Avaya Identity Engines for Avaya Unified Access

Release 9.1
NN47280-503
Issue 02.01
March 2015

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

Avaya Identity Engines for Avaya Unified Access, NN47280–503 is written for network administrators using the Avaya Identity Engines Ignition Server. As an administrator, you are responsible for configuring and maintaining the users, devices, objects, policies, and configurations that Identity Engines Ignition Server uses to secure and control access to your networks and other resources. You must be familiar with network terminology, have experience setting up and maintaining networks, and understand their security implementations.

This document provides information specific to integration between Avaya Identity Engines and Avaya Networking products. Avaya Identity Engines is vendor-agnostic and may be deployed over any vendor standard-based network. Nevertheless, some unique capabilities have been incorporated into Identity Engines that enhance the administration of the deployment and the user experience. This document provides details that are specific to:

- Avaya WLAN 9100
- Avaya Fabric Attach

Avaya WLAN 9100:

This document explains the Identity Engines licensing model with respect to WLAN 9100.

In addition, the document explains how to add a device (for example, a WLAN 9100 Series wireless access point) to Identity Engines to act as an authenticator. An authenticator is a device (wired switch, wireless access point, or VPN gateway) that allows users and devices to connect to your network. The Identity Engines Ignition Server provides access control and service provisioning for wireless access points (WAPs) when the access points are configured as authenticators in Ignition Server.

Avaya Fabric Attach:

This document explains how to configure and use the Identity Engines Ignition Server as a Fabric Attach (FA) Policy server for edge automation.

In addition, the document explains how to use Identity Engines as an FA Policy server with ERS FA Proxy Standalone and FA Client WLAN 9100, including example use cases and access policies.

Related resources

Documentation

See the following related documents.

Title	Purpose	Document number
Avaya Identity Engines Ignition Server Getting Started	Installation and simple configuration	NN47280–300
Avaya Identity Engines Ignition Server Administration	All configuration options	NN47280–600
Configuring and Managing Avaya Identity Engines Single-Sign-On	Configuration, management, and deployment	NN47280–502
Avaya Identity Engines Ignition Guest Manager Configuration	Installation, configuration, and management	NN47280–501
Avaya Identity Engines Ignition CASE Administration	Installation, configuration, and deployment	NN47280–603
Avaya Identity Engines Ignition Access Portal Administration	Installation, configuration, and deployment	NN47280–604
Avaya Identity Engines Ignition Analytics	Installation, configuration, and maintenance	NN47280–601
Avaya Identity Engines Ignition Server Release Notes	Reference	NN47280–400

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

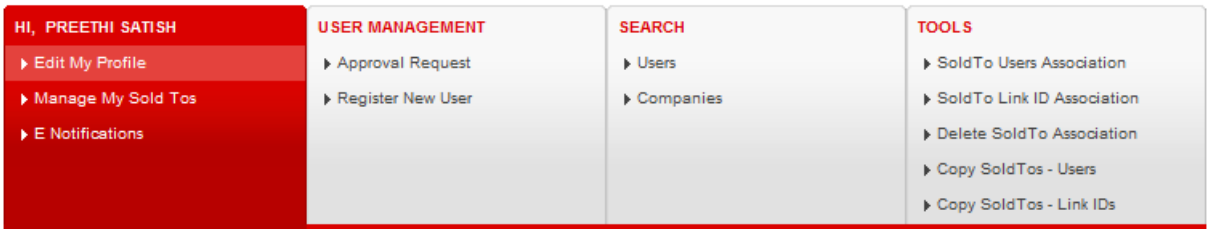
About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

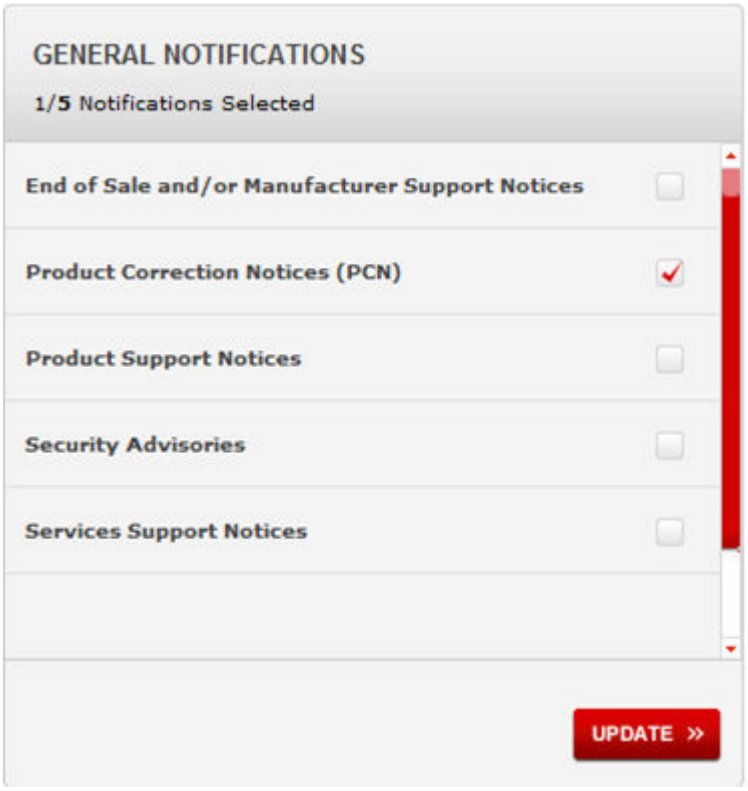
Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Click **MY PROFILE**.

4. On the site toolbar, click your name, and then click **E Notifications**.

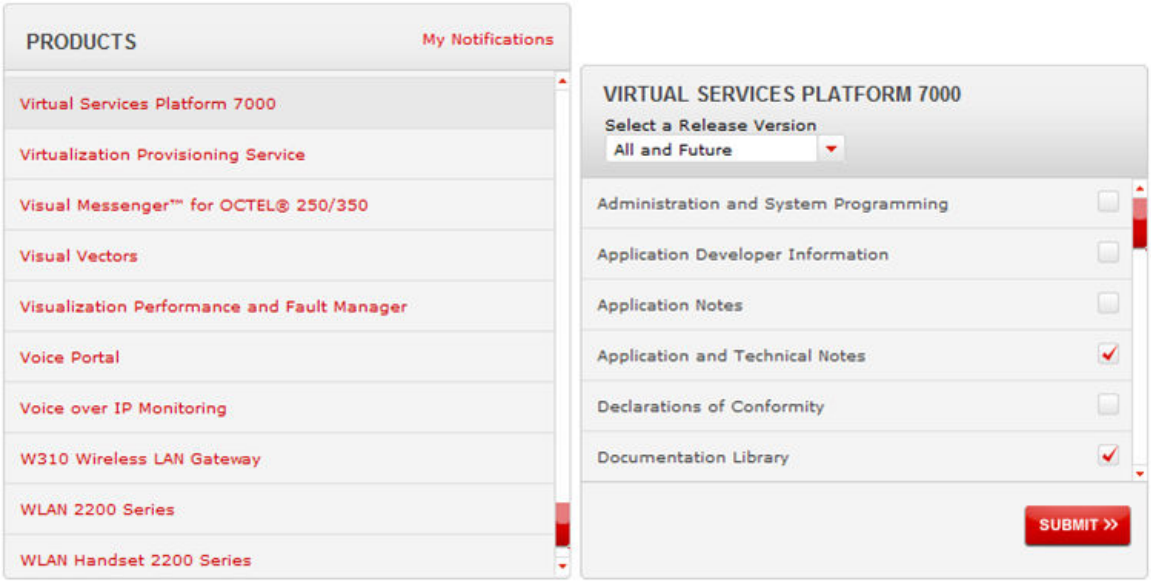


5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments

6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

Avaya Identity Engines for Avaya Unified Access, NN47280–503 has been renamed and updated to support the following product releases:

- Avaya Identity Engines Release 9.1
- Avaya WLAN 9100 Series Release 7.2.5
- Avaya ERS 4800 Series Release 5.9 (when available)
- Avaya ERS 5900 Series Release 7.0 (when available)

Chapter 3: Overview

What is Avaya Identity Engines Ignition Server?

Avaya Identity Engines Ignition Server is an enterprise grade network access policy server. The Ignition server is also an 802.1X-capable RADIUS authentication server that grants users and their devices different access levels, or denies users access to your network based on your access policies. Use the Ignition Server to create a single set of policies that control access for all of the ways that users connect: through wired, wireless, or VPN. Ignition Server stores access policies, while user accounts remain in your traditional user store(s), such as such as Microsoft Active Directory, Open LDAP, Novell eDirectory, RSA Authentication Server, and others.

Ignition Server includes an easy-to-configure policy engine that lets you make network access decisions based on the user's identity, account details and group memberships, location of the login attempt, time of day, and other pieces of information. For example, an Ignition Server policy can grant users access based on their identity, their point of access (which network switch or WAP they are connecting through), and their laptop security state (ensuring their laptop is a company-owned laptop as recorded in the corporate Active Directory store).

Ignition Server's abilities to check whether a user's workstation has passed MAC authentication and Windows machine authentication are key features that set it apart from other network access control tools. Ignition Server lets you combine many policy elements to enforce a single rule, such as how to authenticate a user with PEAP/MSCHAPv2, check that their device has been authenticated, and if those are successful, assign the user to the appropriate VLAN based on their role. Ignition Server also authenticates devices. You can configure Ignition Server to offer a bypass of 802.1X authentication for older devices on your network that cannot perform an 802.1X authentication by using the Ignition Access Portal.

Key characteristics of Ignition Server

The following are the most important, distinct characteristics of Ignition Server:

- **Non-intrusive, out-of-band:** Ignition Server is an out-of-band access control solution and thus easier to install and to scale up than an inline solution. "Out-of-band" means that only the client's *network sign-on transaction* travels through Ignition Server. After it is signed on, the client's network traffic travels its usual path.
- **Standards-oriented:** Since Ignition Server is a standards-compliant RADIUS server, it interacts with and can control nearly *every* type of network endpoint: wired switches, wireless access points, and VPN concentrators.

- **Consolidated AAA platform:** Ignition Server handles the three A's: authentication, authorization and accounting. Ignition Server works with your existing authentication servers (SecurID, Active Directory, and so on) to authenticate the connecting user or device; it uses its policy engine and provisioning framework to authorize the user/device, and it maintains accounting records (audit log) of these connection events in a number of formats.
- **Scales up well:** One Ignition Server serves as the AAA/RADIUS server for *many* network-edge devices: wired, wireless, and VPN.
- **Multiple directory support:** No duplication of user accounts is required. Ignition Server authenticates users and devices against your existing data store that holds those accounts. Ignition Server retrieves information about the user and/or device from many different types and instances of directories: Active Directory, Novell eDirectory, SunONE LDAP, Oracle OID, LDAP, the Ignition Server-local internal store, and others.
- **Split authentication/lookup:** Ignition Server can be configured to authenticate the user against one service and retrieve his or her account details from a separate service for authorization. For example, you can authenticate using RSA SecurID and look up the user account from an LDAP service.
- **Very flexible policy engine:** Ignition Server lets the network administrator use a wide range of criteria including user attributes, device attributes, access type, location, date/time, and others, to make precise, targeted access decisions.
- **Guest access:** A suite of supporting tools lets the network administrator safely and efficiently grant guests access to the network. Avaya Ignition Server Guest Manager delegates the administrative task of adding temporary users and importing groups of temporary users, and it can allow self provisioning, if so configured.
- **Role-based networking** (also called role-based access control): The user's role or group affiliation recorded in the directory determines what networks and resources he or she can access.
- **High Availability:** You can deploy two Ignition Servers as a linked pair that offers a highly available RADIUS service. You can also exchange user and device details between geographically dispersed Ignition Servers for Extended high availability.

What are Avaya WLAN 9100 Series Wireless Access Points?

The Avaya 9100 Series Wireless Access Points (WAPs) are designed to provide distributed intelligence, integrated switching capacity, application-level intelligence, increased bandwidth, and smaller size. The radios support IEEE802.11 ac, a, b, g, and n clients, and feature the capacity and performance needed to replace switched Ethernet to the desktop.

The Wireless Access Point is a high capacity, multi-mode device. Its distributed intelligence eliminates the use of separate controllers and their accompanying bottlenecks.

The Avaya 9100 Series Wireless Access Points are Wi-Fi® compliant and simultaneously support 802.11ac (on .11ac models), 802.11a, 802.11b, 802.11g, and 802.11n clients. The multi-state

design allows you to assign radios to 2.4 GHz and 5 GHz bands (or both) in any desired arrangement. Integrated switching and active enterprise class features such as VLAN support and multiple SSID capability enable robust network compatibility and a high level of scalability and system control.

What is Avaya ERS 4800 switch?

The Avaya Ethernet Routing Switch 4800 Series is a stackable chassis system providing high-performance, convergence-ready, secure and resilient Ethernet switching connectivity. It also uniquely delivers virtual fabric services to the network edge environment through its support of Avaya Fabric Connect. Available in four model variants, supporting 10/100/1000 switching and routing, Power-over-Ethernet/Power-over-Ethernet+, and 1 and 10 Gigabit Ethernet SFP+ uplink options, the Ethernet Routing Switch 4800 Series is ideally suited for next-generation network edge deployments.

What is Avaya ERS 5900 switch?

The Avaya Ethernet Routing Switch 5900 Series is a premium stackable chassis system providing high-performance, convergence-ready, resilient and more secure Ethernet switching connectivity. Supporting Avaya Fabric Connect, it also delivers virtual fabric services to the network edge/wiring closet environment. Available in 4 model variants supporting 10/100/1000 switching and routing, 40 uplink capacity Gbps (4 x SFP+) and Power-over-Ethernet+, the Ethernet Routing Switch 5900 is ideally suited for high-end wiring closet and network edge deployments.

Chapter 4: Ignition Server licensing for WLAN 9100

The Identity Engines Ignition Server has two types of base licenses:

- Ignition Base license – A mandatory license that is based on the number of authenticators (such as the WLAN Access Point 9100) that the Ignition Server will service from a network access control perspective – that is, receive authentication requests and respond with authentication results and service authorization.
- Feature license – An optional license(s). There are different feature licenses such Guest Manager, Access Portal and others.

Identity Engines provides special treatment to the Avaya WLAN 9100 from a licensing perspective as follows:

- Ignition Server Base LITE - 5 Standard Authenticators + 75 x AP 9100
- Ignition Server Base SMALL - 20 Standard Authenticators + 300 x AP 9100
- Ignition Server Base LARGE - Unrestricted Standard Authenticators and AP 9100

To make use of the enhanced licensing support for WLAN 9100, Identity Engines Release 9.0.3 introduced a new Vendor called “Avaya-WLAN” with Vendor ID 45. To configure a WLAN 9100 AP as an authenticator on the Ignition Server, you must choose the following configuration settings:

- Authenticator Type: Wireless
- Vendor: Avaya-WLAN
- Device Template: generic-avaya-wlan

Important:

The minimum software release for the WLAN 9100 AOS is 7.2.5

Chapter 5: Ignition Server configuration for WLAN 9100 Series APs

Each WLAN 9100 Series Access Point (AP) must be configured to point to Identity Engines as its external RADIUS Server.

The following configuration must be performed on the Ignition Server:

- Configure WLAN AP 9100 as an Authenticator. See Configuring WLAN AP 9100 as an Authenticator on page 16.
- Configure the Outbound Values. See Configuring the Outbound Values on page 17.

You must follow the instructions on how to configure WLAN AP 9100 as an Authenticator on the Ignition Server in order to take advantage of the enhanced licensing support for WLAN AP 9100.

Configuring WLAN AP 9100 as an Authenticator

Procedure

1. In the Dashboard Configuration tree, expand **Site Configuration** > **Authenticators**, select a container, and click **New**.

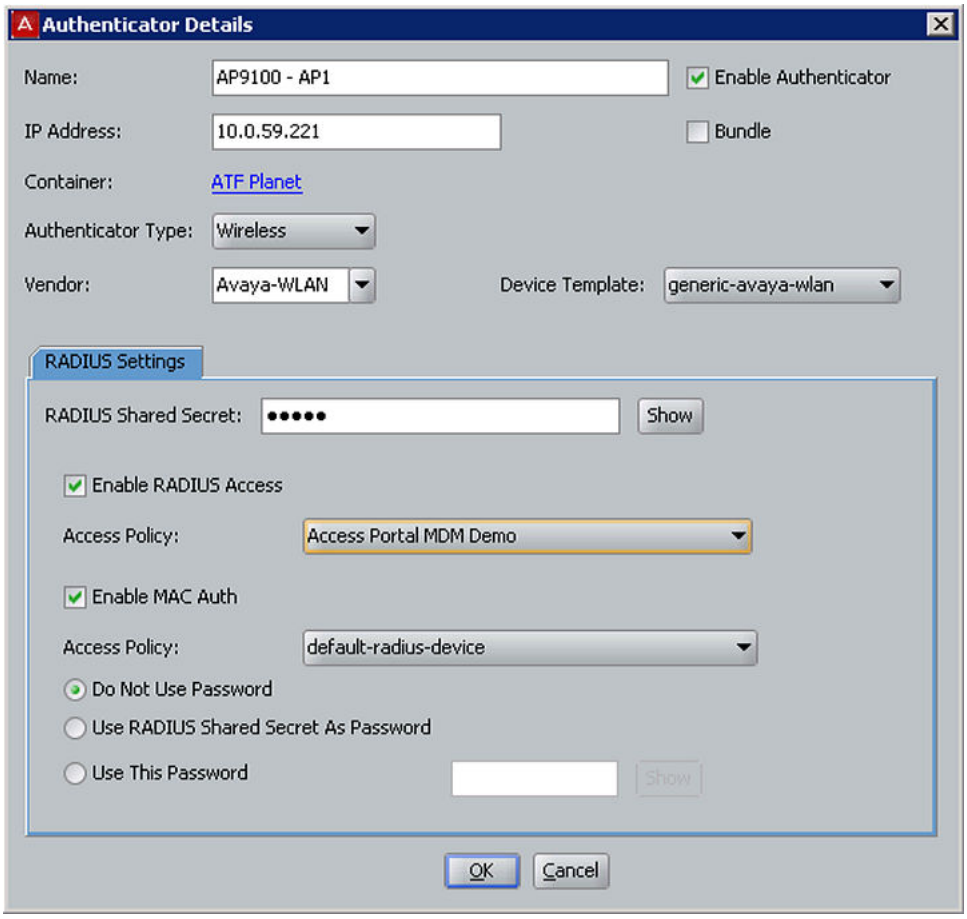
   The Authenticator Details window displays.

2. Fill out the Authenticator details as follows:
   - Enter a name in the **Name** field.
   - Enter the IP address of the AP 9100 in the **IP Address** field.
   - Select **Wireless** from the **Authenticator Type** drop-down list.
   - Select **Avaya-WLAN** from the **Vendor** drop-down list.
   - Select **generic-avaya-wlan** from the **Device Template** drop-down list.
   - Enter the pre-shared key RADIUS Shared Secret in the **RADIUS Shared Secret** field. The Shared Secret must match the Shared Secret entered on the AP9100 itself.
   - Based on your network access design, do one or both of the following:
     - Select the **Enable RADIUS Access** checkbox and select the appropriate Ignition Server RADIUS Access Policy from the **Access Policy** drop-down list.

- Select the **Enable MAC Auth** checkbox and select the appropriate Ignition Server MAC Access Policy from the **Access Policy** drop-down list.

3. Click **OK**.

   The following example shows a WLAN 9100 Access Point configured as an Authenticator on the Ignition Server:



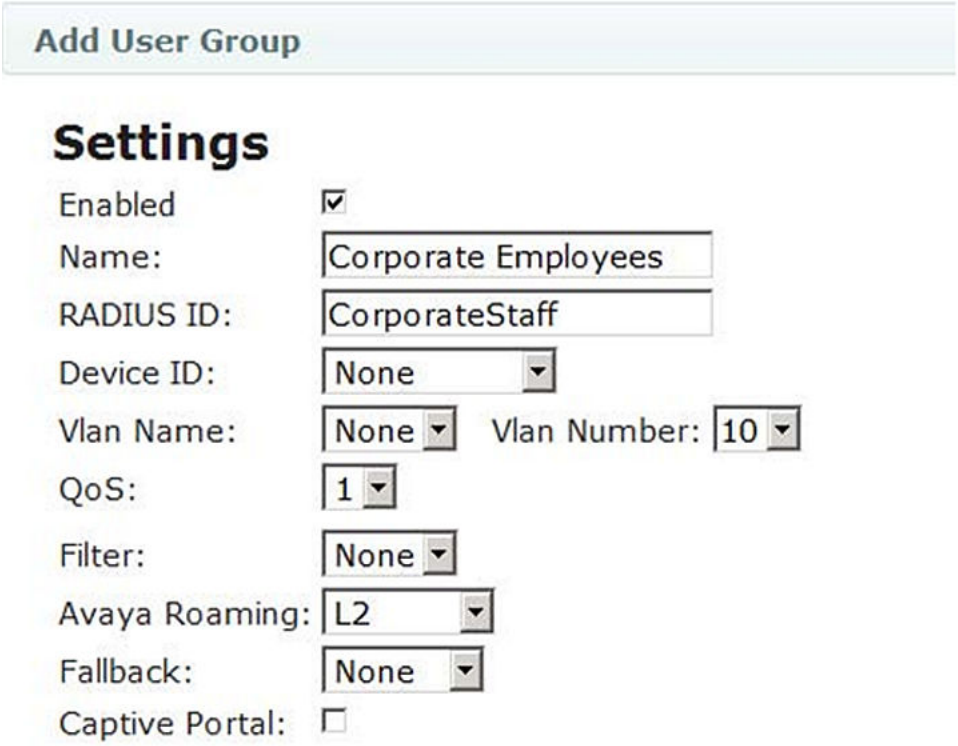
Configuring the Outbound Values

This section contains three examples that illustrate how to configure the Outbound Values for Avaya WLAN 9100.

Outbound Value for assigning a WLAN 9100 Group

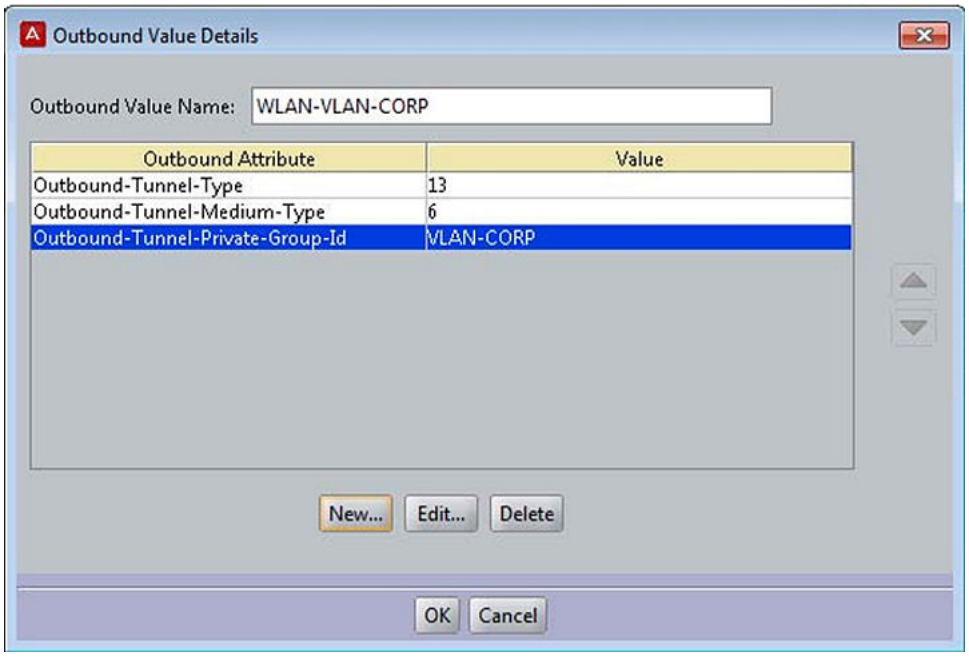
One method for controlling access of a wireless client is by sending an Outbound Value that instructs the WAP 9100 to assign the user that is being authenticated to a specific WLAN 9100 Group. The string value of the standard RADIUS Outbound Attribute Outbound-Filter-Id must *exactly match* the string entered in the WAP 9100 field RADIUS ID for a Group in a Profile.

In this example, the WLAN 9100 AP is configured with a User Group with the RADIUS ID set to “CorporateStaff”. The Outbound Value on the Ignition Server sent to the AP 9100 as a result of a successful authentication and authorization must contain the exact same value of “CorporateStaff” in order for the AP 9100 to apply the User Group to the wireless client traffic:



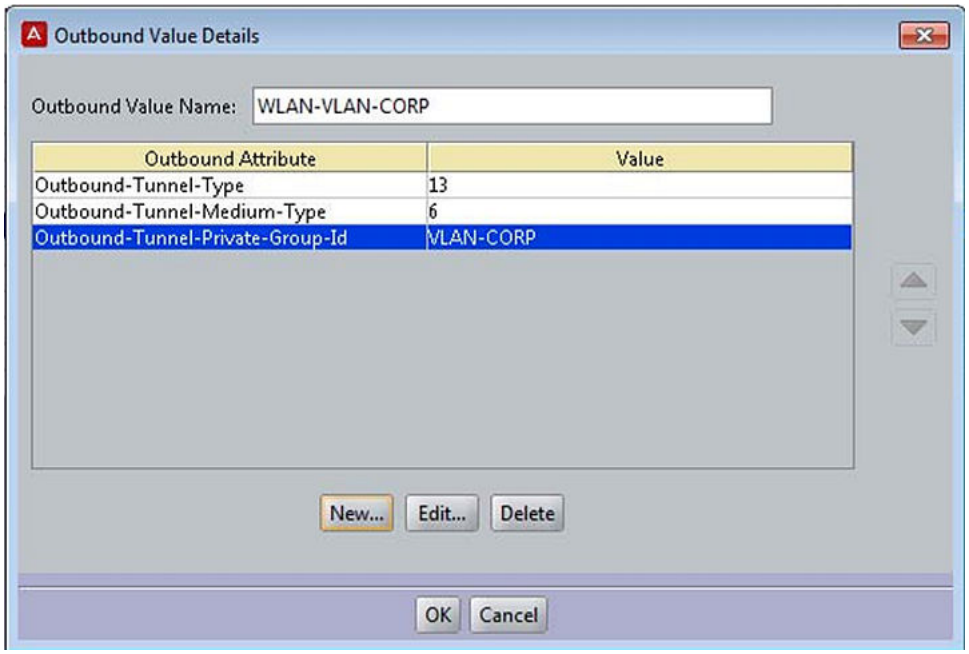
Outbound Value for assigning a VLAN Name

Another method for controlling access of a wireless client is by sending an Outbound Value that instructs the WAP 9100 to assign the user that is being authenticated to a specific WLAN 9100 VLAN Label (VLAN Name):



Outbound Value for assigning a VLAN ID

Another method for controlling access of a wireless client is by sending an Outbound Value that instructs the WAP 9100 to assign the user that is being authenticated to a specific WLAN 9100 VLAN ID (VLAN Number):



Configuring APs as Authenticators in bulk

If you need to create multiple AP authenticators, you can create them in bulk by importing the authenticator information in a specified comma-separated values (CSV) format.

For information, see the section “Importing authenticators” in *Administering Avaya Identity Engines Ignition Server,* NN47280-600.

Chapter 6: Identity Engines Fabric Attach

One of the key benefits of Avaya Fabric Connect technology is simplified operations through access layer only network provisioning. Avaya Fabric Connect delivers an automated core that virtually eliminates the chance of core network misconfiguration. It allows simple and secure deployment of network services without the need to make any configuration changes on intermediate/core nodes, even in environments where clients roam. These benefits had been available only on Avaya Fabric Connect-capable devices.

Avaya has developed Fabric Attach (FA) to extend these same benefits to network elements or hosts that are *not* SPB-capable. Avaya Fabric Attach extends Fabric Connect to deliver Edge Automation capability that reduces the complexity of adding or modifying services. Any FA-capable device (such as a switch or AP) can now be securely connected to the network, be authorized for a network service, and attach to the appropriate network service instance – all automated and based on IT policy.

Fabric Attach elements

The Fabric Attach elements consist of the following:

- FA Server: Avaya Ethernet switch that supports FA Signaling and is Fabric Connect capable.
- FA Proxy: Avaya Ethernet switch that supports FA Signaling and is not Fabric Connect capable.
- FA Client: Ethernet device that supports FA Signaling, and may or may not be an Avaya device.
- FA Policy Server: Avaya network access policy server.

Fabric Attach uses FA Signaling. FA Signaling is an application-level protocol that leverages standard network protocols to exchange messages and data between Fabric Attach elements to orchestrate network edge automation.

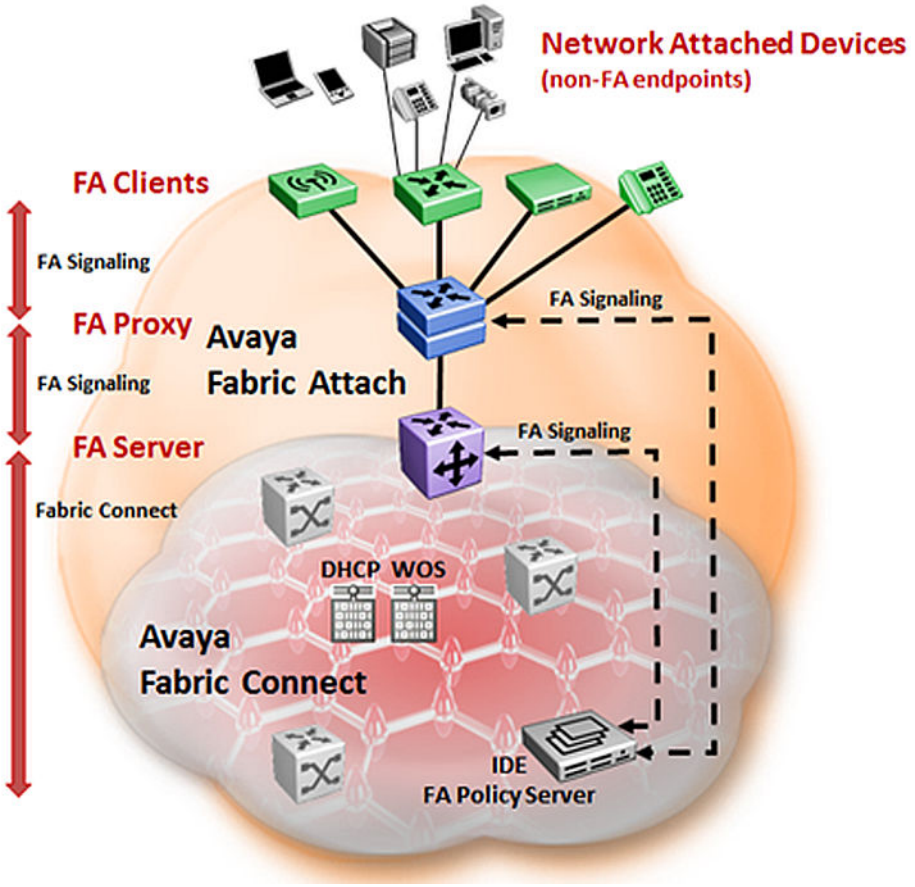


Figure 1: Fabric Attach elements

Access edge automation

A network that deploys Avaya Fabric Connect takes full advantage of automating the access edge through Fabric Attach. Fabric Connect virtualized services extend to the network access layer:

- Automated and secure core with SPB
- Automated and secure edge with Fabric Attach

Network access automation through Fabric Attach on a legacy network (no SPB) allows customers to leverage automation for access/aggregation layers and provides a migration path to full automation with Fabric Connect later. When the customer is ready, Fabric Connect core can be implemented to add end-to-end virtualized services with no changes needed at the access/ aggregation layers:

- Automated and secure edge with Fabric Attach

A unique mode of operation of the FA Proxy switch is FA Proxy Standalone. With FA Proxy Standalone, customers achieve wiring closet access edge automation with Fabric Attach technology to automate the edge, without requiring an FA Server:

- Automated and secure edge of standard (non-FA) and FA Clients

With FA Proxy Standalone, customers benefit from automation of service provisioning (VLAN-based only). This document focuses on providing use case examples of wiring closet access edge automation with:

- ERS 4800 as FA Proxy Standalone
- WLAN AP9100 as FA Client
- Identity Engines as FA Policy server

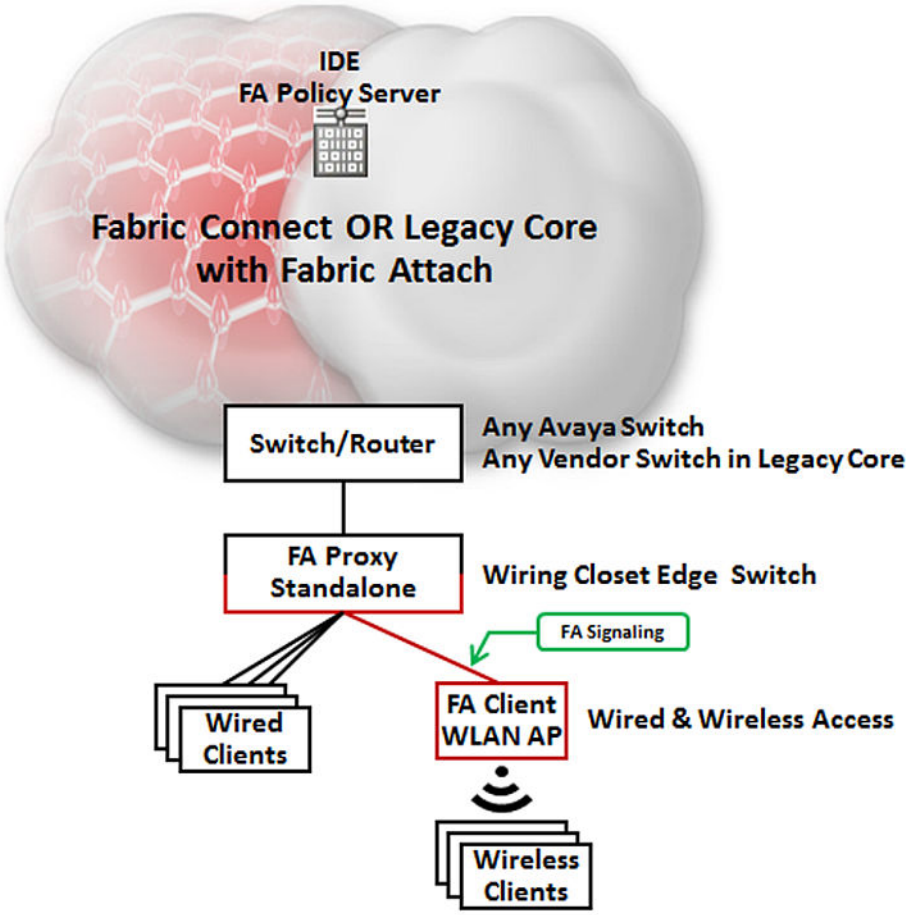


Figure 2: FA Proxy Standalone deployment

Configuring WLAN AP 9100 as FA client

This section provides configuration tips and general direction for deploying a WLAN 9100 Access Point as a FA client. Detailed configuration information is available in the following documents:

- *Using the Avaya Wireless Orchestration System*, NN47252-103
- *Using the Avaya OS for Avaya WLAN AP 9100 Series*, NN47252-102

Avaya WLAN 9100 Access Point requires a minimum software level of AOS Release 7.2.5 to incorporate FA client capability.

Fabric Attach setting on WOS

The Network configuration page of the Access Point controls the Avaya Fabric Attach settings and LLDP settings. Link Layer Discovery Protocol (LLDP) is a Layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. Access Points can both advertise their presence by sending LLDP announcements, and gather and display information sent by neighbors. The LLDP protocol is used by FA Signaling for discovery and communication.

Use the Configuration window to configure your Fabric Attach and LLDP settings.

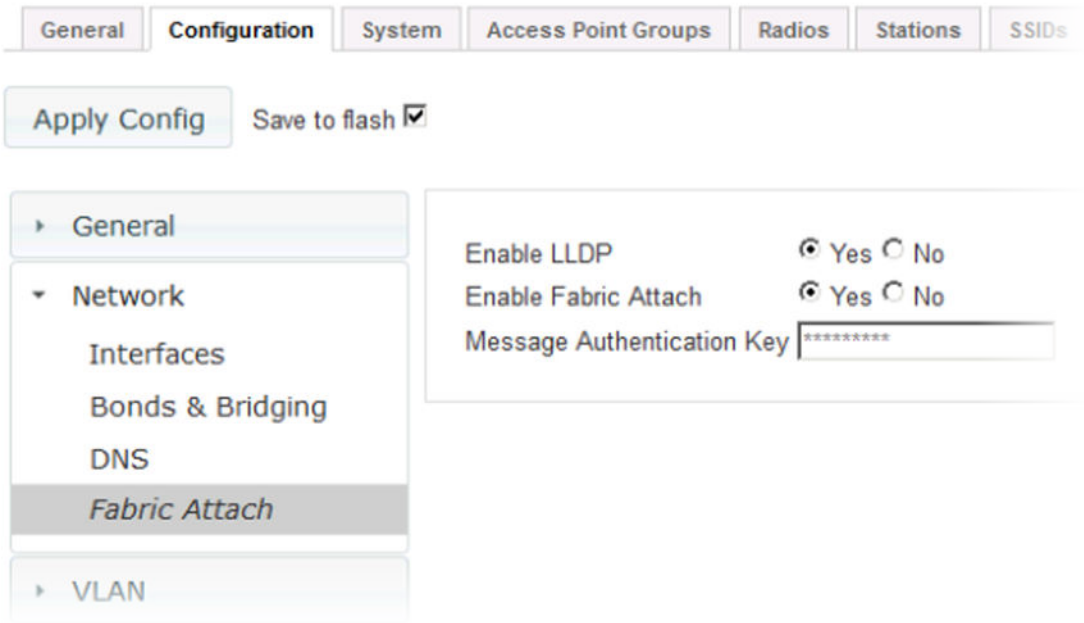


Figure 3: Fabric Attach settings

Configuring Fabric Attach settings on WOS

Procedure

1. Enable LLDP. Select **Yes**.

   When LLDP in enabled, the Access Point sends out LLDP announcements of the Access Point's presence and gathers LLDP data sent by neighbors. When disabled, it does neither. LLDP is enabled by default.

2. Enable Fabric Attach. Select **Yes** to enable the WAP as a Fabric Attach client device.

   Access Points support the Avaya Fabric Attach feature to simplify network deployment. Fabric Attach is enabled by default. Fabric Attach uses LLDP packets for communication and requires LLDP to be enabled.

3. Enter the Message Authentication Key used by Fabric Attach. Enter a key of length 1 to 32 octets. The key must match the key on the FA Proxy Standalone.

Access Point details for Fabric Attach

The Access Point details page for Fabric Attach shows Fabric Attach information for the Access Point in two tables: Fabric Attach Status and Fabric Attach Elements. LLDP must be enabled on the Access Point to gather and display this information.

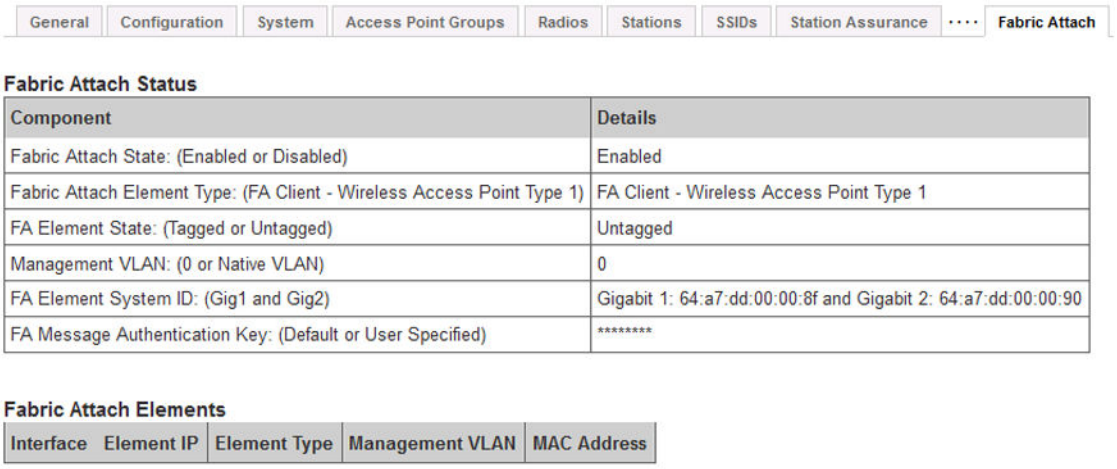


Figure 4: Access Point details

The Fabric Attach Status table shows the FA configuration for this WAP, including the management VLAN (this is the WAP's Native VLAN if one is defined, else 0), and whether tagging is in use.

The Fabric Attach Elements table shows other network elements that are known to this WAP and that play a role in Fabric Attach. The types of elements include FA Server, FA Proxy, FA Server—No Auth, and FA Proxy—No Auth.

The WAP uses LLDP to perform FA Signaling for discovery on the network on an ongoing basis. For each FA element, this table shows the IP and MAC Address, the device interface that is connected to the network (the port that was discovered), and the management VLAN.

Fabric Attach settings on AOS

This status only window lists devices on the WAP's network that support the Link Layer Discovery Protocol (LLDP). This allows you to see Avaya switches that you are using to supply power and data to your WAPs.

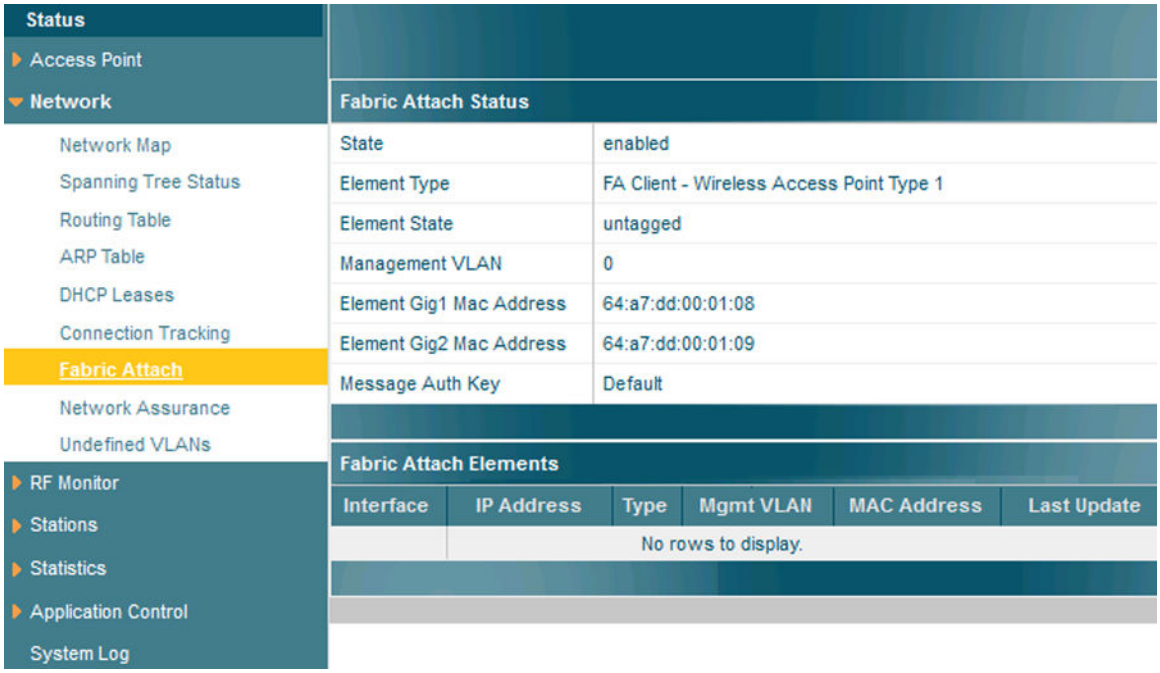


Figure 5: LLDP list

The WAP performs discovery on the network on an ongoing basis. This list shows the devices that are discovered — devices on the network that have LLDP running. For each device, it shows the device's host name, IP address and model name, the device interface that is connected to the network (that is, the port that was discovered), and the network capabilities of the device (such as switch, router, and supported protocols).

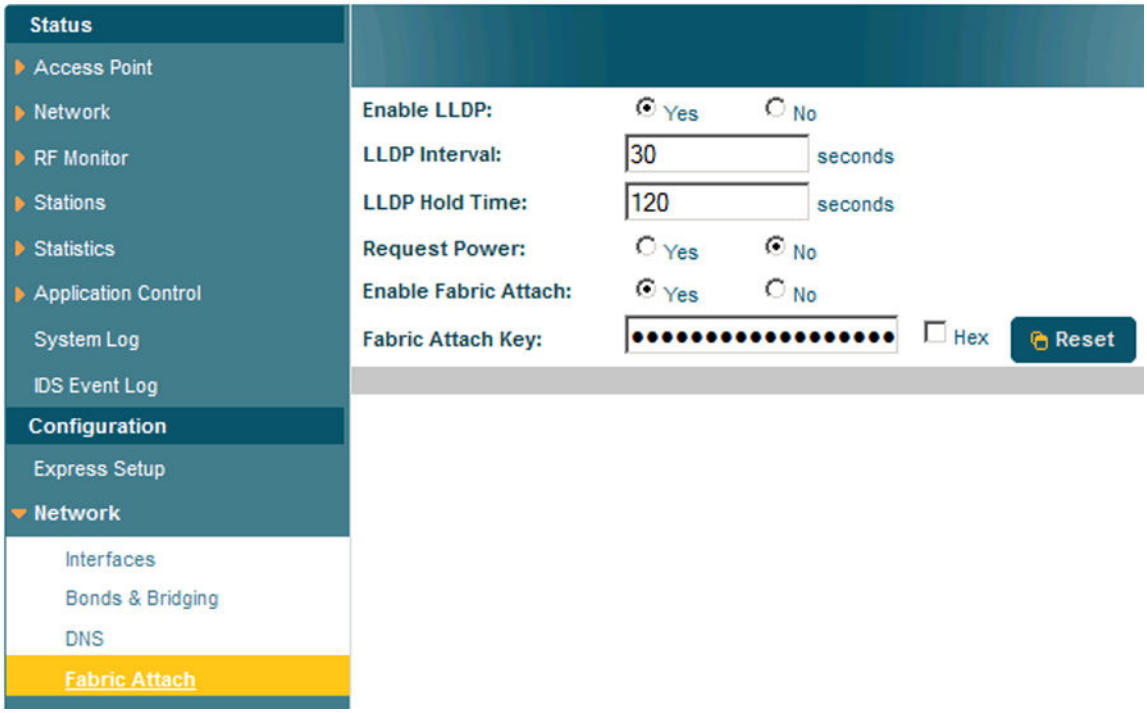
LLDP must be enabled on the WAP in order to gather and display this information.

Configuring Fabric Attach settings on AOS

About this task

The Network> Fabric Attach page controls the Avaya Fabric Attach settings and LLDP settings. Link Layer Discovery Protocol (LLDP) is a Layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly

connected network devices. WAPs can both advertise their presence by sending LLDP announcements, and gather and display information sent by neighbors.



Procedure

1. In the **Enable LLDP** field, select **Yes**.

   When LLDP is enabled, the WAP sends out LLDP announcements of the WAP's presence, and gathers LLDP data sent by neighbors. When LLDP is disabled, the WAP does neither. LLDP is enabled by default.

2. In the **LLDP Interval** field, enter a value in seconds.

   The WAP sends out LLDP announcements advertising its presence at this interval. The default is 30 seconds.

3. In the **LLDP Hold Time** field, enter a value in seconds.

   LLDP information received from neighbors is retained for this period of time before aging out of the WAP's neighbor list. If a neighbor stops sending announcements, the LLDP information no longer appears on the Fabric Attach List window after the LLDP Hold Time seconds from its last announcement. The default is 120 seconds.

4. In the **Request Power** field, select **No**. You must enable LLDP before you can enable this feature.

   For more information about this setting, see *Using the Avaya OS for Avaya WLAN AP 9100 Series*, NN47252-102.

5. In the **Enable Fabric Attach** field, select **Yes** to enable the WAP as a Fabric Attach client device.

WAPs support the Avaya Fabric Attach feature to simplify network deployment. This feature is enabled by default. Fabric Attach uses LLDP packets for communication and requires LLDP to be enabled.

6. To change the message authentication key that Fabric Attach uses, enter a new key of 1 to 32 octets in the **Fabric Attach Key** field.
7. Select **Save** to save changes.

Configuring ERS 4800 or ERS 5900 as an FA Proxy Standalone

About this task

Configure the minimum configuration on the ERS 4800 or ERS 5900:

- The ERS 4800 must be running Release 5.9 (when available).
- The ERS 5900 must be running Release 7.0 (when available).

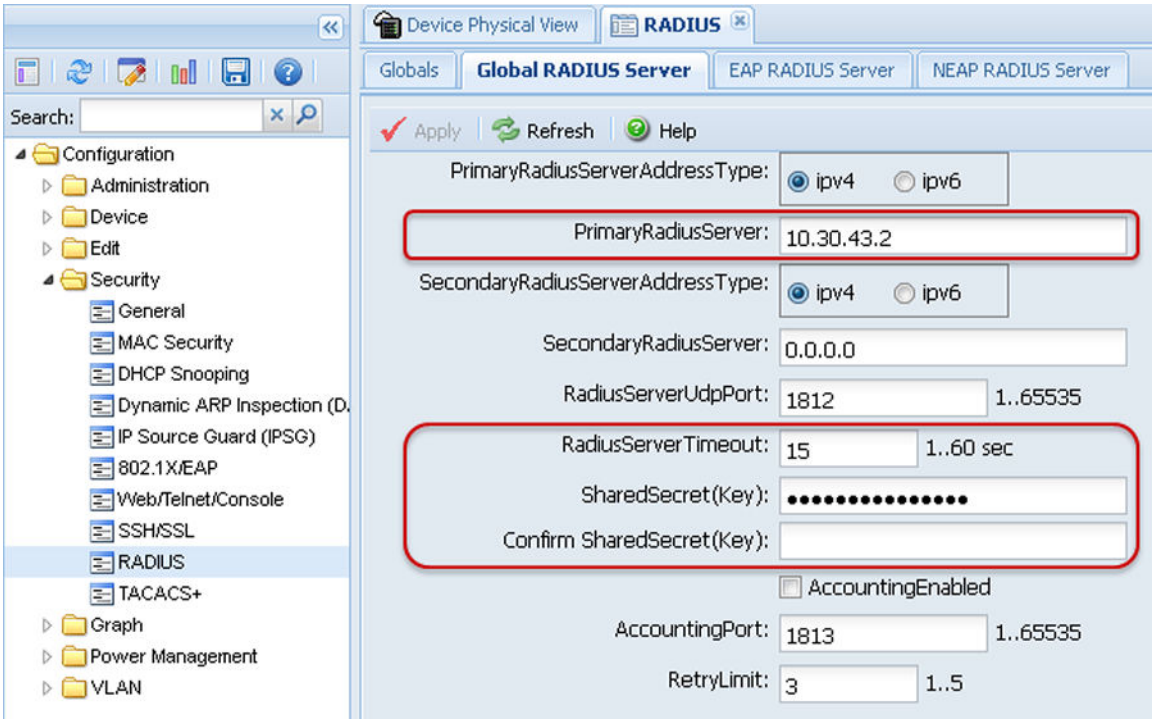
Note:

The configuration done through the GUI can also be done using CLI commands or a configuration file.

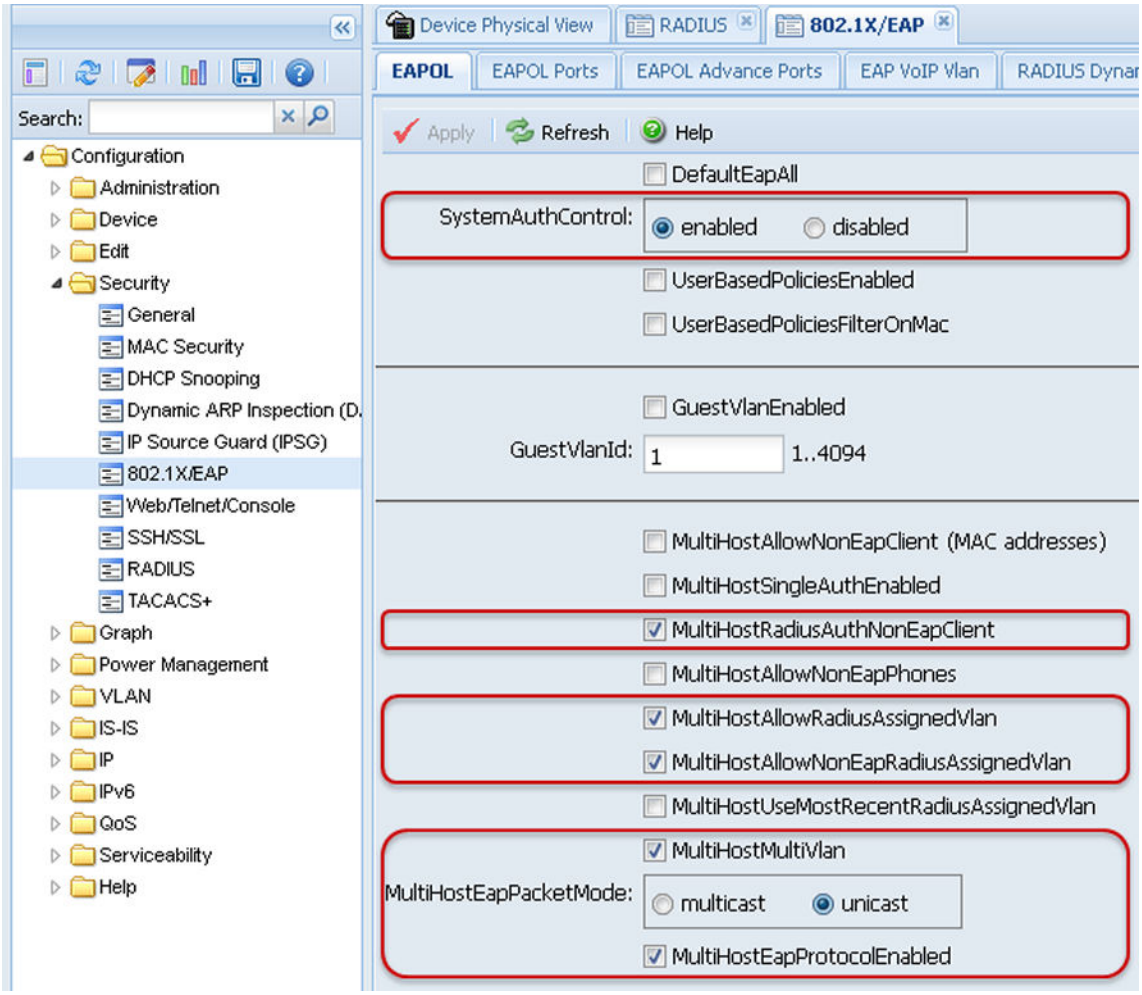
Procedure

1. Go to **Configuration** > **Administration** > **Quick Start** > **IP/Community/Vlan** and do the following:
   a. Enter the In-band Switch IP address.
   b. Enter the In-band Switch Subnet Mask.
   c. Enter the In-band Default Gateway.
   d. Apply the configuration settings.

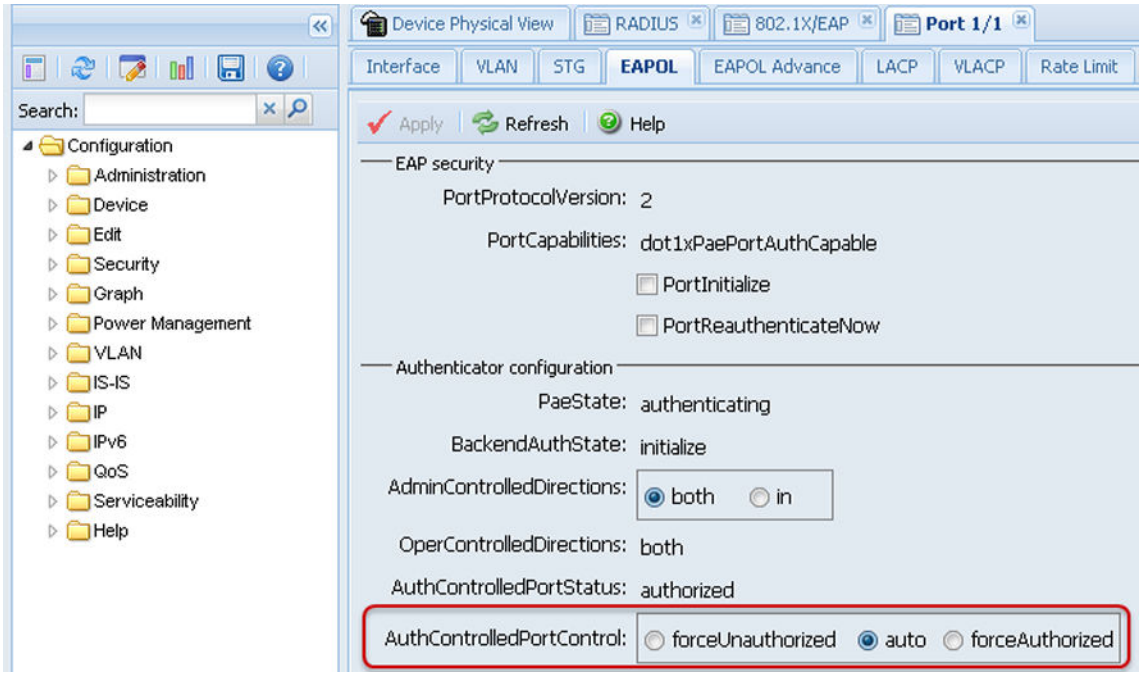
2. Go to **Configuration** > **Security** > **RADIUS** > **Global RADIUS Server** and do the following:
   a. Enter the IP address of the Primary RADIUS server.
   b. Enter **15** in the **RadiusServerTimeout** field.
   c. Enter the **SharedSecret(Key)**.
   d. Confirm the **SharedSecret(Key)**.
   e. Apply the configuration settings.



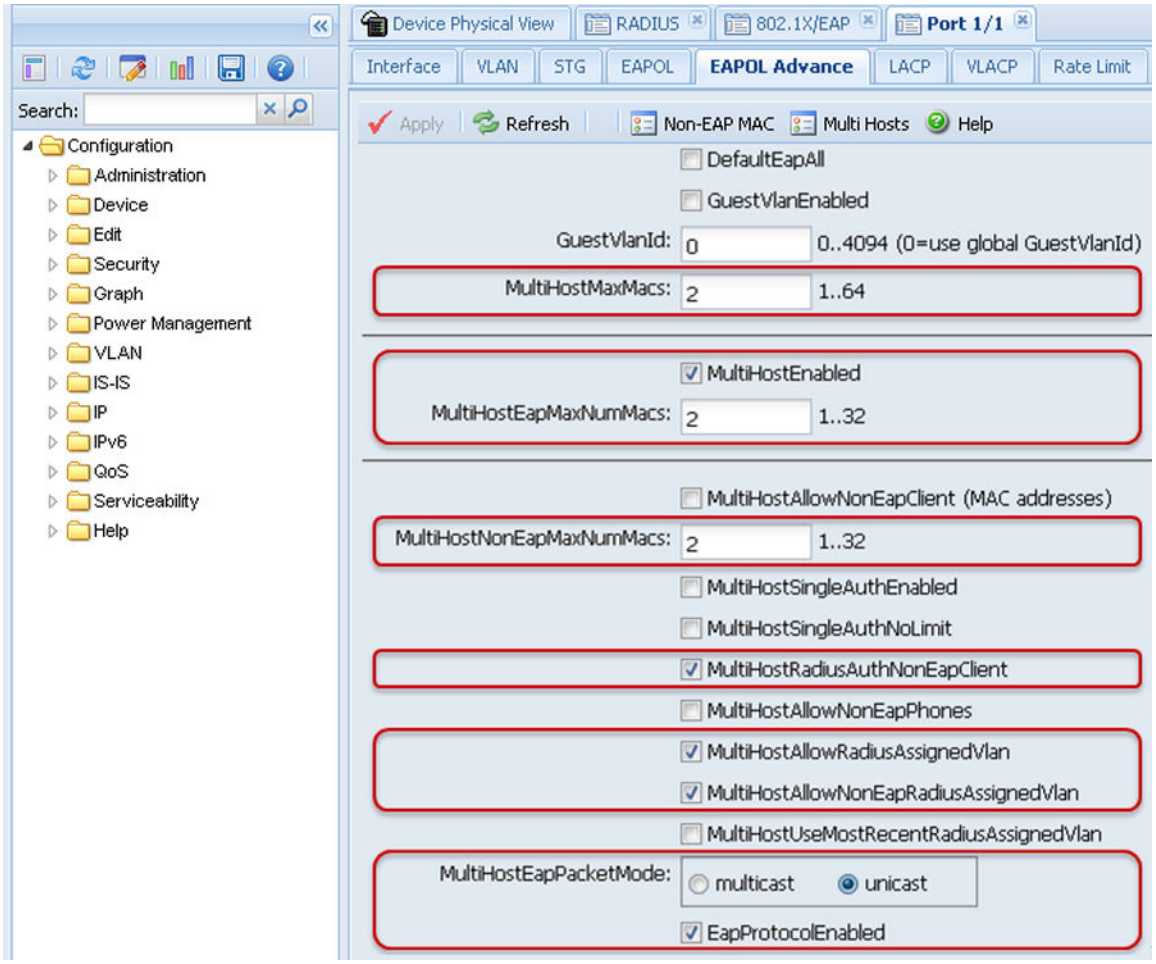
3. Go to **Configuration** > **Security** > **802.1x/EAP** > **EAPOL** and do the following:
   a. Check **MultiHostRadiusAuthNonEapClient**.
   b. Check **MultiHostAllowRadiusAssignedVlan**.
   c. Check **MultiHostAllowNonEapRadiusAssignedVlan**.
   d. Check **MultiHostMultiVlan**.
   e. Select **unicast** for the **MultiHostEapPacketMode**.
   f. Check **MultiHostEapProtocolEnabled**.
   g. Apply the configuration settings.
   h. Enable **SystemAuthControl**.
   i. Apply the configuration settings.



4. Go to **Configuration** > **Security** > **Port 1/1** > **EAPOL** and do the following:
   a. Select the desired port.
   b. Set **AuthControlIdPortControl** to **auto**.
   c. Apply the configuration settings.
   d. Configure these settings on all access ports except the port designated as the uplink port.



5. Go to **Configuration** > **Security** > **Port 1/1** > **EAPOL Advanced** and do the following:
   a. In the **MultiHostMaxMacs** field, enter **2**.
   b. Check **MultiHostEnabled**,
   c. In the **MultiHostEapMaxNumMacs** field, enter **2**.
   d. In the **MultiHostNonEapMaxNumMacs** field, enter **2**.
   e. Check **MultiHostRadiusAuthNonEapClient**.
   f. Check **MultiHostAllowRadiusAssignedVlan**.
   g. Check **MultiHostAllowNonEapRadiusAssignedVlan**.
   h. Select **unicast** for the **MultiHostEapPacketMode**.
   i. Check **EapProtocolEnabled**.
   j. Apply the configuration settings.
   k. Configure these settings on all access ports except the port designated as the uplink port.



6. Go to the CLI and enter the following commands:

   a. `fa standalone-proxy`

      This command puts the switch into FA Proxy Standalone mode.

   b. `fa uplink port XX`

      - XX is the port number of the port designated as the uplink port.
      - This command configures the switch with the port designated as the uplink port.
      - This command is necessary as there is no FA Server behind the FA Proxy Standalone switch to discover the uplink port.

   c. `fa zero-touch-option auto-port-mode-fa-client`

      - This command enables the switch to automatically configure a port to the required mode when an FA Client is discovered and is attached to the port.
      - In the case of an FA Client WALN 9100 AP, the port is automatically put into MHSA mode and the normal 32 clients port limitation is removed. This lets wireless clients

connect to the AP through the network without being authenticated by the switch as they are authenticated by the AP 9100 itself as an authenticator.

Identity Engines Ignition Server configuration

Identity Engines Ignition Server R9.1 takes the role of the FA Policy Server. The Identity Engines components required for FA Policy are the following:

- Ignition Server
- Ignition Dashboard

All other Identity Engines components such as the Ignition Guest Manager and Ignition Access Portal are optional and not required for Fabric Attach. These components may be required for other workflows depending on customer requirements.

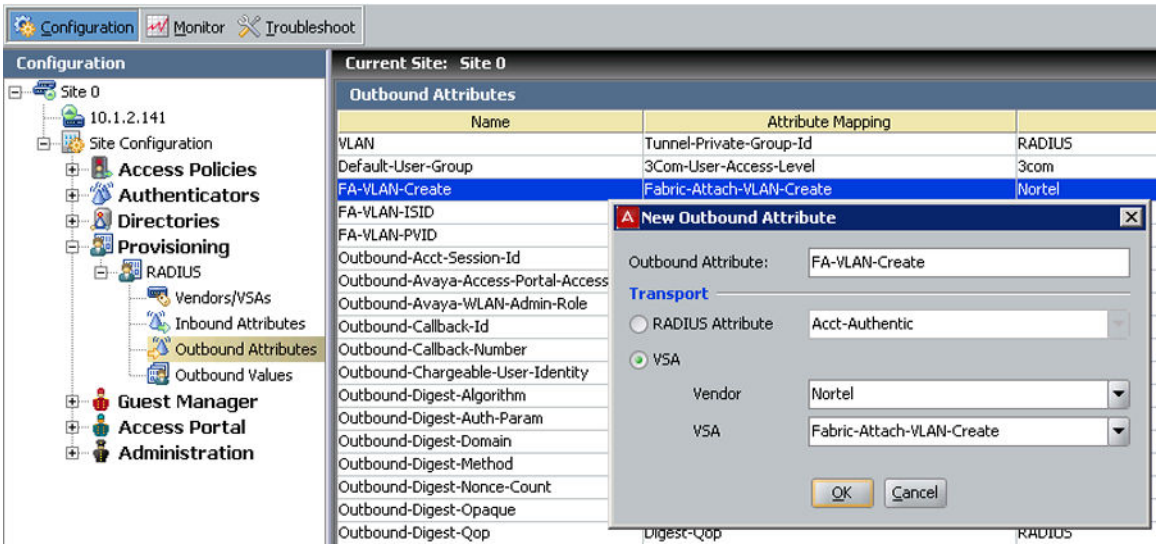
In the following use case example, the WLAN 9100 AP is configured with SSID for Engineering and SSID for Guests. Each SSID is associated with a WLAN 9100 Group with a VLAN as follows:

- VLAN for Engineering traffic = 200
- VLAN for Guest traffic = 400

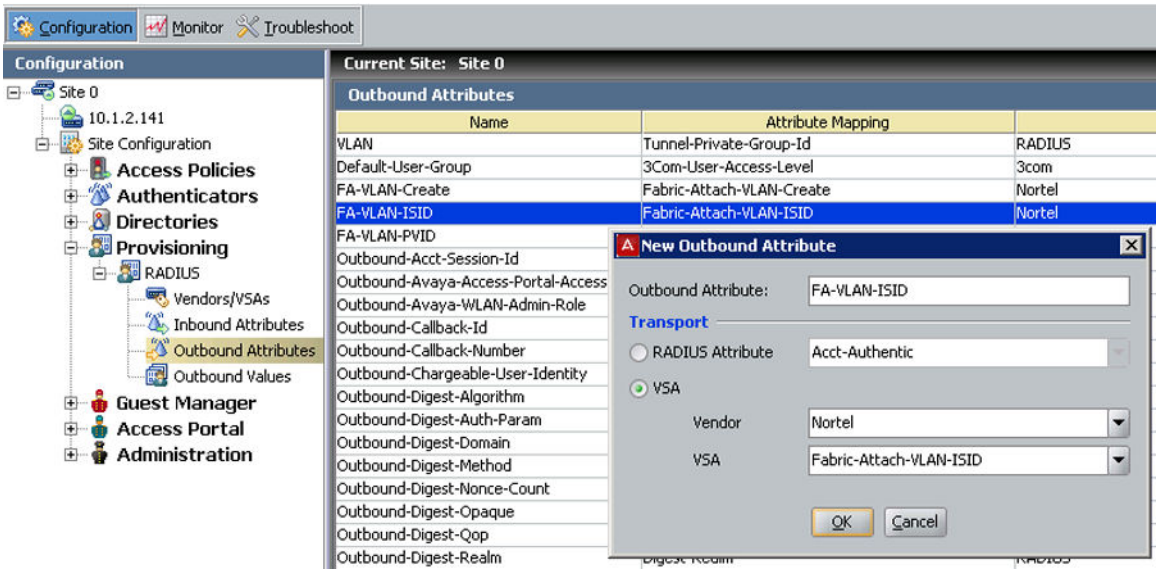
Configuring Fabric Attach outbound attributes

Procedure

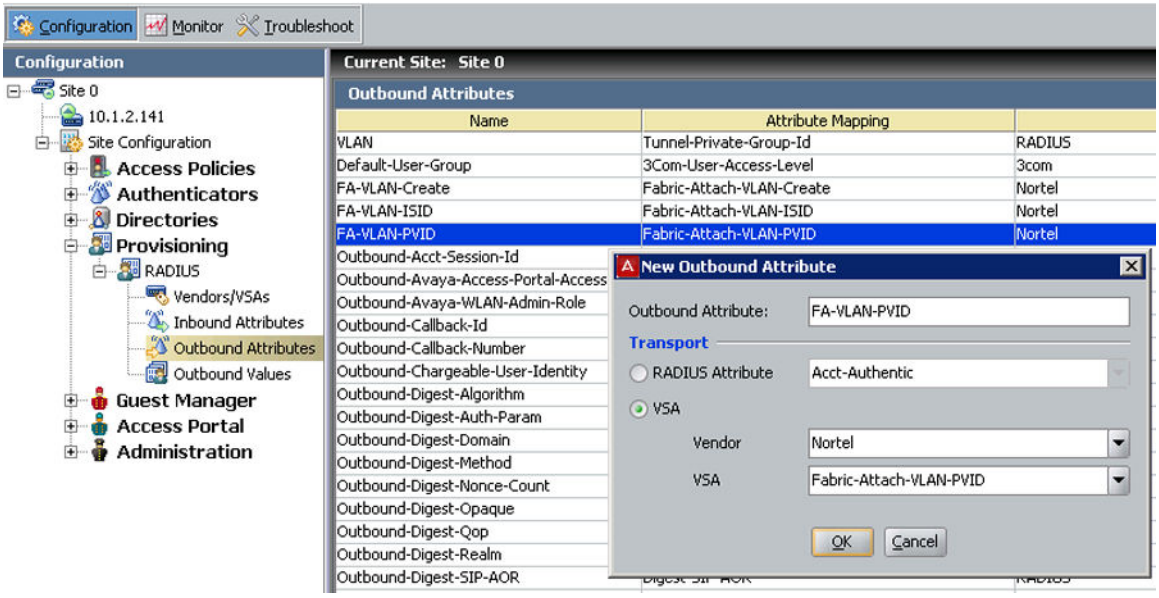
1. On the Ignition Dashboard Configuration tab, select **Provisioning** > **Radius** > **Outbound Attributes.**
2. Add the outbound attribute FA-VLAN-Create based on FA VSA Fabric-Attach-VLAN-Create.



3. Add the outbound attribute FA-VLAN-ISID based on FA VSA Fabric-Attach-VLAN-ISID.



4. Add the outbound attribute FA-VLAN-PVID based on FA VSA Fabric-Attach-VLAN-PVID.

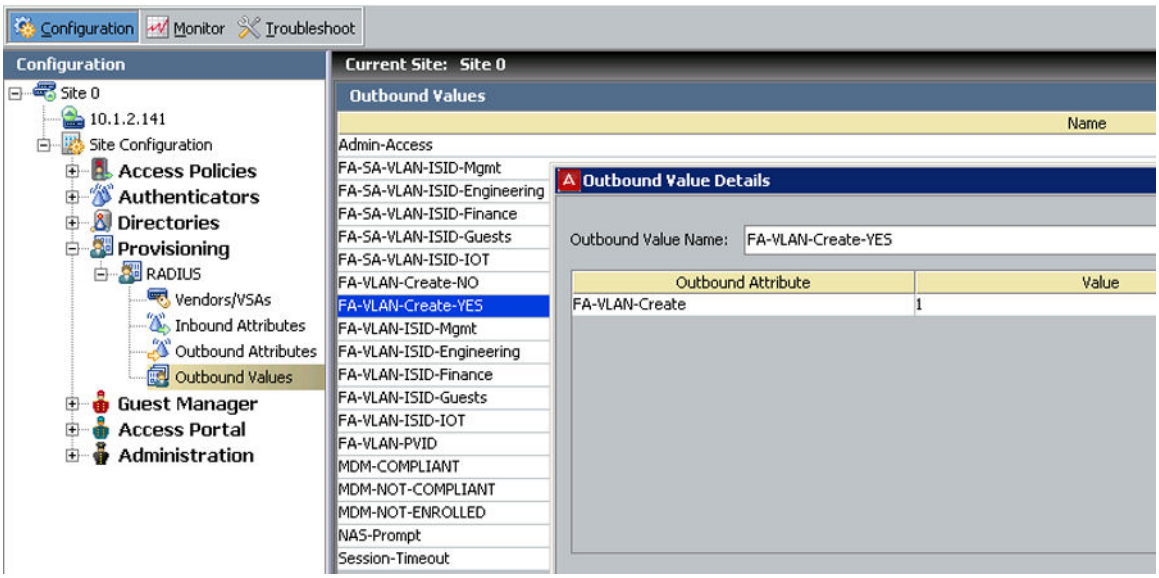


Configuring Fabric Attach outbound values

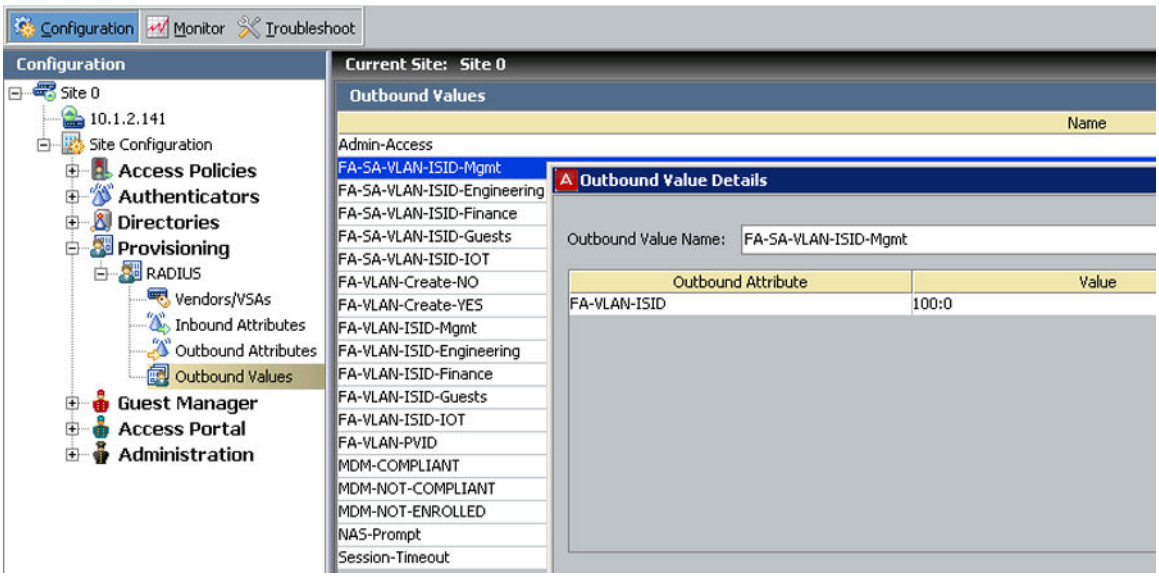
Procedure

1. On the Ignition Dashboard Configuration tab, select **Provisioning** > **Radius** > **Outbound Values.**

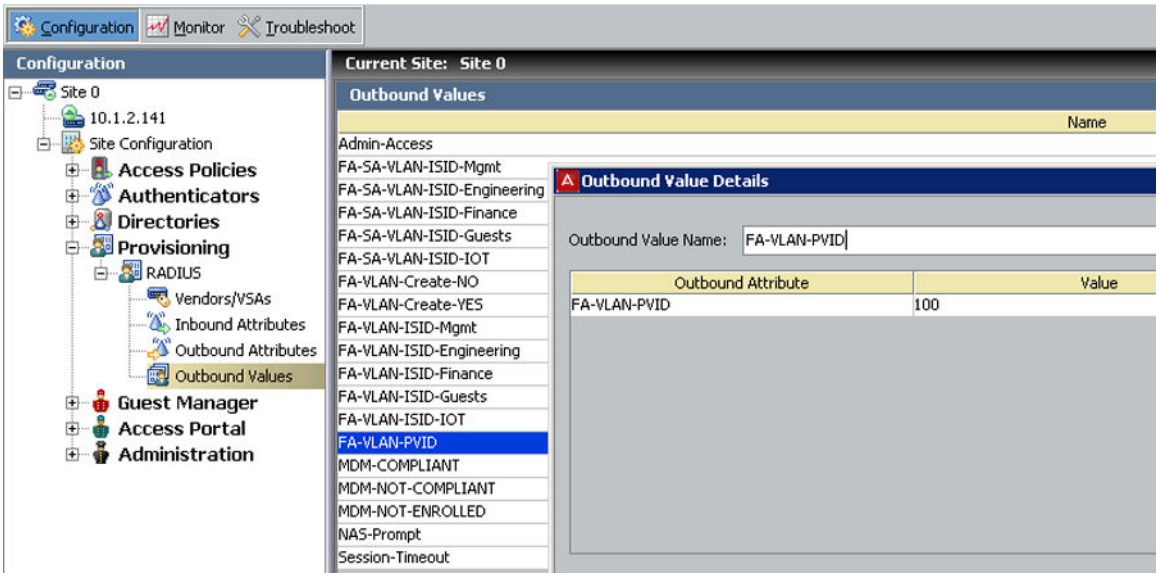
2. Add the outbound value FA-VLAN-Create-YES based on the attribute FA-VLAN-Create equals 1.



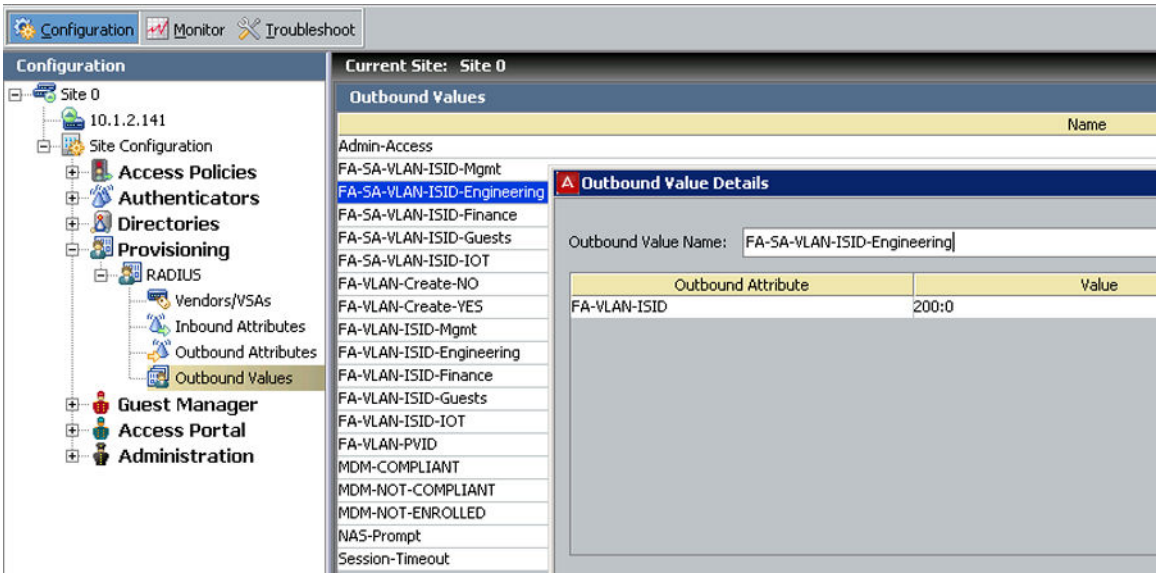
3. Add the outbound value FA-VLAN-ISID-Mgmt based on the attribute FA-VLAN-ISID equals 100:0.



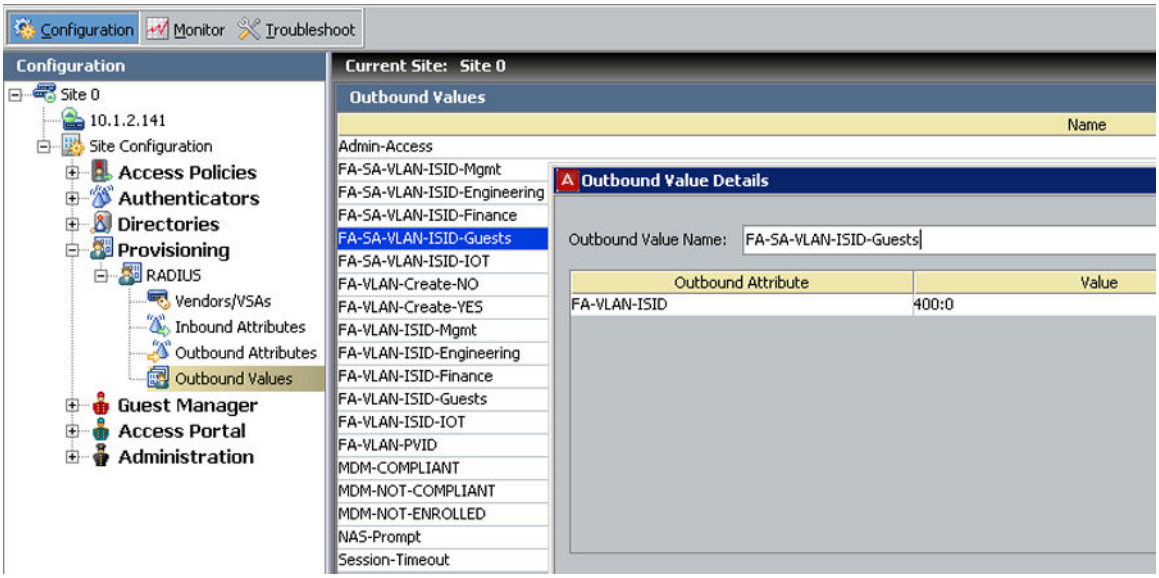
4. Add the outbound value FA-VLAN-PVID based on the attribute FA-VLAN-PVID equals 100.



5. Add the outbound value FA-VLAN-ISID-Engineering based on the attribute FA-VLAN-ISID equals 200:0.



6. Add the outbound value FA-VLAN-ISID-Guest based on the attribute FA-VLAN-ISID equals 400:0.



Access policies for WLAN 9100 as an FA Client

The following sections describe three example use cases of access policies to attach WLAN FA clients to the network.

For more information and procedures on how to configure access policies, see *Administering Avaya Identity Engines Ignition Server*, NN42780–600.

Simple rule: FA-Client-AP9100–Simple

To configure a simple rule to authenticate and provide service authorization for an FA Client WLAN 9100 AP, the AP 9100 MAC address must be onboarded onto the Ignition Server local store in the group “FA Client AP9100 Group”.

The simplest and fastest method to onboard a device onto the Ignition Server local store is to connect the WLAN 9100 AP to a switch and have it fail authentication. On the Access Logs on the Ignition Dashboard, right-click and select **Add MAC to Internal Devices**. The MAC address automatically populates. You can now edit the device details and associate the device with the “FA Client AP9100 Group”.

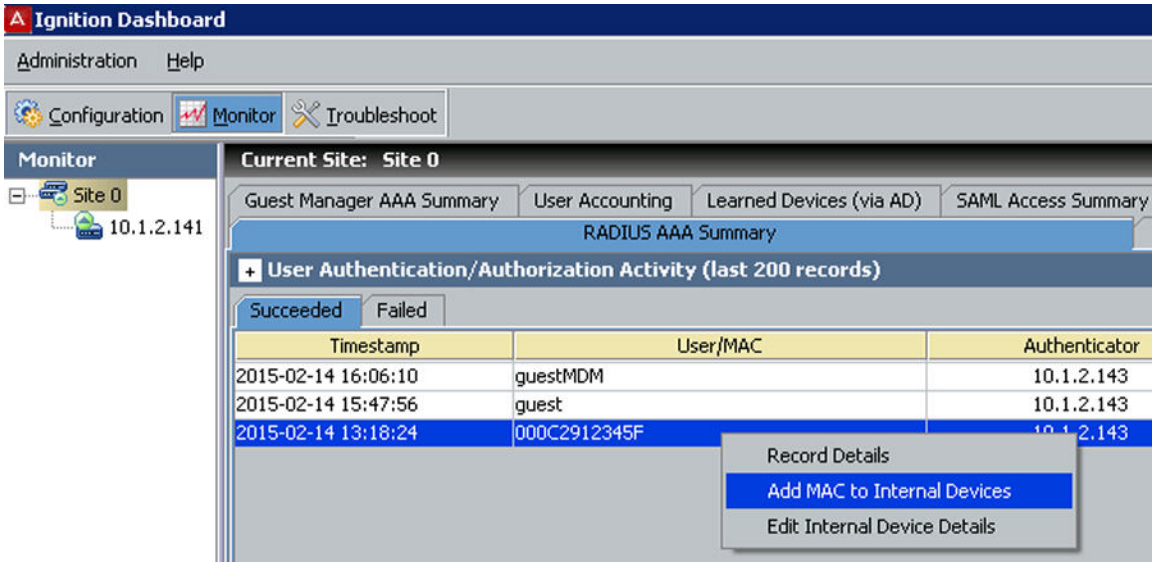


Figure 6: Right-click to onboard AP 9100 MAC address

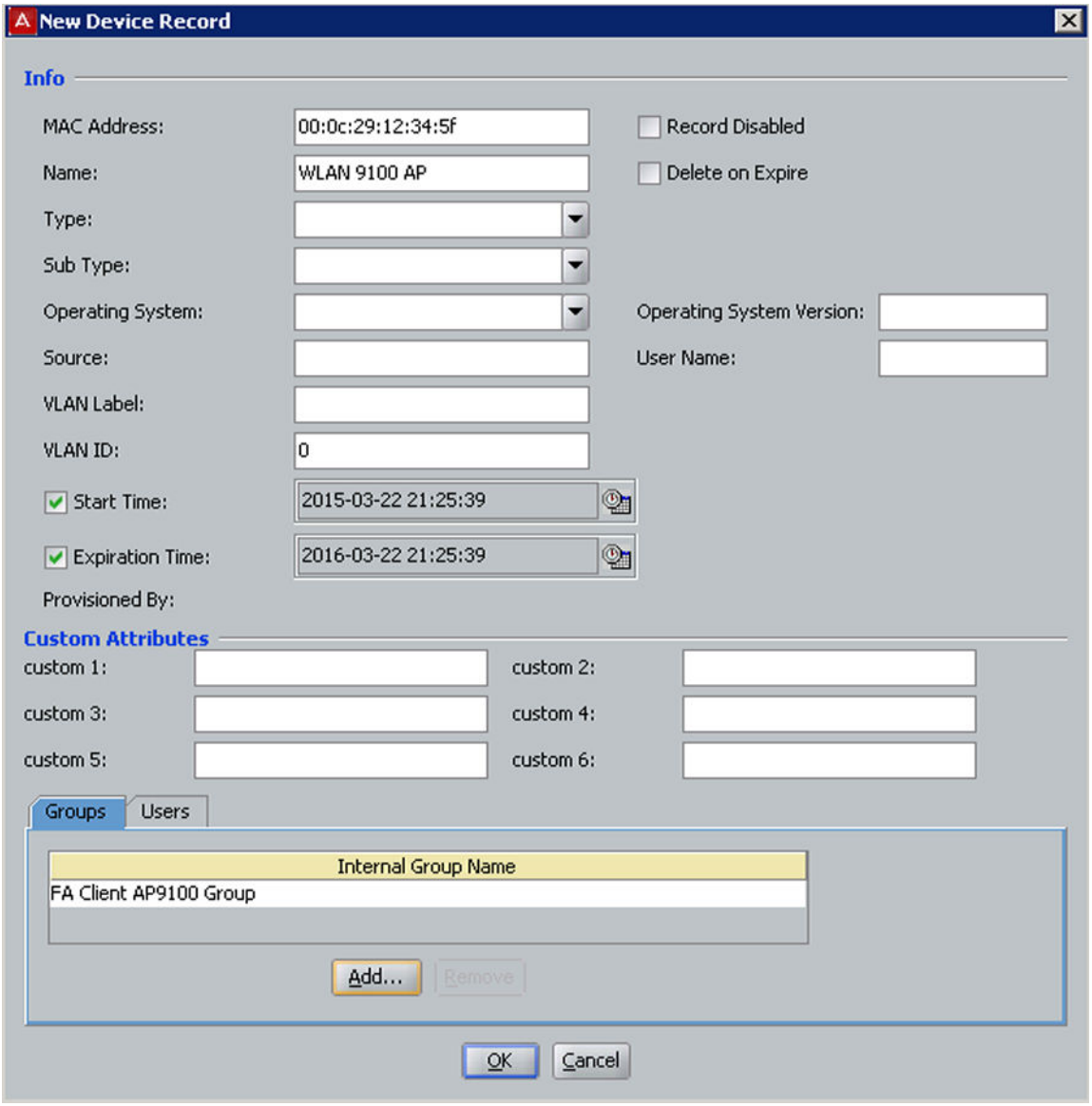
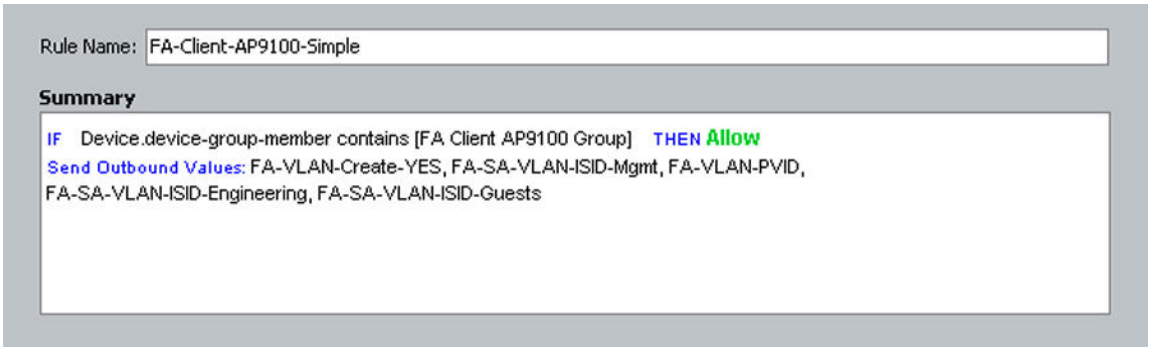


Figure 7: Associate the device with the FA Client AP9100 Group

Simple access policy

Configure the Simple access policy rule to do the following:

- Check if the device belongs to the WLAN 9100 AP group.
- If the device belongs, have Ignition Server sends the switch a collection of outbound values that instruct the switch to do the following:
  - Create VLANs if they do not exist.
  - Provide the management VLAN and PVID, and the Engineering and Guests VLANs so that the traffic sent by the Access Point will appropriately ingress the network.



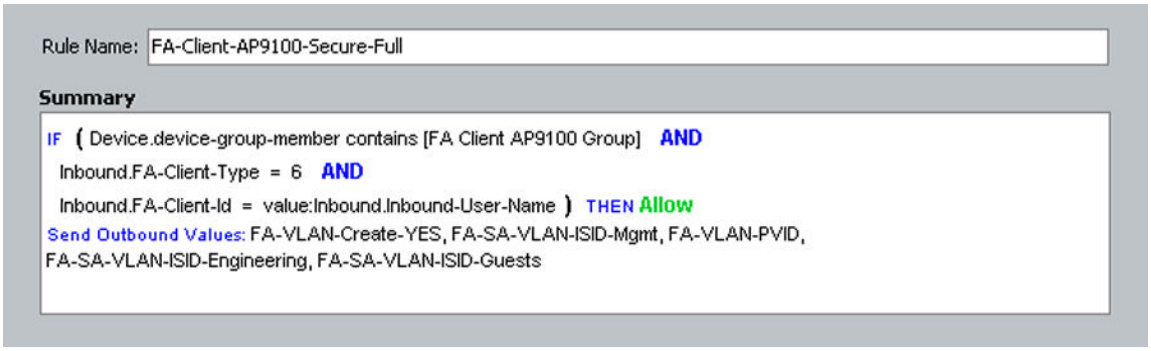
Secure rule: FA-Client-AP9100–Secure-Full

This is a rule for secure MAC authentication taking advantage of FA Signaling and the information communicated between the FA Proxy Standalone switch and the FA Client.

The WLAN 9100 AP as FA Client communicates (by way of FA Signaling) its device type as “FA Client Wireless AP Type 1” which has value of 6.

In addition, the WLAN 9100 AP as FA Client communicates (by way of FA Signaling) its MAC address to the FA Proxy Standalone switch. This MAC address is compared by the Access Policy to the MAC address seen on the wire by the FA Proxy Standalone switch and sent by way of standard attribute Calling-Station-Id.

All three conditions of the Access Rule (that is, device in “FA Client AP9100 Group”, FA Client device communicates its type as 6, and FA Client device communicates its Id that must match the device MAC address seen on the wire) have to be met before the Ignition server will allow the attachment of the AP9100 to the network and will send a collection of Outbound values that instruct the switch to create VLANs if they do not exist, provide the management VLAN and PVID, and the Engineering and Guests VLANs so that the traffic sent by the Access Point will appropriately ingress the network.



Secure rule without device onboarding: FA-Client-AP9100–Secure-noDB

This is a rule for secure MAC authentication taking advantage of FA Signaling and the information communicated between the FA Proxy Standalone switch and the FA Client without the need to pre-onboard the FA Client device onto the Ignition Server local store.

Make sure your that the Ignition Server is loaded with the Everything.csv device wild cards. This file contains 256 wild card entries that cover all possible MAC addresses. The Everything.csv file is available on the Identity Engines support download site.

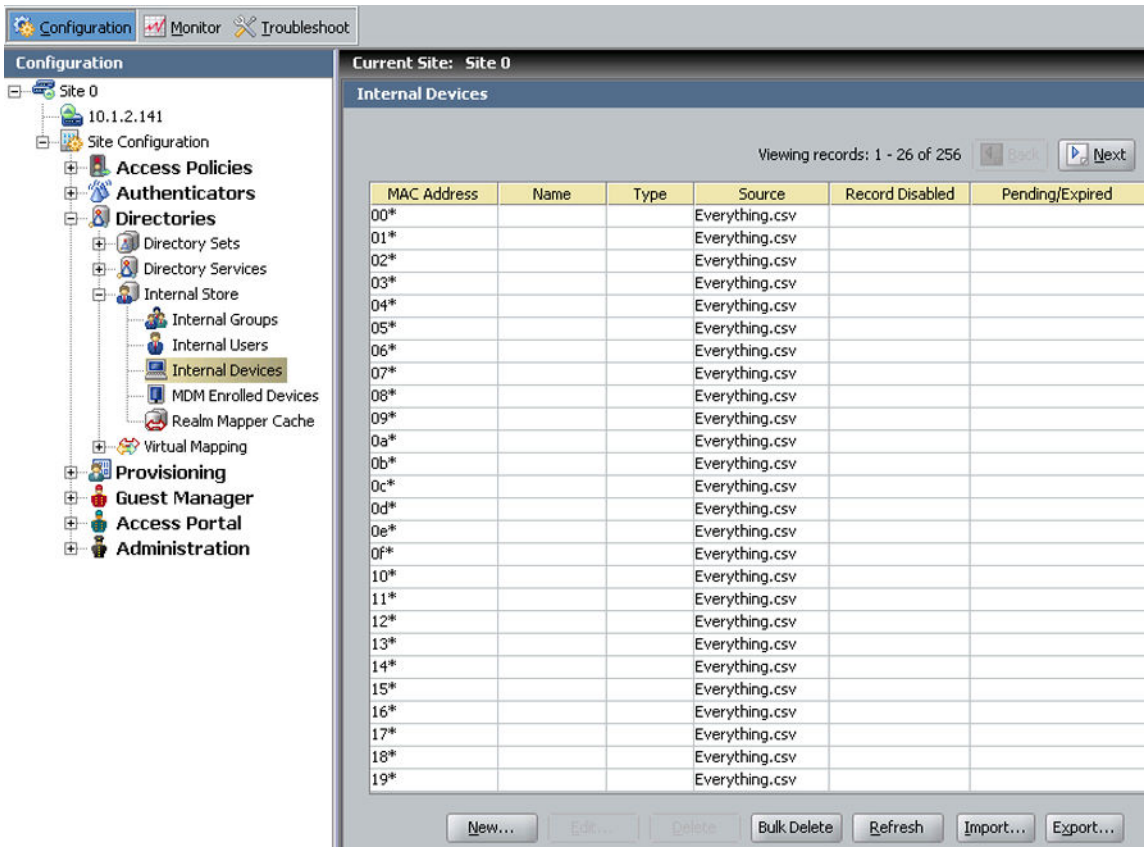
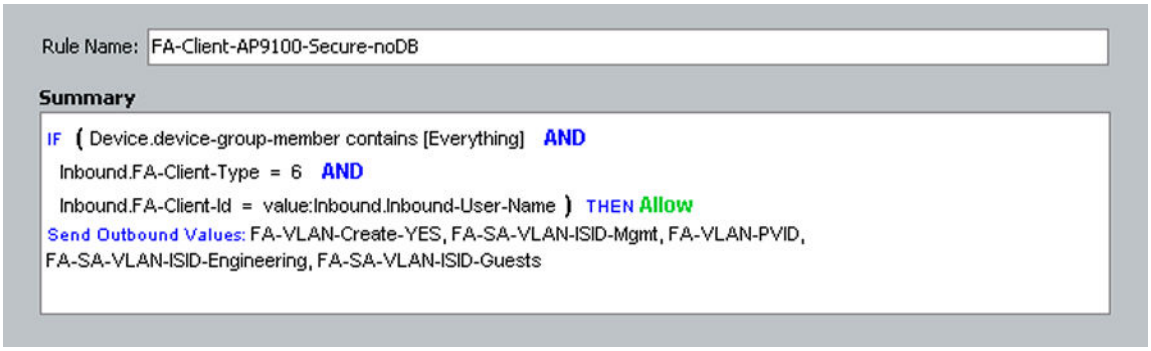


Figure 8: Everything.csv device wild cards

The Access Rule can now validate the FA Client device against the Everything group which always tests positive.

The Access Rule conditions (that is, the FA Client device communicates its type as 6, and the FA Client device communicates its Id that must match the device MAC address seen on the wire) must be met before the Ignition server sends a collection of Outbound values that instructs the switch to create VLANs if they do not exist, provide the management VLAN and PVID, and the Engineering and Guests VLANs so that the traffic sent by the Access Point will appropriately ingress the network.



Viewing an access record for a FA Client WLAN 9100 AP network attachment

Procedure

1. On the Ignition Dashboard, go to the **Monitor** tab.
2. Select the **RADIUS AAA Summary** tab.

3. Double-click on the access record to see the details of the FA Client access information.