Before remote network access can occur on the ACE through an Ethernet port, you must create a traffic policy that identifies the network management traffic that can be received by the ACE. Configure remote management access to the ACE by following these steps:

```
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any
!
policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit
!
interface vlan 170
  service-policy input remote_mgmt_allow_policy
```

In this example, we have an ACL permitting ip and icmp. Admin users will need to change this as required for their operational needs:

```
access-list PERMIT-ALL line 8 extended permit ip any any
access-list PERMIT-ALL line 16 extended permit icmp any any
!
interface vlan 170
  access-group input PERMIT-ALL
  access-group output PERMIT-ALL
```

Configure Fault Tolerant Connection—bn14-ace

Configure the Fault Tolerant peering information on the bn14-ace appliance:

```
peer hostname bn15-ace-1
hostname bn14-ace-1
shared-vlan-hostid 2
peer shared-vlan-hostid 1
!
interface port-channel 14
  ft-port vlan 114
!
ft interface vlan 114
  ip address 10.230.114.14 255.255.255.0
  peer ip address 10.230.114.15 255.255.255.0
  no shutdown
!
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 114
!
ft group 1
  peer 1
  priority 110
  peer priority 105
  associate-context Admin
  inservice
```

Configure Fault Tolerant Connection—bn15-ace

Configure the Fault Tolerant peering information on the bn15-ace appliance:

```
peer hostname bn14-ace-1
hostname bn15-ace-1
shared-vlan-hostid 2
peer shared-vlan-hostid 1
!
interface port-channel 14
  ft-port vlan 114
!
ft interface vlan 114
  ip address 10.230.114.15 255.255.255.0
  peer ip address 10.230.114.14 255.255.255.0
  no shutdown
!
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 114
!
```

```
ft group 1
  peer 1
  priority 105
  peer priority 110
  associate-context Admin
  inservice


bn14-ace-1/Admin# sh ft peer summary

Peer Id                       : 1
State                         : FSM_PEER_STATE_COMPATIBLE
Maintenance mode              : MAINT_MODE_OFF
FT Vlan                       : 114
FT Vlan IF State              : UP
My IP Addr                    : 10.230.114.14
Peer IP Addr                  : 10.230.114.15
Query Vlan                    : Not Configured
Query Vlan IF State           : DOWN
Peer Query IP Addr            : 0.0.0.0
Heartbeat Interval            : 300
Heartbeat Count               : 10
SRG Compatibility             : COMPATIBLE
License Compatibility         : COMPATIBLE
FT Groups                     : 1
```

Create ACE Virtual Context (VC)

Step 1 On the active ACE, configure a new Virtual Context:

```
context lb
  allocate-interface vlan 112-113
```

Step 2 Add an additional FT group for the new context:

```
ft group 2
  peer 1
  priority 110
  peer priority 105
  associate-context lb
  inservice
```

Configure Virtual Context

On the active ACE, change to the new context using the **changeto** command:

```
bn14-ace/Admin# changeto lb
bn14-ace/lb#
```

Configure Client and Server Side VLANs

On the active ACE, which in this case is bn14-ace, create the Server and Client side VLANs using the information in Table 22.


```
interface vlan 112
  description Client Side VIP VLAN
  ip address 10.230.112.14 255.255.255.0
  alias 10.230.112.11 255.255.255.0
  peer ip address 10.230.112.15 255.255.255.0
  no shutdown
!
interface vlan 113
  description ISE side VLAN 113
  ip address 10.230.113.14 255.255.255.0
  alias 10.230.113.11 255.255.255.0
  peer ip address 10.230.113.15 255.255.255.0
  no shutdown
!
ip route 0.0.0.0 0.0.0.0 10.230.112.1
```

Configure Real Servers and Server Farms

Step 1 On the active ACE, configure the real servers, which will be each of the Policy Service nodes:

```
rserver host ise-vm-psn-1
  ip address 10.230.113.205
  inservice
!
rserver host ise-vm-psn-2
  ip address 10.230.113.206
  inservice
!
rserver host ise-vm-psn-3
  ip address 10.230.113.207
  inservice
!
rserver host ise-vm-psn-4
  ip address 10.230.113.208
  inservice
```

Step 2 Add the rservers under a serverfarm. Here we create two serverfarms, ise-psn for radius load balancing and ise-psn-web for https traffic. We are using the “leastconns” predictor for load balancing.

```
serverfarm host ise-psn
  predictor leastconns
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
!
serverfarm host ise-psn-web
   predictor leastconns
  rserver ise-vm-psn-1
```

```
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
      inservice
```

Configure ACE Probes

When configuring the ACE RADIUS probe, it is recommended to use a probe interval shorter than the RADIUS dead timer configured on the switch. If a long interval is used, the switch may declare the ACE's VIP to be dead and the dot1x authentication would fail.

A downside to the lower interval rate is the increase in ISE probe authentications, detailed in ISE Probe Output.

Step 1 Create the RADIUS probe:

```
probe radius psn-probe
  interval 4
  faildetect 1
  credentials bn-4710 Cisco12345 secret Cisco12345
```

Step 2 Create the ICMP probe:

```
probe icmp ping
```

Step 3 On the active ACE, create the server farm for RADIUS and apply the probe ping and probe psn-probe:

```
serverfarm host ise-psn
  probe ping
  probe psn-probe
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
```

Configure RADIUS Load Balancing

Step 1 Create RADIUS sticky based on framed-ip and calling-station-id to ensure Authentication and Accounting for the same client stay with the same Policy Service node:

```
sticky radius framed-ip calling-station-id RADIUS-STICKY
  serverfarm ise-psn
```

Step 2 Create a class-map and VIP address for RADIUS:

```
class-map match-all RAD-L4-CLASS
  2 match virtual-address 10.230.112.200 udp range 1812 1813
```

Step 3 Create a virtual server traffic policy and map load-balancing policies to specific server farms:

```
policy-map type loadbalance radius first-match RAD-L7-POLICY
```

```
  class class-default
    sticky-serverfarm RADIUS-STICKY
```

Step 4 Define the service policy that will be applied to the ACE client side VLAN:

```
policy-map multi-match RAD-L4-POLICY
  class RAD-L4-CLASS
    loadbalance vip inservice
    loadbalance policy RAD-L7-POLICY
    loadbalance vip icmp-reply
```

Configure HTTPS Profiling Load Balancing

Step 1 Create the tcp https probe:

```
probe tcp https-probe
  port 8443
  interval 30
  passdetect interval 90
  connection term forced


serverfarm host ise-psn-web
  probe https-probe
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
```

Step 2 Create a Sticky-IP group:

```
sticky ip-netmask 255.255.255.0 address source SRC-IP-STICKY
  timeout 5
  serverfarm ise-psn-web
```

Step 3 Create a class-map and VIP address for HTTPS:

```
   class-map match-any HTTPS-CLASS
     2 match virtual-address 10.230.112.200 tcp eq www
     3 match virtual-address 10.230.112.200 tcp eq https
     4 match virtual-address 10.230.112.200 tcp eq 8443
     5 match virtual-address 10.230.112.200 tcp eq 8444
```

Step 4 Create a virtual server traffic policy and map load-balancing policies to specific server farms:

```
policy-map type loadbalance generic first-match WEB-L4-POLICY
  class class-default
    sticky-serverfarm SRC-IP-STICKY
```

Step 5 Define the service policy that will be applied to the ACE client side VLAN:

```
policy-map multi-match RAD-L4-POLICY
  class RAD-L4-CLASS
    loadbalance vip inservice
    loadbalance policy RAD-L7-POLICY
    loadbalance vip icmp-reply
  class HTTPS-CLASS
```

```
    loadbalance vip inservice
    loadbalance policy WEB-L4-POLICY
    loadbalance vip icmp-reply
```

Configure DHCP Profiling Load Balancing

Step 1 Create a class-map and VIP address for HTTPS:

```
class-map match-all DHCP-CLASS
  2 match virtual-address 10.230.112.200 udp eq 67
```

Step 2 Create a virtual server traffic policy and map load-balancing policies to specific server farms:

```
policy-map type loadbalance generic first-match DHCP-L4-POLICY
  class class-default
    sticky-serverfarm SRC-IP-STICKY
```

Step 3 Define the service policy that will be applied to the ACE client side VLAN:

```
policy-map multi-match RAD-L4-POLICY
  class RAD-L4-CLASS
    loadbalance vip inservice
    loadbalance policy RAD-L7-POLICY
    loadbalance vip icmp-reply
  class HTTPS-CLASS
    loadbalance vip inservice
    loadbalance policy WEB-L4-POLICY
    loadbalance vip icmp-reply
  class DHCP-CLASS
    loadbalance vip inservice
    loadbalance policy DHCP-L4-POLICY
    loadbalance vip icmp-reply
  class class-default
```

Optional ACL for Client and Server-facing Interface

An optional ACL can be defined to permit traffic to and from each interface.

Step 1 Define the ACL:

```
access-list PERMIT-ALL line 1 extended permit ip any any
access-list PERMIT-ALL line 2 extended permit icmp any any
```

Step 2 Apply the ACL to the client and server-facing interfaces:

```
interface vlan 112
  description Client Side VIP VLAN
  access-group input PERMIT-ALL
!
interface vlan 113
  description ISE side VLAN 113
  no icmp-guard
  access-group input PERMIT-ALL
```

Configure NAT for PSN CoA Requests

Step 1 Configure the ACL to match on:

```
access-list NAT-COA line 5 extended permit udp 10.230.113.205 0.0.0.0 any eq 1700
access-list NAT-COA line 6 extended permit udp 10.230.113.206 0.0.0.0 any eq 1700
access-list NAT-COA line 7 extended permit udp 10.230.113.207 0.0.0.0 any eq 1700
access-list NAT-COA line 8 extended permit udp 10.230.113.208 0.0.0.0 any eq 1700
```

Step 2 Configure the ACL to match on:

```
class-map match-any NAT-CLASS
  2 match access-list NAT-COA
```

Step 3 Configure the policy-map:

```
policy-map multi-match NAT-POLICY
  class NAT-CLASS
    nat dynamic 1 vlan 112
```

Step 4 Configure the nat-pool:

```
interface vlan 112
  description Client Side VIP VLAN
  nat-pool 1 10.230.112.200 10.230.112.200 netmask 255.255.255.255 pat
```

Step 5 Apply the service-policy to the server side VLAN:

```
interface vlan 113
  description ISE side VLAN 113
  mac-sticky enable
  no icmp-guard
  access-group input ALL
  service-policy input NAT-POLICY
```

ISE Configuration

PSN Should be Configured in a Node Group

Typically there is more than one Policy Service node in a distributed deployment; in this case we have four.

All Policy Service personas that reside behind a load balancer share a common multicast address and can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes in that group process the requests of the node that has failed, thereby providing high availability.

The Policy Service nodes in the Node Group must be Layer 2 adjacent; members of the Node Group exchange heartbeats using multicast.

To create a node group, use the following procedure on the ISE admin node:

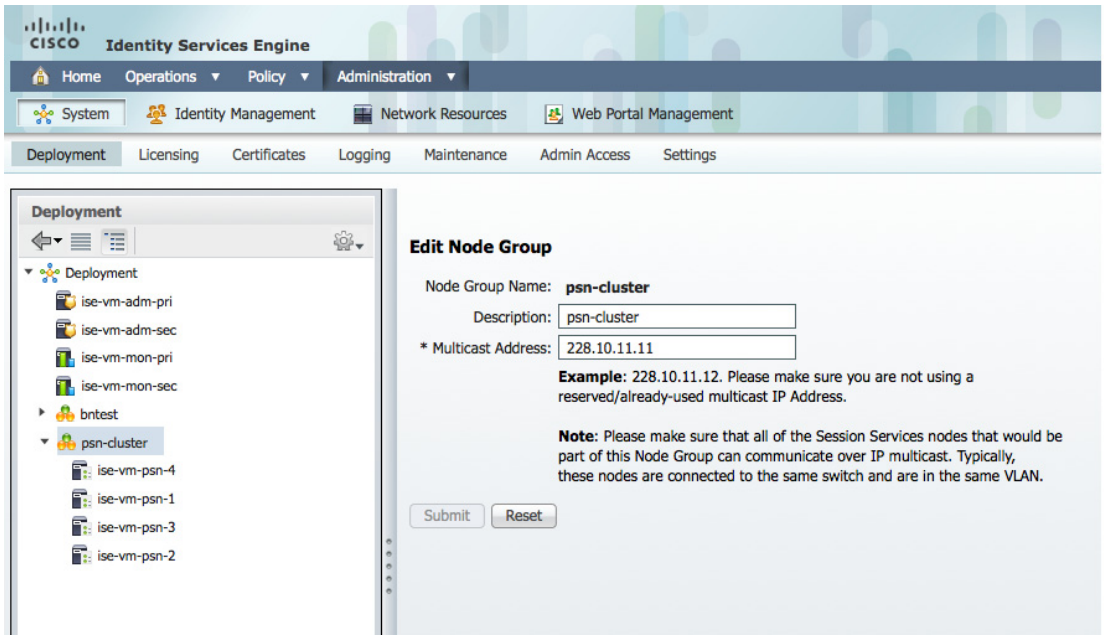
Step 1 Navigate to **Administration > System > Deployment** and **Create node group**.

Step 2 Assign **Node Group Name**, **Description**, and **Multicast Address**.

Step 3 Add Policy Service nodes to the node group.

Once the procedure is complete you can view the nodes and Node Group details, as shown in Figure 341.

Figure 341 Node Group



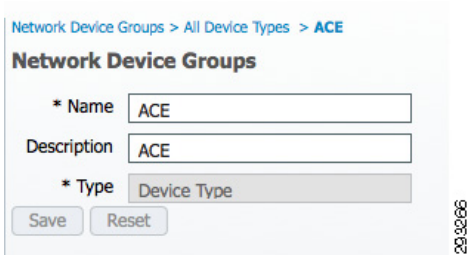
NAD Should be Added for Each ACE

The ACE appliances must each be added as a Network Appliance Device. To add the ACE appliances:

Step 1 Navigate to **Administration > Network Device Groups > All Device Types > Add**.

Step 2 Create **Network Device Group**, **Name**:Ace, **Description**: Ace, **Type**: Device Type (see Figure 342).

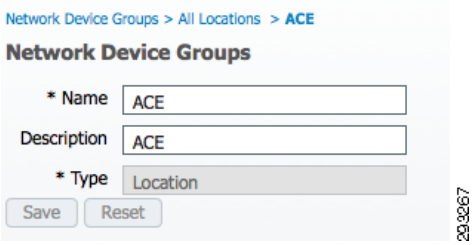
Figure 342 Device Type ACE



Step 3 Navigate to **Administration > Network Device Groups > All Locations > Add**.

Step 4 Create **Network Device Group**, **Name**:Ace, **Description**: Ace, **Type**: Location (see Figure 343).

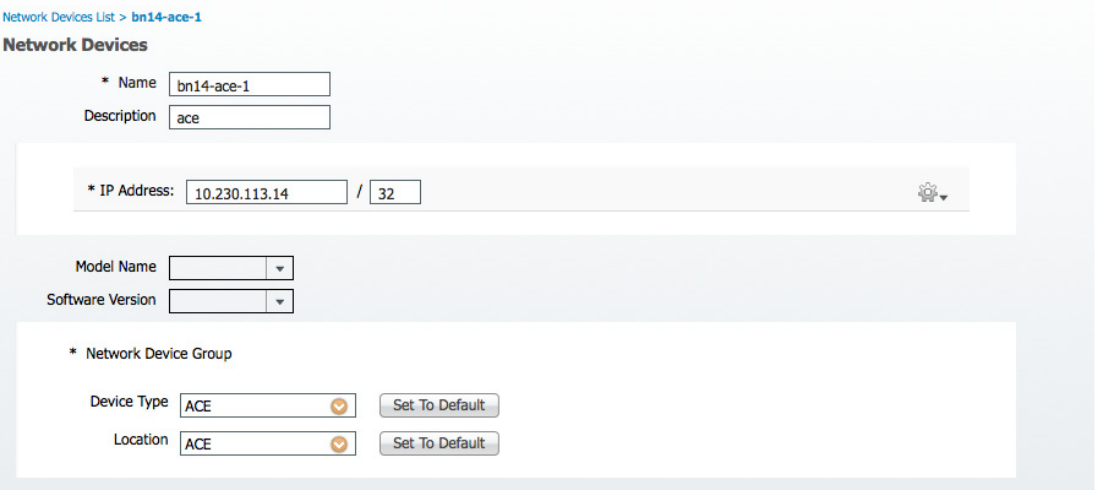
Figure 343 Location ACE



Step 5 Navigate to **Administration > Network Devices > Add**.

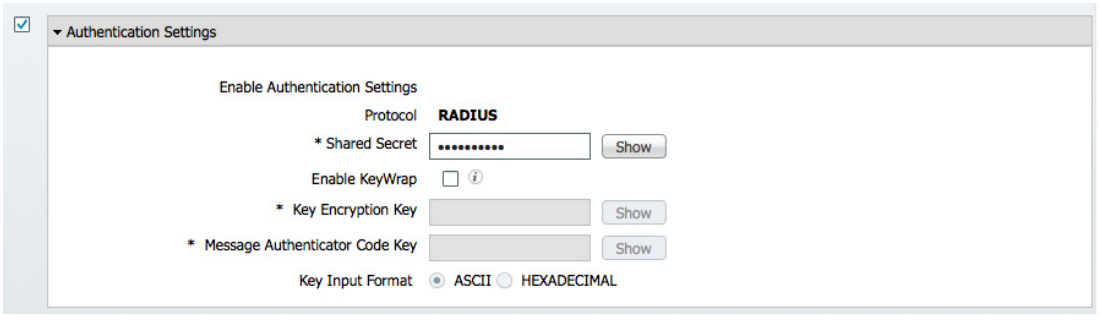
Step 6 For each ACE, add **Name**:Ace, **Description**: Ace, **IP Address**: x.x.x.x, **Device Type**: ACE, **Location**: ACE. See Figure 344 for an example from bn14-ace-1.

Figure 344 Add NAD



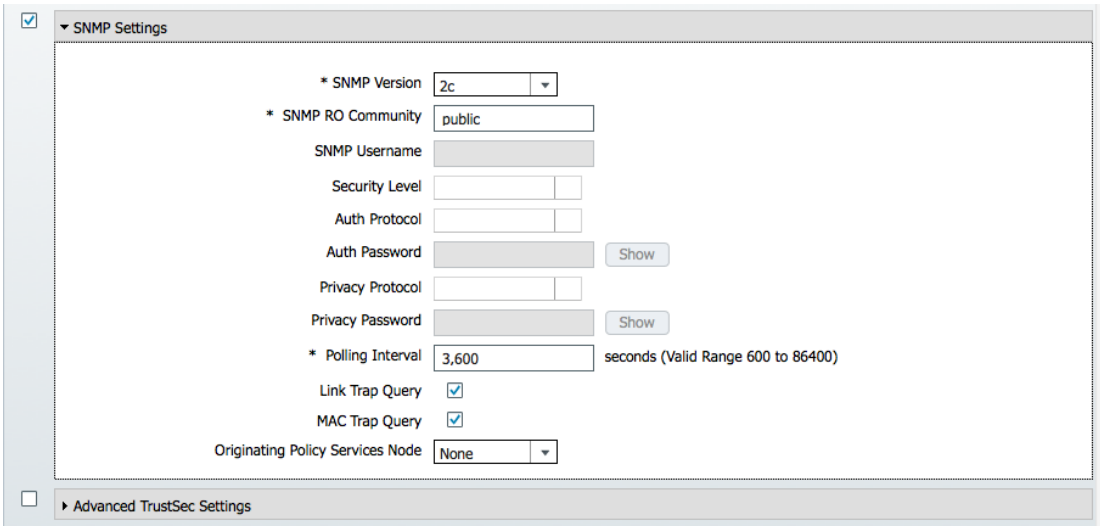
Step 7 For each ACE, select the checkbox for **Authentication Settings** and enter the **Shared Secret**. See Figure 345 for an example from bn14-ace-1.

Figure 345 Add NAD—Authentication Settings



Step 8 For each ACE, select the checkbox for **SNMP Settings**. Enter the **SNMP Version**, in this case v2C, then enter the **SNMP RO Community**. See Figure 346 for an example from bn14-ace-1.

Figure 346 Add NAD—SNMP Settings



Required Authentication and Authorization Policies

The ACE appliance is configured to use a RADIUS probe against the PSN to verify the AAA Services (see Configure ACE Probes).

The probe user account and password must exist in the specified ID store for the ACE probe requests. For example, if Active Directory is being used, then the user account must be created.

For the probe to be successful and the VIP to be up, the ISE must be configured to allow the successful authentication and authorization of the ACE RADIUS Probe.

The Authentication Policy used in this example is a basic policy, matching on the Device Type: ACE:

```
If DEVICE: Device Type EQUALS Device Type# All Device Types#ACE allow protocols Allowed
Protocol: Default Network
```

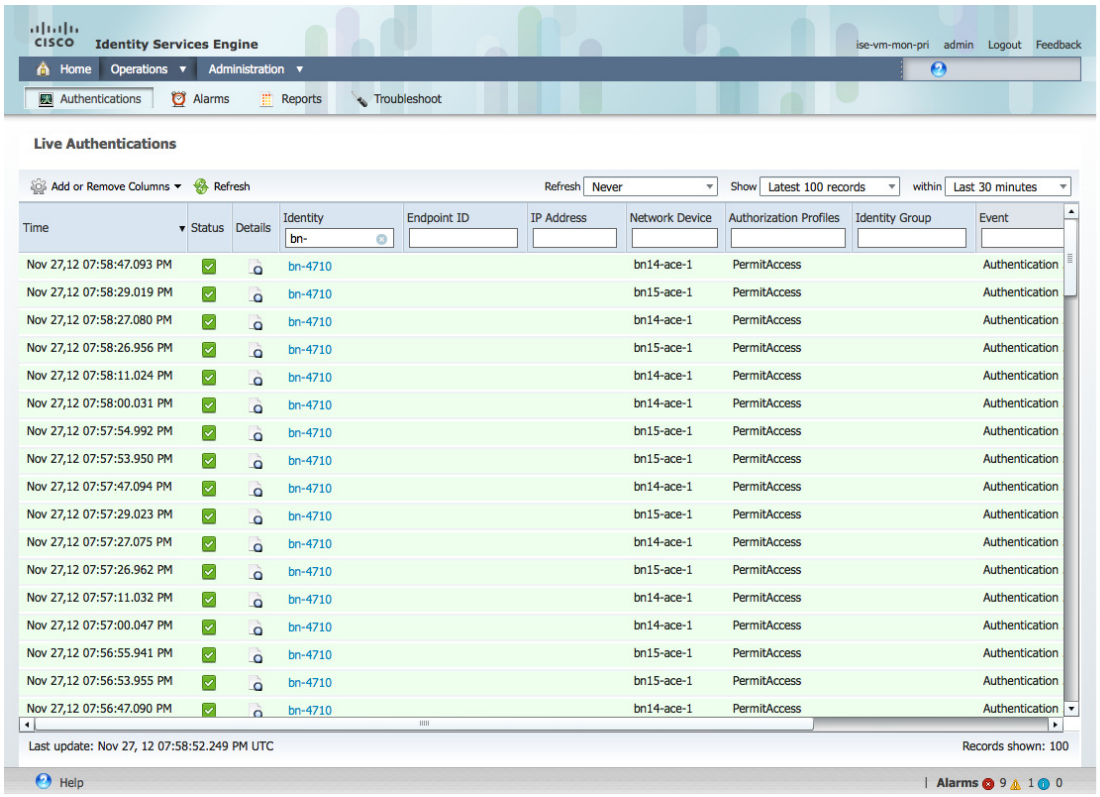
The Authorization Policy used in this example is a basic policy, matching on the Location: ACE:

```
If DEVICE: Location EQUALS All Locations#ACE then ACCESS_ACCEPT
```

ISE Probe Output

The ISE Live Authentications log will show if the probes are successful. Both ACE appliances will send probes to each of the real servers listed in the server farm to which the probe are applied. So if the probe interval is set to 60 seconds, then every 60 seconds we will see 8 probe messages on the ISE Live Log. In ISE 1.1.2 there is no facility to filter out these messages.

Figure 347 ACE RADIUS Probes on ISE Log



WLC Configuration

Each WLC needs to have the ACE VIP added to the RADIUS server list:

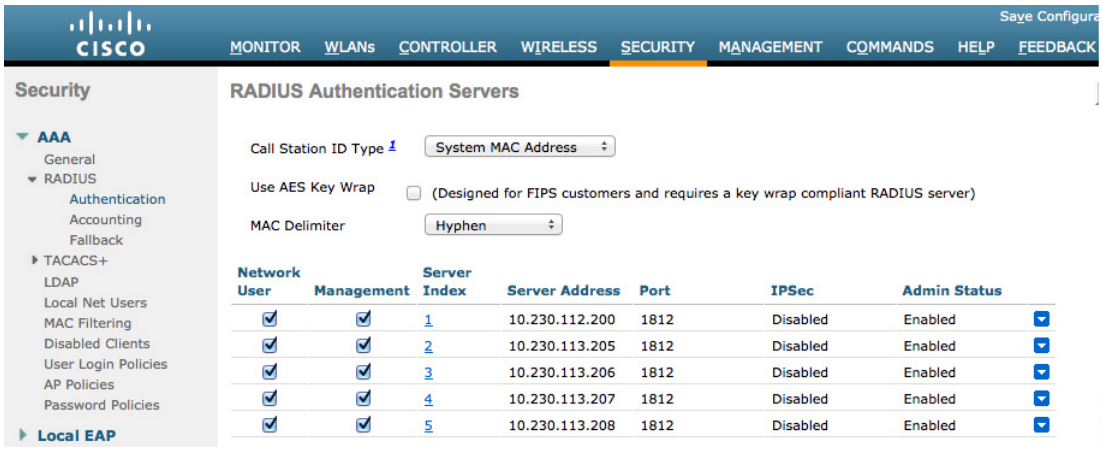
Step 1 Open WLC in a browser.

Step 2 Navigate to **SECURITY > AAA > RADIUS > Authentication**.

Step 3 Select **New**. Add the ACE VIP details and select **Apply**.

Step 4 If NAT CoA is configured add only the ACE VIP, otherwise add each additional ISE PSN to the server list (the output is shown in Figure 348).

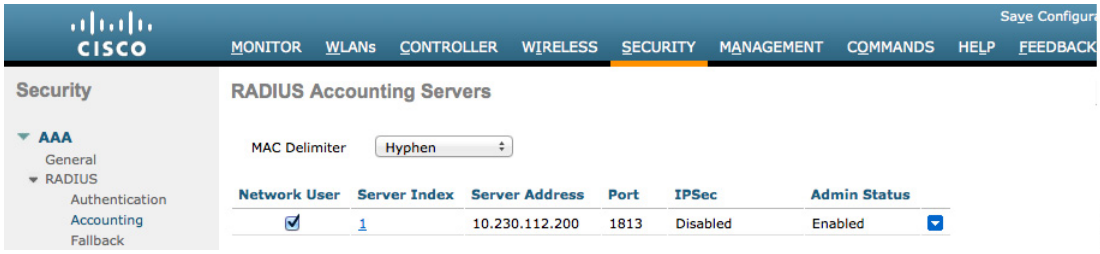
Figure 348 RADIUS Authentication Servers



Step 5 Navigate to **SECURITY > AAA > RADIUS > Accounting**.

Step 6 Select **New**. Add the ACE VIP details and select **Apply** (the output is shown in Figure 349).

Figure 349 RADIUS Accounting Servers



For guidance on configuring the Wireless LAN Controller (WLC), see: http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_11_universal_wlc_config.pdf.

Wired Switch Configuration

The wired configuration was touched on in Port Configuration of Wired Switches. Some configuration changes are required to include the ACE appliances.

Radius-Server Host

When there are no ACE appliances deployed, each PSN is to be listed under the **radius-server host** command. However with the introduction of ACE into the topology, only the ACE VIP is listed:

```
radius-server host 10.230.112.200 auth-port 1812 acct-port 1813 key **********
```

Enable RADIUS Change of Authorization (CoA)

This step is used to define the servers that are allowed to perform change of authorization (RFC 3576) operations:

```
C3750X(config)#aaa server radius dynamic-author
```

```
C3750X(config-locsvr-da-radius)#client 10.230.112.200 server-key shared_secret
```

When user is not using NAT for PSN CoA requests, the PSN IP addresses must be populated under the "aaa server radius dynamic-author":

```
aaa server radius dynamic-author
 client 10.230.113.205 server-key Cisco12345
 client 10.230.113.206 server-key Cisco12345
 client 10.230.113.207 server-key Cisco12345
 client 10.230.113.208 server-key Cisco12345
```

When user is using NAT for PSN CoA requests, the ACE VIP addresses must be populated under the "aaa server radius dynamic-author":

```
aaa server radius dynamic-author
 client 10.230.112.200 server-key Cisco12345
```

ACE Configuration File

BN14-ACE-1 Admin Context

```
bn14-ace-1/Admin# sh run
Generating configuration....

logging enable
logging standby
logging console 0
logging timestamp
logging trap 5
logging history 0
logging buffered 7
logging persistent 0
logging monitor 7
logging device-id context-name

boot system image:c4710ace-t1k9-mz.A5_1_2.bin

login timeout 60

peer hostname bn15-ace-1
hostname bn14-ace-1
shared-vlan-hostid 1
peer shared-vlan-hostid 2
interface gigabitEthernet 1/1
  description link to bn14-n7k-1-agg_e4/11
  speed 1000M
  duplex FULL
  carrier-delay 30
  channel-group 14
  no shutdown
interface gigabitEthernet 1/2
  description link to bn14-n7k-1-agg_e4/12
  speed 1000M
  duplex FULL
  carrier-delay 30
  channel-group 14
  no shutdown
interface gigabitEthernet 1/3
  description Link to bn13-n5k-a_gi1/3
  speed 1000M
```

```
  duplex FULL
  channel-group 15
  no shutdown
interface gigabitEthernet 1/4
  description Link to bn13-n5k-a_gi1/4
  speed 1000M
  duplex FULL
  channel-group 15
  no shutdown
interface port-channel 14
  description port-channel to bn14-n7k-1-agg
  ft-port vlan 114
  switchport trunk native vlan 170
  switchport trunk allowed vlan 112,170
  port-channel load-balance src-dst-port
  no shutdown
interface port-channel 15
  description port-channel to bn13-n5k-a_e1/3-4
  switchport access vlan 113
  no shutdown

switch-mode
ntp server 172.26.171.43


access-list PERMIT-ALL line 8 extended permit ip any any
access-list PERMIT-ALL line 16 extended permit icmp any any



rserver host ise-vm-psn-1
  ip address 10.230.113.205
  inservice
rserver host ise-vm-psn-2
  ip address 10.230.113.206
  inservice
rserver host ise-vm-psn-3
  ip address 10.230.113.207
  inservice
rserver host ise-vm-psn-4
  ip address 10.230.113.208
  inservice

serverfarm host ise-psn
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
serverfarm host ise-psn-web
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice

class-map type management match-any remote_access
  2 match protocol xml-https any
```

```
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

interface vlan 170
  description Management VLAN
  no ipv6 normalization
  no ipv6 icmp-guard
  ip address 172.26.171.156 255.255.254.0
  peer ip address 172.26.171.166 255.255.254.0
  access-group input PERMIT-ALL
  access-group output PERMIT-ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown

ft interface vlan 114
  ip address 10.230.114.14 255.255.255.0
  peer ip address 10.230.114.15 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 114
ft group 1
  peer 1
  priority 110
  peer priority 105
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 172.26.170.1

context lb
  allocate-interface vlan 112-113

snmp-server contact "byod@cisco.com"
snmp-server location "bn14"
snmp-server community public group Network-Monitor
snmp-server community private group Network-Monitor

snmp-server trap-source vlan 170


ft group 2
  peer 1
  priority 110
  peer priority 105
  associate-context lb
  inservice
username admin password 5 $1$lukQFv31$AoGgoHvNDCB6CP9xE8oLe1  role Admin domain
default-domain
username www password 5 $1$.ycpS9Wy$EcdRmUTObAAojyY1vqlKH/  role Admin domain de
fault-domain

ssh key rsa 1024 force
```

BN14-ACE-1 VC Context

```
bn14-ace-1/lb# sh run
Generating configuration....

logging enable
logging timestamp
logging buffered 7
logging monitor 7


login timeout 60



access-list NAT-COA line 5 extended permit udp 10.230.113.205 0.0.0.0 any eq 170
0
access-list NAT-COA line 6 extended permit udp 10.230.113.206 0.0.0.0 any eq 170
0
access-list NAT-COA line 7 extended permit udp 10.230.113.207 0.0.0.0 any eq 170
0
access-list NAT-COA line 8 extended permit udp 10.230.113.208 0.0.0.0 any eq 170
0
access-list PERMIT-ALL line 1 extended permit ip any any
access-list PERMIT-ALL line 2 extended permit icmp any any

probe tcp https-probe
  port 8443
  interval 2
  passdetect interval 90
  connection term forced
probe icmp ping
probe radius psn-probe
  interval 4
  faildetect 1
  credentials bn-4710 Cisco12345 secret Cisco12345

rserver host ise-vm-psn-1
  ip address 10.230.113.205
  inservice
rserver host ise-vm-psn-2
  ip address 10.230.113.206
  inservice
rserver host ise-vm-psn-3
  ip address 10.230.113.207
  inservice
rserver host ise-vm-psn-4
  ip address 10.230.113.208
  inservice

serverfarm host ise-psn
  predictor leastconns
  probe ping
  probe psn-probe
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
```

```
serverfarm host ise-psn-web
  predictor leastconns
  probe https-probe
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice

sticky ip-netmask 255.255.255.0 address source source-ip
sticky radius framed-ip calling-station-id RADIUS-STICKY
  serverfarm ise-psn
sticky ip-netmask 255.255.255.0 address source SRC-IP-STICKY
  timeout 5
  serverfarm ise-psn-web


class-map match-all DHCP-CLASS
  2 match virtual-address 10.230.112.200 udp eq 67
class-map match-any HTTPS-CLASS
  2 match virtual-address 10.230.112.200 tcp eq www
  3 match virtual-address 10.230.112.200 tcp eq https
  4 match virtual-address 10.230.112.200 tcp eq 8443
  5 match virtual-address 10.230.112.200 tcp eq 8444
class-map match-any NAT-CLASS
  2 match access-list NAT-COA
class-map match-all RAD-L4-CLASS
  2 match virtual-address 10.230.112.200 udp range 1812 1813

policy-map type loadbalance radius first-match RAD-L7-POLICY
  class class-default
    sticky-serverfarm RADIUS-STICKY

policy-map type loadbalance generic first-match DHCP-L4-POLICY
  class class-default
    sticky-serverfarm SRC-IP-STICKY
policy-map type loadbalance generic first-match WEB-L4-POLICY
  class class-default
    sticky-serverfarm SRC-IP-STICKY

policy-map multi-match NAT-POLICY
  class NAT-CLASS
    nat dynamic 1 vlan 112
policy-map multi-match RAD-L4-POLICY
  class RAD-L4-CLASS
    loadbalance vip inservice
    loadbalance policy RAD-L7-POLICY
    loadbalance vip icmp-reply
  class HTTPS-CLASS
    loadbalance vip inservice
    loadbalance policy WEB-L4-POLICY
    loadbalance vip icmp-reply
  class DHCP-CLASS
    loadbalance vip inservice
    loadbalance policy DHCP-L4-POLICY
    loadbalance vip icmp-reply
  class class-default

interface vlan 112
  description Client Side VIP VLAN
  ip address 10.230.112.14 255.255.255.0
```

```
  alias 10.230.112.11 255.255.255.0
  peer ip address 10.230.112.15 255.255.255.0

  access-group input PERMIT-ALL
  nat-pool 1 10.230.112.200 10.230.112.200 netmask 255.255.255.255 pat
  service-policy input RAD-L4-POLICY
  no shutdown
interface vlan 113
  description ISE side VLAN 113
  ip address 10.230.113.14 255.255.255.0
  alias 10.230.113.11 255.255.255.0
  peer ip address 10.230.113.15 255.255.255.0
  mac-sticky enable
         no icmp-guard
  access-group input PERMIT-ALL
  service-policy input NAT-POLICY
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.230.112.1
```

BN15-ACE-1 Admin Context

```
bn15-ace-1/Admin# sh run
Generating configuration....



logging enable
logging standby
logging console 0
logging timestamp
logging trap 5
logging history 0
logging buffered 7
logging persistent 0
logging monitor 7
logging device-id context-name

boot system image:c4710ace-t1k9-mz.A5_1_2.bin

login timeout 60

peer hostname bn14-ace-1
hostname bn15-ace-1
shared-vlan-hostid 2
peer shared-vlan-hostid 1
interface gigabitEthernet 1/1
  description link to bn14-n7k-1-agg_e4/11
  speed 1000M
  duplex FULL
  carrier-delay 30
  channel-group 14
  no shutdown
interface gigabitEthernet 1/2
  description link to bn14-n7k-1-agg_e4/12
  speed 1000M
  duplex FULL
  carrier-delay 30
  channel-group 14
  no shutdown
interface gigabitEthernet 1/3
  description Link to bn13-n5k-a_gi1/3
```

```
  speed 1000M
  duplex FULL
  channel-group 15
  no shutdown
interface gigabitEthernet 1/4
  description Link to bn13-n5k-a_gi1/4
  speed 1000M
  duplex FULL
  channel-group 15
  no shutdown
interface port-channel 14
  description port-channel to bn14-n7k-1-agg
  ft-port vlan 114
  switchport trunk native vlan 170
  switchport trunk allowed vlan 112,170
  port-channel load-balance src-dst-port
  no shutdown
interface port-channel 15
  description port-channel to bn13-n5k-a_e1/3-4
  switchport access vlan 113
  no shutdown

switch-mode
ntp server 172.26.171.43


access-list PERMIT-ALL line 8 extended permit ip any any
access-list PERMIT-ALL line 16 extended permit icmp any any



rserver host ise-vm-psn-1
  ip address 10.230.113.205
  inservice
rserver host ise-vm-psn-2
  ip address 10.230.113.206
  inservice
rserver host ise-vm-psn-3
  ip address 10.230.113.207
  inservice
rserver host ise-vm-psn-4
  ip address 10.230.113.208
  inservice

serverfarm host ise-psn
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
serverfarm host ise-psn-web
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
```

```
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

interface vlan 170
  description Management VLAN
  no ipv6 normalization
  no ipv6 icmp-guard
  ip address 172.26.171.166 255.255.254.0
  peer ip address 172.26.171.156 255.255.254.0
  access-group input PERMIT-ALL
  access-group output PERMIT-ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown

ft interface vlan 114
  ip address 10.230.114.15 255.255.255.0
  peer ip address 10.230.114.14 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 114
ft group 1
  peer 1
  priority 105
  peer priority 110
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 172.26.170.1

context lb
  allocate-interface vlan 112-113

snmp-server contact "byod@cisco.com"
snmp-server location "bn14"
snmp-server community public group Network-Monitor
snmp-server community private group Network-Monitor

snmp-server trap-source vlan 170


ft group 2
  peer 1
  priority 105
  peer priority 110
  associate-context lb
  inservice
username admin password 5 $1$lukQFv31$AoGgoHvNDCB6CP9xE8oLe1  role Admin domain
default-domain
username www password 5 $1$.ycpS9Wy$EcdRmUTObAAojyY1vqlKH/  role Admin domain
default-domain
```

```
ssh key rsa 1024 force
```

BN15-ACE-1 VC Context

```
bn15-ace-1/lb# sh run
Generating configuration....

logging enable
logging timestamp
logging buffered 7
logging monitor 7


login timeout 60



access-list NAT-COA line 5 extended permit udp 10.230.113.205 0.0.0.0 any eq 1700
access-list NAT-COA line 6 extended permit udp 10.230.113.206 0.0.0.0 any eq 1700
access-list NAT-COA line 7 extended permit udp 10.230.113.207 0.0.0.0 any eq 1700
access-list NAT-COA line 8 extended permit udp 10.230.113.208 0.0.0.0 any eq 1700
access-list PERMIT-ALL line 1 extended permit ip any any
access-list PERMIT-ALL line 2 extended permit icmp any any


probe tcp https-probe
  port 8443
  interval 2
  passdetect interval 90
  connection term forced
probe icmp ping
probe radius psn-probe
  interval 4
  faildetect 1
  credentials bn-4710 Cisco12345 secret Cisco12345

rserver host ise-vm-psn-1
  ip address 10.230.113.205
  inservice
rserver host ise-vm-psn-2
  ip address 10.230.113.206
  inservice
rserver host ise-vm-psn-3
  ip address 10.230.113.207
  inservice
rserver host ise-vm-psn-4
  ip address 10.230.113.208
  inservice

serverfarm host ise-psn
  predictor leastconns
  probe ping
  probe psn-probe
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice
serverfarm host ise-psn-web
```

```
  predictor leastconns
  probe https-probe
  rserver ise-vm-psn-1
    inservice
  rserver ise-vm-psn-2
    inservice
  rserver ise-vm-psn-3
    inservice
  rserver ise-vm-psn-4
    inservice

sticky ip-netmask 255.255.255.0 address source source-ip
sticky radius framed-ip calling-station-id RADIUS-STICKY
  serverfarm ise-psn
sticky ip-netmask 255.255.255.0 address source SRC-IP-STICKY
  timeout 5
  serverfarm ise-psn-web


class-map match-all DHCP-CLASS
  2 match virtual-address 10.230.112.200 udp eq 67
class-map match-any HTTPS-CLASS
  2 match virtual-address 10.230.112.200 tcp eq www
  3 match virtual-address 10.230.112.200 tcp eq https
  4 match virtual-address 10.230.112.200 tcp eq 8443
  5 match virtual-address 10.230.112.200 tcp eq 8444
class-map match-any NAT-CLASS
  2 match access-list NAT-COA
class-map match-all RAD-L4-CLASS
  2 match virtual-address 10.230.112.200 udp range 1812 1813

policy-map type loadbalance radius first-match RAD-L7-POLICY
  class class-default
    sticky-serverfarm RADIUS-STICKY

policy-map type loadbalance generic first-match DHCP-L4-POLICY
  class class-default
    sticky-serverfarm SRC-IP-STICKY
policy-map type loadbalance generic first-match WEB-L4-POLICY
  class class-default
    sticky-serverfarm SRC-IP-STICKY

policy-map multi-match NAT-POLICY
  class NAT-CLASS
    nat dynamic 1 vlan 112
policy-map multi-match RAD-L4-POLICY
  class RAD-L4-CLASS
    loadbalance vip inservice
    loadbalance policy RAD-L7-POLICY
    loadbalance vip icmp-reply
  class HTTPS-CLASS
    loadbalance vip inservice
    loadbalance policy WEB-L4-POLICY
    loadbalance vip icmp-reply
  class DHCP-CLASS
    loadbalance vip inservice
    loadbalance policy DHCP-L4-POLICY
    loadbalance vip icmp-reply
  class class-default

interface vlan 112
  description Client Side VIP VLAN
  ip address 10.230.112.15 255.255.255.0
  alias 10.230.112.11 255.255.255.0
```

```
  peer ip address 10.230.112.14 255.255.255.0
  access-group input PERMIT-ALL
  nat-pool 1 10.230.112.200 10.230.112.200 netmask 255.255.255.255 pat
  service-policy input RAD-L4-POLICY
  no shutdown
interface vlan 113
  description ISE side VLAN 113
  ip address 10.230.113.15 255.255.255.0
  alias 10.230.113.11 255.255.255.0
  peer ip address 10.230.113.14 255.255.255.0
  mac-sticky enable
  no icmp-guard
  access-group input PERMIT-ALL
  service-policy input NAT-POLICY
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.230.112.1
```

Policy Enforcement

For this validated design, policy enforcement was implemented using different types of Access Control Lists across wired (downloadable (dACL)/static) and wireless (named/flex) access. To validate that a unified policy can be applied to both wired and wireless access without impacting platform performance, a set of test scenarios for partial access use case were executed based on the referenced design. This section outlines the results collected during the test. For more details on the partial access use case, see Design Use Case 1—Enhanced Access.

Sample Partial Access Control Policy

The partial access use case, in addition to Internet, allows the client to access some internal resources. The following partial access ACL allows the client to access the Internet and partially allows access to some internal resources while restricting access to the rest. Based on an enterprise's needs and requirements, they can construct their ACL to allow or deny certain internal resources along with Internet access. The following partial access ACL construct was applied for both wired and wireless scenarios; the configuration commands shown here are the IOS configuration. For wireless, a similar ACL construct was created.

```
dACL_Partial_Access
permit ip any host 10.230.1.45
permit ip any host 10.230.1.46
permit ip any host 10.225.41.114
permit ip any host 10.225.41.115
permit ip any host 10.230.112.200
permit ip any host 10.230.113.201
permit ip any host 10.230.113.202
permit ip any host 10.230.113.203
permit ip any host 10.230.113.204
permit ip any host 10.230.113.205
permit ip any host 10.230.113.206
permit ip any host 10.230.113.207
permit ip any host 10.230.113.208
permit ip any host 10.230.113.209
permit tcp any host 10.225.50.28 eq www
permit tcp any host 10.230.1.81 eq www
deny ip any 10.230.0.0 0.0.255.255
deny ip any 10.225.0.0 0.0.255.255
permit ip any 10.200.16.0 0.0.0.255
deny ip any 10.200.0.0 0.0.255.255
```

```
permit ip any any
```

The access-list shown above has the following characteristics:

- Allow access to DNS servers (10.230.1.45, 10.230.1.46) and ISE Servers (10.225.41.114, 10.225.41.115).
- Deny access to data center subnets (10.230.0.0).
- Deny access to router links 10.225.0.0.
- Allow access to all other internal subnets and Internet access.

The access list is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

Sample Default Access Control Policy

ACL-DEFAULT—This ACL is used as a default ACL on the port and its purpose is to prevent unauthorized access.

In an 802.1X authentication/authorization scenario, after the device is authenticated and authorized, if there is no dACL applied to the port or if there is a mistake in the syntax of the downloadable ACL and the switch rejects the dACL sent by ISE, ACL-DEFAULT protects the port in the above mentioned scenarios. An example of a default ACL is shown below:

```
ACL-DEFAULT
10 permit udp any eq bootpc any eq bootps
20 permit udp any any eq domain
30 permit icmp any any
40 permit udp any any eq tftp
50 deny ip any any log
```

The ACL-DEFAULT shown above allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

Test Methodology

Scale and performance testing of downloadable ACLs (dACLs) were performed on the access switching platforms Catalyst 4500-E, Catalyst 3750-E, and Catalyst 3560-E to enforce policy for unified access BYOD. The goal of these tests was to identify the impact on Ternary Content Addressable Memory (TCAM) resources and CPU utilization when using dACLs with 64 Access control entries (ACEs) and **not** on testing product specific limits, i.e., TCAM exhaustion. In a wireless LAN controller, an ACL can have a maximum of 64 ACEs.

The primary goal for this testing was to promote the use of a single policy and understand the impact of the same ACL with 64 ACEs defined when applied to both of the Catalyst switching platforms to ensure that TCAM allocation and CPU utilization where applicable are within accepted levels. Acceptable levels are considered to be no high CPU utilization and not more than 50% of total TCAM resource consumption.

Test Bed Setup

The tests were performed in the unified access BYOD test bed. The test bed followed the guidelines and configurations as outlined in Design Overview and Configuring the Infrastructure. Multiple authentication and authorization profiles with dynamic ACL configurations were configured in the ISE

to scale across the access platforms. To simulate real world deployments, 64 ACEs with Layer 4 operators were configured. The Partial access use case was used for testing as it usually would have multiple ACEs in a dACL. The 64 ACE partial access dACL was developed based on the sample partial access control policy shown in Sample Partial Access Control Policy. In addition to Internet, partial access allows access to some internal resources. For more details, see Design Use Case 1—Enhanced Access. Functionality, performance, and scaling of DUTs were performed by generating control and data plane traffic using the IXIA Network test tool with PEAP as the authentication mechanism.

Results Summary

A default ACL (ACL-DEFAULT) is statically configured on all ports in the access switch. After authentication the client is authorized by dynamically assigning it to a configured VLAN and by applying a dACL on the access switch interface. The dACL overrides the manually configured default ACL and is enforced until the session is active. The TCAM allocation and CPU utilization are measured for both control and data plane. In summary, TCAM allocation and CPU utilization stayed within accepted levels for the Catalyst 4500-E, Catalyst 3750-E, and Catalyst 3560-E access platforms.

TCAM resources are used when features such as ACL, QoS policy, or IPv4/IPv6 routes are configured in the platform. Blocks of TCAM are allocated for each feature. Each TCAM entry consumes some of the available memory and the total number of entries is limited by the size of available TCAM. The number of TCAM entries used by a dACL varies according to the number of ACEs present in the dACL. Features such as IPv6 can consume more than one TCAM entry. The impact of dACLs on TCAM resources was evaluated for access platforms and compared to the base levels.

TCAM Allocation on Catalyst 4500-E

The Catalyst 4500 has a TCAM utilization enhancement that allows the same TCAM entry to be shared across multiple interfaces when the same dACL is applied. In a scenario where there are multiple clients (MAC addresses) present on the same interface, the TCAM entry is not shared due to client IP address insertion even when the same dACL is used. Each unique dACL consumes TCAM according to the number of ACEs present in it. The Catalyst 4500 with Sup 7E can have up to 128K (64K input + 64K output) entries and with Sup 7LE can have up to 64K (34K input + 34K output) entries. By default all the entries are available under “Input unallocated”. When a feature such as ACL, QoS, etc. is configured, a block of TCAM resource is allocated to it from the unallocated pool. When the allocated block for the feature is consumed, an additional block is allocated to it from the unallocated pool. The TCAM resources are allocated in a similar way for the output entries. The following output shows the TCAM allocation outputs for default ACL and when 44 unique dACLs are applied to each interface on a Catalyst 4500 with Supervisor 7E.

The following output shows the TCAM allocation when the default ACL is configured on 44 interfaces. From the output, we can observe that initially the “Input security” is allocated a 2K (2048) block. A statically configured default ACL consumes 1% of the 2048 block.

```
4500-sup7E#sh platform hardware acl statistics utilization brief
CAM Utilization Statistics
--------------------------

                          Used          Free          Total
                          ---------------------------------
Input  Security    (160)  33    (1  %)  2015  (99 %)  2048
Input  Security    (320)  42    (2  %)  2006  (98 %)  2048
Input  Forwarding  (160)  7     (0  %)  2041  (100%)  2048
Input  Forwarding  (320)  24    (1  %)  2024  (99 %)  2048
Input  Unallocated (160)  0     (0  %)  57344 (100%)  57344

Output Security    (160)  6     (0  %)  2042  (100%)  2048
Output Security    (320)  12    (0  %)  2036  (100%)  2048
```

```
Output Qos          (160)   10     (0  %)  2038  (100%) 2048
Output Qos          (320)   2      (0  %)  2046  (100%) 2048
Output Unallocated (160)    0      (0  %)  57344 (100%) 57344

Input Profiles (logical) : used 1 / 32
Input Profiles (physical): used 4 / 32

Output Profiles (logical) : used 1 / 32
Output Profiles (physical): used 4 / 32
```

The following output shows the TCAM allocation when 44 unique dACLs are applied to each interface. From the output, we can observe the "Input security" is allocated an additional 2K block from "Input unallocated" after it consumed its initially allocated 2K block. When compared to the previous output, we see a considerable increase in TCAM allocation when applying 44 unique dACLs across the interface. From the output we can infer that 44 unique dACLs applied to each interface consume less than 50% of the total TCAM resource.

```
4500-sup7E#sh platform hardware acl statistics utilization brief
CAM Utilization Statistics
--------------------------

                           Used          Free          Total
                           ---------------------------------
Input  Security    (160)   3640  (88 %)  456   (12 %) 4096
Input  Security    (320)   42    (2  %)  2006  (98 %) 2048
Input  Forwarding  (160)   7     (0  %)  2041  (100%) 2048
Input  Forwarding  (320)   24    (1  %)  2024  (99 %) 2048
Input  Unallocated (160)   0     (0  %)  55296 (100%) 55296

Output Security    (160)   6     (0  %)  2042  (100%) 2048
Output Security    (320)   12    (0  %)  2036  (100%) 2048
Output Qos         (160)   10    (0  %)  2038  (100%) 2048
Output Qos         (320)   2     (0  %)  2046  (100%) 2048
Output Unallocated (160)   0     (0  %)  57344 (100%) 57344

Input Profiles (logical) : used 1 / 32
Input Profiles (physical): used 4 / 32

Output Profiles (logical) : used 1 / 32
Output Profiles (physical): used 4 / 32
```

TCAM Allocation on Catalyst 3560E/3750E

At present the Catalyst 3750E/3560E requires multiple TCAM entries when the same dACL is applied to multiple interfaces, as there is no concept of shared TCAM resources as there is with the Catalyst 4500. Due to this, the TCAM allocation remains the same when the same or unique dACLs are applied to different interfaces. Each dACL consumes TCAM resources according to the number of ACEs present in it. The following output shows the TCAM allocation outputs for the default ACL and when 44 unique dACLs are applied to each interface on the Catalyst 3750E.

The following output shows the TCAM allocation when the default ACL is configured on 44 interfaces. "IPv4 security aces" in ASIC#1 and ASIC#2 shows the TCAM allocation.

```
bn6-3750x-1#sh platform tcam utilization asic all

CAM Utilization for ASIC# 0                    Max            Used
                                             Masks/Values    Masks/values

 Unicast mac addresses:                       6364/6364        113/113
 IPv4 IGMP groups + multicast routes:         1120/1120          1/1
 IPv4 unicast directly-connected routes:      6144/6144         73/73
 IPv4 unicast indirectly-connected routes:    2048/2048         48/48
```

```
 IPv4 policy based routing aces:               452/452          12/12
 IPv4 qos aces:                                512/512          21/21
 IPv4 security aces:                           964/964          38/38

Note: Allocation of TCAM entries per feature uses
a complex algorithm. The above information is meant
to provide an abstract view of the current TCAM utilization


CAM Utilization for ASIC# 1                      Max            Used
                                                Masks/Values    Masks/values

 Unicast mac addresses:                        6364/6364        113/113
 IPv4 IGMP groups + multicast routes:          1120/1120          1/1
 IPv4 unicast directly-connected routes:       6144/6144         73/73
 IPv4 unicast indirectly-connected routes:     2048/2048         48/48
 IPv4 policy based routing aces:                452/452           0/0
 IPv4 qos aces:                                 512/512          21/21
 IPv4 security aces:                            964/964          44/44

Note: Allocation of TCAM entries per feature uses
a complex algorithm. The above information is meant
to provide an abstract view of the current TCAM utilization


CAM Utilization for ASIC# 2                      Max            Used
                                                Masks/Values    Masks/values

 Unicast mac addresses:                        6364/6364        113/113
 IPv4 IGMP groups + multicast routes:          1120/1120          1/1
 IPv4 unicast directly-connected routes:       6144/6144         73/73
 IPv4 unicast indirectly-connected routes:     2048/2048         48/48
 IPv4 policy based routing aces:                452/452           0/0
 IPv4 qos aces:                                 512/512          21/21
 IPv4 security aces:                            964/964          44/44

Note: Allocation of TCAM entries per feature uses
a complex algorithm. The above information is meant
to provide an abstract view of the current TCAM utilization
```

The following output shows the TCAM allocation when 44 unique dACLs are applied to each interface. “IPv4 security aces” in ASIC#1 and ASIC#2 shows the TCAM allocation. When compared to the previous output, we see a considerable increase in TCAM allocation when applying 44 unique dACL across the interface. From the output we can observe that 44 separate dACLs consume less than 50% of the total TCAM resource allocated for the feature.

```
3750E#sh platform tcam utilization asic all

CAM Utilization for ASIC# 0                      Max            Used
                                                Masks/Values    Masks/values

 Unicast mac addresses:                        6364/6364        114/114
 IPv4 IGMP groups + multicast routes:          1120/1120          1/1
 IPv4 unicast directly-connected routes:       6144/6144         77/77
 IPv4 unicast indirectly-connected routes:     2048/2048         86/86
 IPv4 policy based routing aces:                442/442          12/12
 IPv4 qos aces:                                 512/512          21/21
 IPv4 security aces:                            954/954          44/44

Note: Allocation of TCAM entries per feature uses
a complex algorithm. The above information is meant
to provide an abstract view of the current TCAM utilization
```

```
CAM Utilization for ASIC# 1                    Max            Used
                                             Masks/Values    Masks/values

 Unicast mac addresses:                       6364/6364        114/114
 IPv4 IGMP groups + multicast routes:         1120/1120          1/1
 IPv4 unicast directly-connected routes:      6144/6144         77/77
 IPv4 unicast indirectly-connected routes:    2048/2048         86/86
 IPv4 policy based routing aces:               442/442           0/0
 IPv4 qos aces:                                512/512          21/21
 IPv4 security aces:                           954/954         252/252

Note: Allocation of TCAM entries per feature uses
a complex algorithm. The above information is meant
to provide an abstract view of the current TCAM utilization


CAM Utilization for ASIC# 2                    Max            Used
                                             Masks/Values    Masks/values

 Unicast mac addresses:                       6364/6364        114/114
 IPv4 IGMP groups + multicast routes:         1120/1120          1/1
 IPv4 unicast directly-connected routes:      6144/6144         77/77
 IPv4 unicast indirectly-connected routes:    2048/2048         86/86
 IPv4 policy based routing aces:               442/442           0/0
 IPv4 qos aces:                                512/512          21/21
 IPv4 security aces:                           954/954         212/212


Note: Allocation of TCAM entries per feature uses
a complex algorithm. The above information is meant
to provide an abstract view of the current TCAM utilization
```

Appendix A—References

Cisco BYOD Smart Solution:
http://www.cisco.com/go/byod/

TrustSec Guides:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Unified Access Design Guide:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/Unified_Access_Book.html

Flex 7500 Wireless Branch Controller Deployment Guide:
http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml#override

Wireless BYOD for FlexConnect Deployment Guide:
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bcb905.shtml

FlexConnect Feature Matrix:
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b3690b.shtml

Cisco ISE, Release 1.1.1 Documentation:
http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html

Catalyst 4500 Series Switch Software Configuration Guide
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/15.1/XE_330SG/configuration/guide/dot1x.html#wp1324657

Catalyst 3750 Switch Software Configuration Guide
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/15.0_2_se/configuration/guide/sw8021x.html#wp1434612

Catalyst 3560 Switch Software Configuration Guide

http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/15.0_2_se/configuration/guide/sw8021x.html#wp1434612

Cisco Borderless Campus 1.0 Cisco Validated Design Guide:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1.0/Borderless_Campus_1.0_Design_Guide.html

Medianet Campus QoS Design 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html

Cisco AnyConnect 3.1 Administrator Guide:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/administration/guide/anyconnectadmin31.html

Configuring Certificates:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

Configuring Tunnel Groups, Group Policies, and Users:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/vpngrp.html

iPhone OS Enterprise Deployment Guide:
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Cisco Enterprise Mobility 4.1 Design Guide:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

For further information regarding Cisco Jabber clients, see the product collateral and documentation:
http://www.cisco.com/go/jabber

Cisco Unified Communications System 9.X SRND:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/9x/mobilapp.html

Cisco Visual Networking Index:

http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

Appendix B—Software Versions

The following tables highlight the hardware and software components used for validation testing in this design guide. While other software versions provide the required BYOD functionality, the Validated Software Version column indicates the software version used during the validation.

For specific feature support, consult the Cisco Feature Navigator: http://www.cisco.com/go/fn.

Table 23 Security

Component	Role	Validated Software Version
Active Directory	Server	Windows 2008 Server R2
Certificate Authority	Server	Windows 2008 Server R2

Table 23 Security

Component	Role	Validated Software Version
RSA Authentication Manager	Server	7.1
Identity Services Engine	Authentication/Policy Server	1.1.1.268

Table 24 Wired Access

Component	Role	Validated Software Version
Catalyst 3560-X	Wired Access	15.0(2)SE
Catalyst 3750-X	Wired Access	15.0(2)SE
Catalyst 2960S	Branch Access	15.0(2)SE
Catalyst 4500E Sup7-E	Wired Access/Distribution	3.3.1SG
Catalyst 6500 VSS 1400 Catalyst 6500-E VSS4T	Campus Distribution/Core	15.0(1)SY2 - Sup2T 12.2(33)SXJ3 - Sup720
Cisco Nexus® 7000	Campus Core/Data Center	5.2.5
MacBook	Wired/Wireless Device	OSX 10.6.8
Windows Laptop	Wired/Wireless Device	64 bit Windows 7

Table 25 Wireless Access

Component	Role	Validated Software Version
AP3502	Access Point	N/A
AP3602	Access Point	N/A
AP2602	Access Point	N/A
Cisco 5508 Wireless Controller	Wireless LAN Controller	7.3.101.0
Flex 7500 Wireless Controller	Wireless LAN Controller	7.3.101.0
iPad	Wireless Device	iOS 5.1.1 and 6.0
iPhone®	Wireless Device	iOS 5.1.1
Asus Transformer Primer 201	Wireless Device	Android 4.0.3
Samsung™ GT-P7510 Galaxy Tab	Wireless Device	Android 3.2
Samsung Galaxy Tab 8.9 LTE	Wireless Device	Android 3.2
Samsung Galaxy SIII	Wireless Device	Android 4.0.4
Samsung Galaxy Nexus	Wireless Device	Android 4.0.4

The document *Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x* provides a detailed description of which end user devices are supported (http://www.cisco.com/en/US/docs/security/ise/1.1.1/compatibility/ise_sdt.html#wp80321).

Appendix C—BYOD Access Policies

Figure 350 highlights the different access policies tested in this design guide, along with the different requirements and permissions granted by each policy. These policies, along with detailed configurations, are explained in this design guide.

Figure 350 Access Policies and Permissions

Policy	Identity Group	AD Group	Profile	Permission	
Personal_Full Access	RegisteredDevices	BYOD_Access		Full	
Personal_Partial Access	RegisteredDevices	Domain Users		Partial	
Personal_Internet Only	RegisteredDevices	Internet_Access		Internet Only	
Corporate Owned	Whitelist	Corp_Devices		Full	
Deny Android Devices			Android	Deny	
Employee on Guest SSID		In AD Group		Internet Only	
Employee on Guest-Like SSID		In AD Group		Partial	
Guests				Internet Only	

292826