Avaya Identity Engines Integration with WLAN 9100 Series

Release 9.0.1 and WLAN 9100 7.0
NN47280-503
Issue 01.01
June 2014

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 Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, 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 Customer 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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 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.

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.

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.

Contents

Chapter 1: New in this release

Avaya Identity Engines Integration with WLAN 9100 Series, NN47280–503 is a new document created to support the following product releases:

- Avaya Identity Engines Release 9.0.1
- Avaya Identity Engines Release 8.0.2
- Avaya WLAN 9100 Series Release 7.0

Chapter 2: Introduction

Avaya Identity Engines Integration, NN47280–503 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 (switch, wireless access point, or VPN gateway) that allows users and devices to connect to your network. The Identity Engines Ignition Server manages access control and provisioning for wireless access points (WAP) when the WAPs are configured as authenticators in Ignition Server.

This guide 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.

Related Links

[What is Avaya Identity Engines Ignition Server?](#) on page 6
[What are Avaya WLAN 9100 Series Wireless Access Points?](#) on page 8
[Resources](#) on page 8

What is Avaya Identity Engines Ignition Server?

Avaya Identity Engines Ignition Server is an 802.1X-capable RADIUS authentication server and TACACS+ server that grants or denies users access to your network based on your policies. Use the Ignition Server to create a single set of policies that control access for all the ways users connect: through wired, wireless, or VPN. Ignition Server stores access policies, and user accounts remain in your traditional user store(s), such as such as Microsoft Active Directory, Open LDAP, Novell eDirectory, RSA Authentciation 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 and ensuring it has up-to-date antivirus profiles installed).

Ignition Server abilities to check whether the user's workstation has passed MAC authentication, Windows machine authentication, and/or a security posture check 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 the 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.

Related Links

Introduction on page 6
Key characteristics of Ignition Server on page 7

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.

Related Links

What is Avaya Identity Engines Ignition Server? on page 6

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.

Related Links

Introduction on page 6

Resources

Related Links

Introduction on page 6
Training on page 9
Avaya Mentor videos on page 9
Support on page 9

Training

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

Related Links

Resources on page 8

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, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://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 site.

    Note:

    Videos are not available for all products.

Related Links

Resources on page 8

Support

Visit 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.

Related Links

Resources on page 8

Chapter 3: Licensing

The Identity Engines Ignition Server has three types of base licenses.

Base license type	Number of supported authenticators
LITE	5
SMALL	20
LARGE	Unrestricted

Identity Engines provides special treatment to the Avaya WLAN 9100 from a licensing perspective. Fifteen WLAN 9100 APs are considered 1 standard authenticator.

The Identity Engines licensing support for WLAN 9100 is delivered in two phases:

- Long term solution
- Intermediate term solution

Long Term Solution

The long term solution will be delivered through an upcoming future release of Identity Engines that will incorporate out of the box licensing, device template and RADIUS attribute support for the WLAN 9100.

- Out-of-the-box support WLAN 9100
- Pre-configured Identity Engines with Avaya WLAN as a new vendor with supported VSAs by the WAP 9100
- Pre-configured Identity Engines with WLAN 9100 Device Template
- Pre-configured Identity Engines with Outbound Attributes supported by the WAP 9100
- Identity Engines built-in logic for considering 15 x WAP 9100 APs = 1 x Standard Authenticator

Intermediate Term Solution

The intermediate term solution is based on the following process:

- Customer purchase Identity Engines based on 15 x WAP 9100 APs = 1 x IDE Authenticator
- Customer or partner should continue to follow the standard process of requesting licenses for Identity Engines by sending an email to datalicensing@avaya.com. The E-mail request must note that the deployment includes Avaya WLAN 9100 APs so that the appropriate licenses will be provided
- Customer or partner will be provided with temporary long term Identity Engines licenses that will accommodate the number of Avaya WLAN 9100 APs being deployed

- When the release of Identity Engines which incorporates the built-in licensing logic is available, the temporary licenses will be replaced with appropriate permanent licenses
- Questions or concerns should be directed to datalicensing@avaya.com

Chapter 4: 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 RADIUS Server.

The following configuration must be performed on the Ignition Server:

- Configure a Vendor Type. See Configuring Vendor Type on page 13.
- Configure a Device Template. See Configuring the Device Template on page 16.
- Configuring the Outbound Values. See Configuring the Outbound Values on page 17.
- Add the APs to Ignition Server as Authenticators. See Adding APs to Ignition Server as Authenticators on page 19.

Related Links

Configuring Vendor Avaya WLAN on page 13
Configuring the Device Template on page 16
Configuring the Outbound Values on page 17
Adding the APs to Ignition Server as Authenticators on page 19
Configuring APs as Authenticators in bulk on page 21

Configuring Vendor Avaya WLAN

About this task

Configure the WLAN 9100 Series Vendor Type in Ignition Server.

Note:

This procedure only needs to be performed once for the WLAN 9100 Series APs.

Procedure

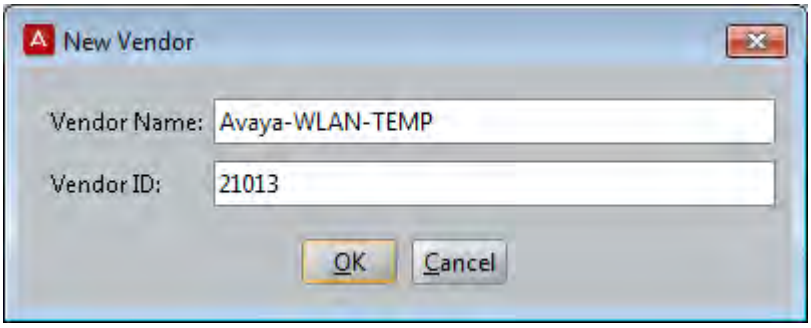
1. In the Ignition Server navigation pane, expand **Site Configuration**, expand **Provisioning**, and click **Vendors/VSAs**.

   The **Vendors** window displays.

2. At the top of the Vendors list, click **Actions**, and select **New Vendor** from the drop-down list.

   The **New Vendor** window displays.

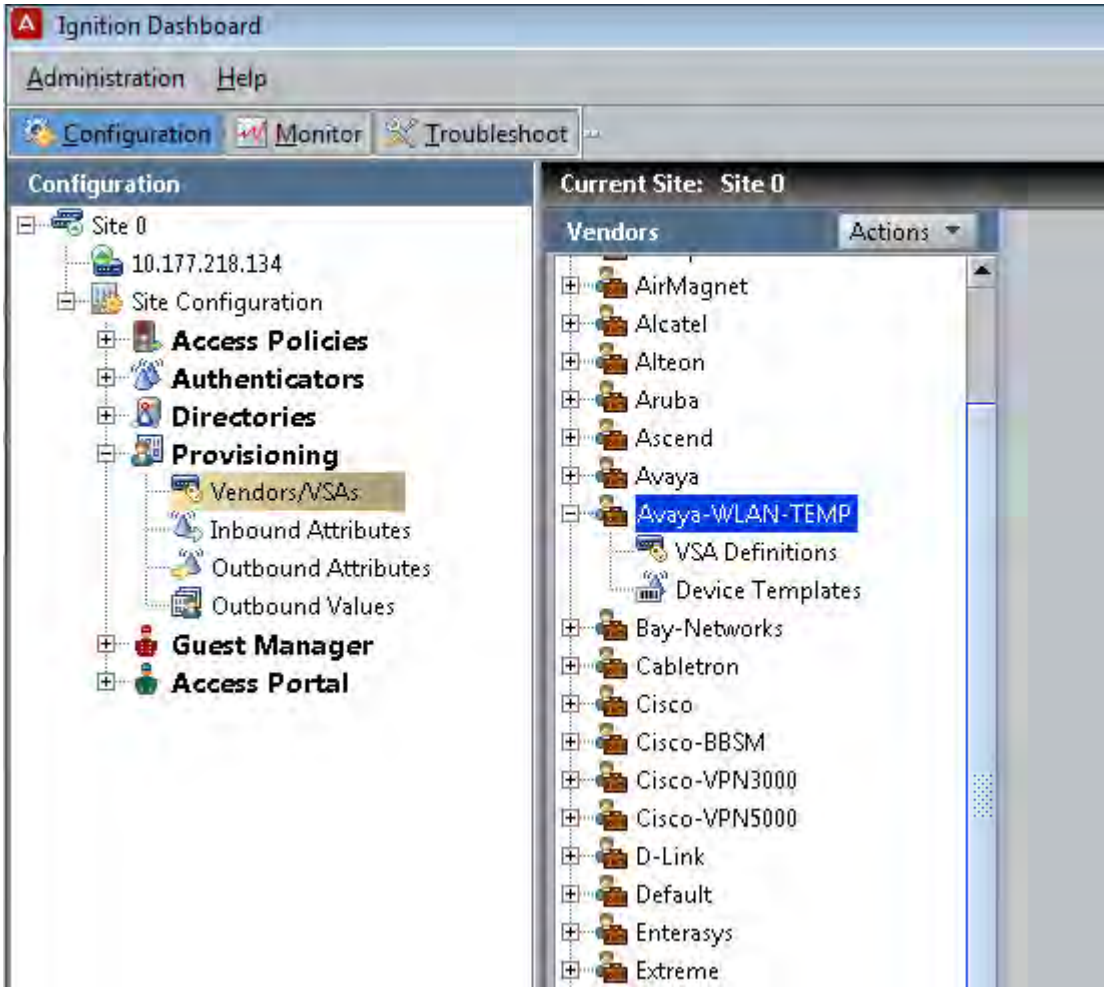
3. In the **Vendor Name** field, type the name `Avaya-WLAN-TEMP`.
4. In the **Vendor ID** field, type `21013`.



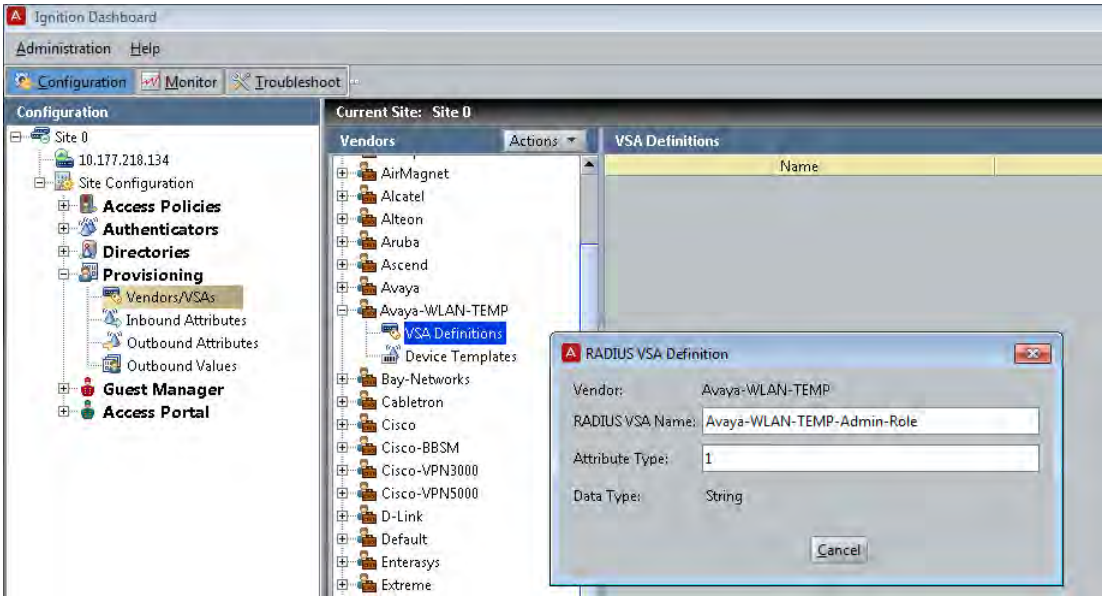
5. Click **OK**.

   The Vendor Type **Avaya-WLAN-TEMP** is created and added to the Vendors list.

6. In the Vendors window, expand **Avaya-WLAN-TEMP** and click **VSA Definitions**.

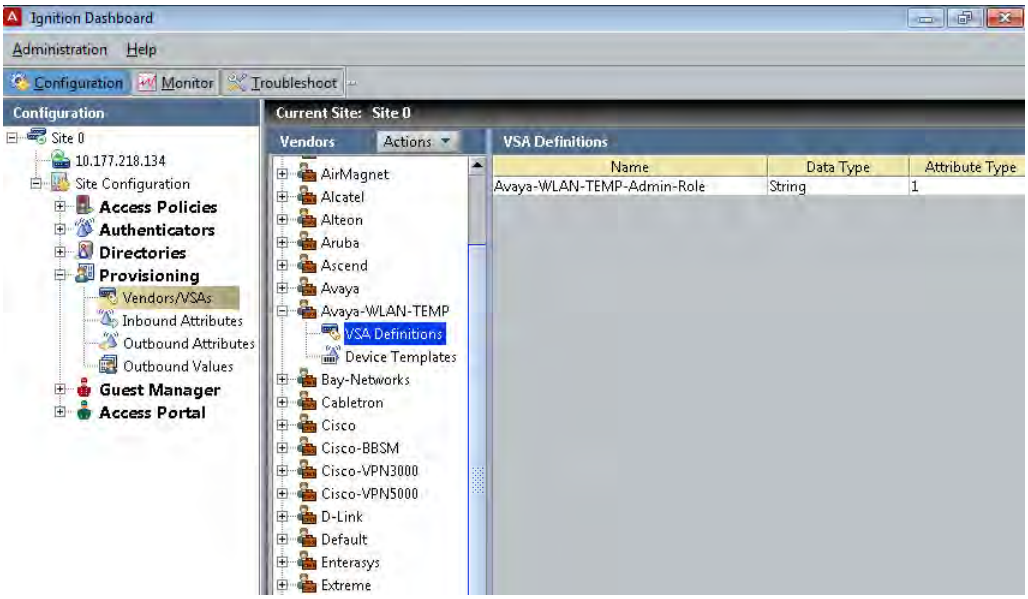


The **VSA Definitions** window displays.



7. Click New..... .

   The **RADIUS VSA Definition** window displays.



8. In the **RADIUS VSA Name** field, type `Avaya-WLAN-TEMP-Admin-Role`.
9. In the **Attribute Type** field, type `1`.
10. From the **Data Type** drop-down list, select **string**.
11. Click **OK**.

Related Links

Ignition Server configuration for WLAN 9100 Series APs on page 13

Configuring the Device Template

About this task

Configure the Device Template for the WLAN 9100 Series AP Vendor Type.

Note:

This procedure only needs to be performed once for the WLAN 9100 Series APs.

Procedure

1. In the **Vendors** window, expand **Avaya-WLAN-TEMP** and click **Device Templates**.

   The **Device Templates** window displays.

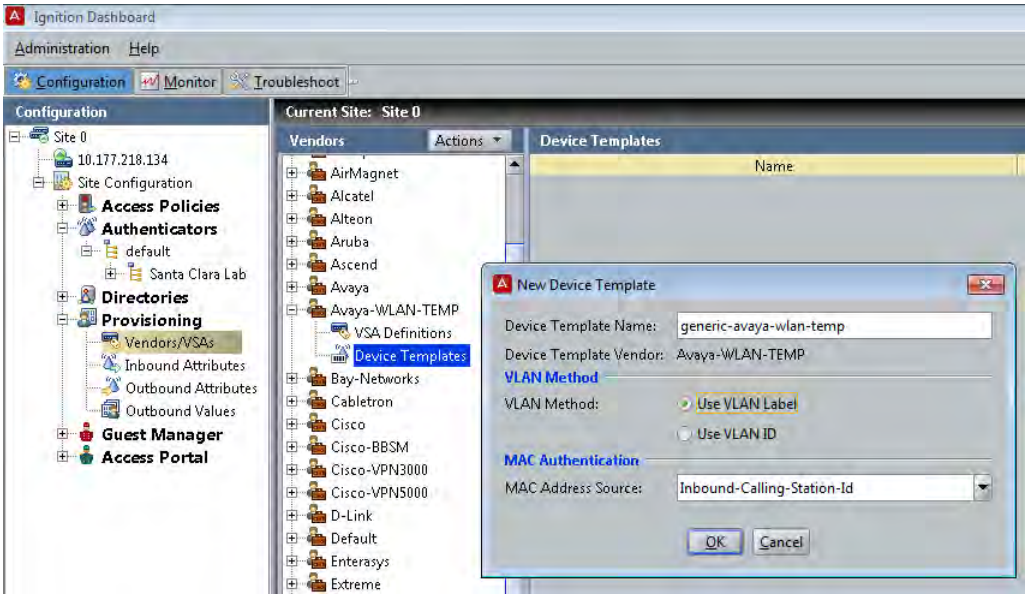
2. Click **New.....**.

   The **New Device Template** window displays.

3. In the **Device Template Name** field, type `generic-avaya-wlan-temp`.

4. Under **VLAN Method**, select **Use VLAN ID**.

5. In the **MAC Address Source** drop-down list, select **Inbound-Calling-Station-Id**.



6. Click **OK.**

   The **Edit Device Template** window displays.

7. Click **Done**.

Related Links

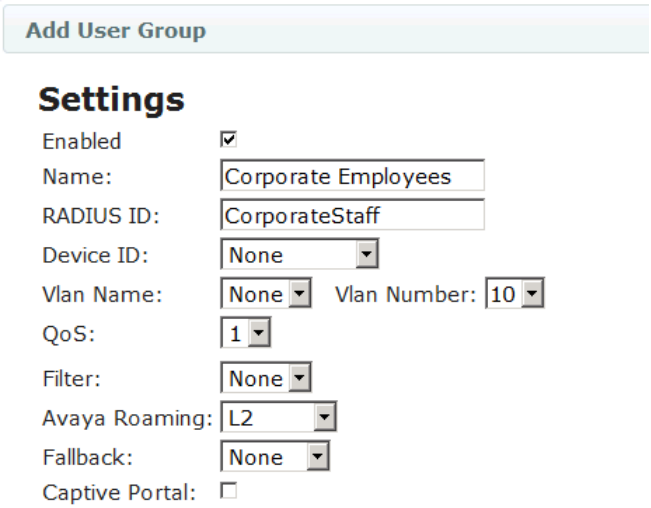
Ignition Server configuration for WLAN 9100 Series APs on page 13

Configuring the Outbound Values

In this section three examples are given which illustrate how to configure the Outbound Values for Avaya WLAN 9100.

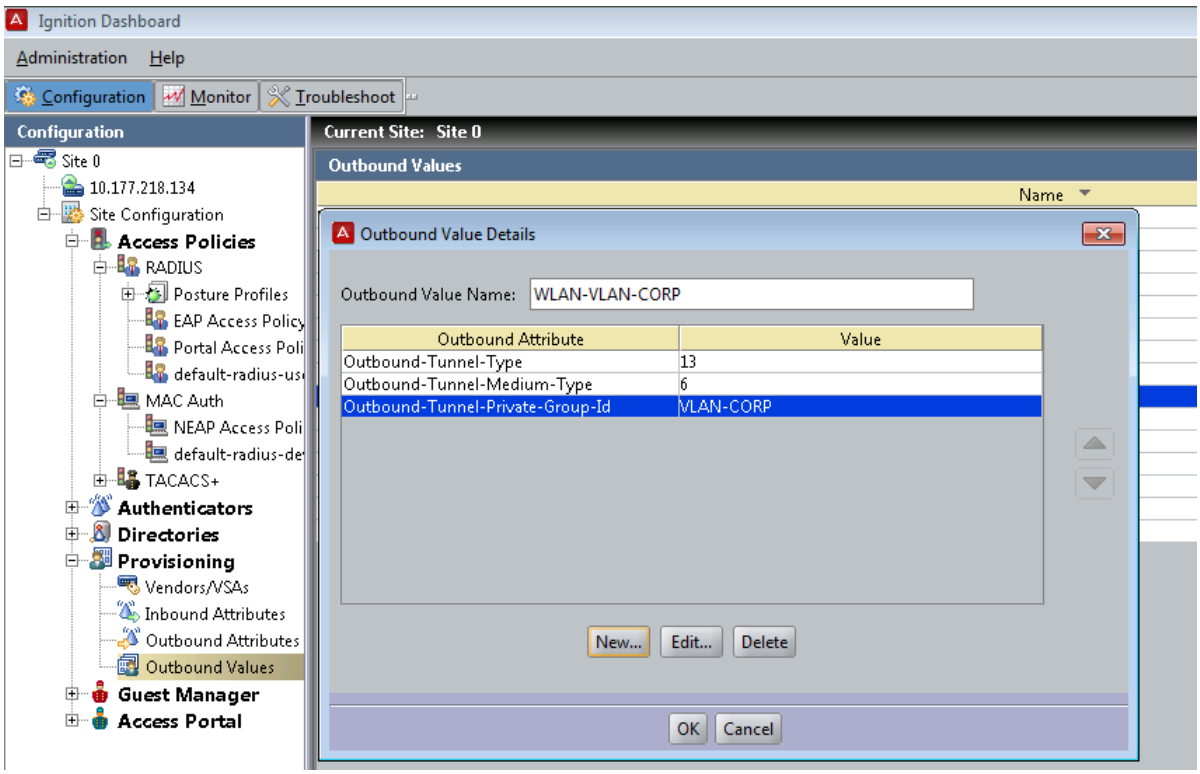
Outbound Value 1

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 match exactly the string entered in the WAP 9100 field RADIUS ID for a Group in a Profile.



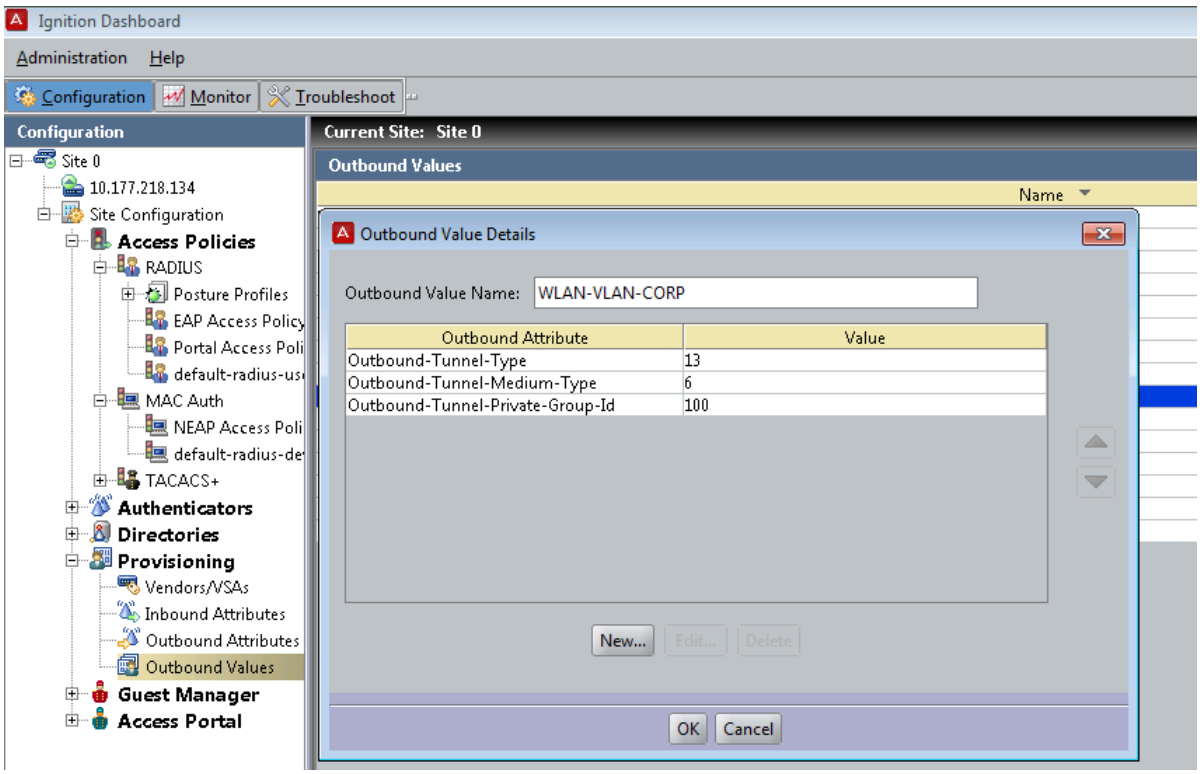
Outbound Value 2

Outbound Value that instructs the WAP9100 to assign the user that is being authenticated to a specific WLAN 9100 VLAN Label (aka VLAN Name)



Outbound Value 3

Outbound Value that instructs the WAP9100 to assign the user that is being authenticated to a specific WLAN 9100 VLAN ID (aka VLAN Number)



Related Links

Ignition Server configuration for WLAN 9100 Series APs on page 13

Adding the APs to Ignition Server as Authenticators

Before you begin

Obtain the following information:

- Container name (if required)
- IP addresses of the APs
- RADIUS Shared Secret password

About this task

The WLAN 9100 Series Access Points (APs) must point to Identity Engines as the RADIUS Server. Follow this procedure to add APs to Identity Engines Ignition Server as Authenticators.

Follow this procedure to create an AP Container (if not already created) and add an AP to the Container.

Procedure

1. In Ignition Server's navigation pane, expand **Site Configuration > Authenticators > default > your_network_name**.
2. Check to see if a Container has been created for the APs.

If there is no Container, you must create one.

- In the navigation pane, right-click **default** and click **Add Container**.

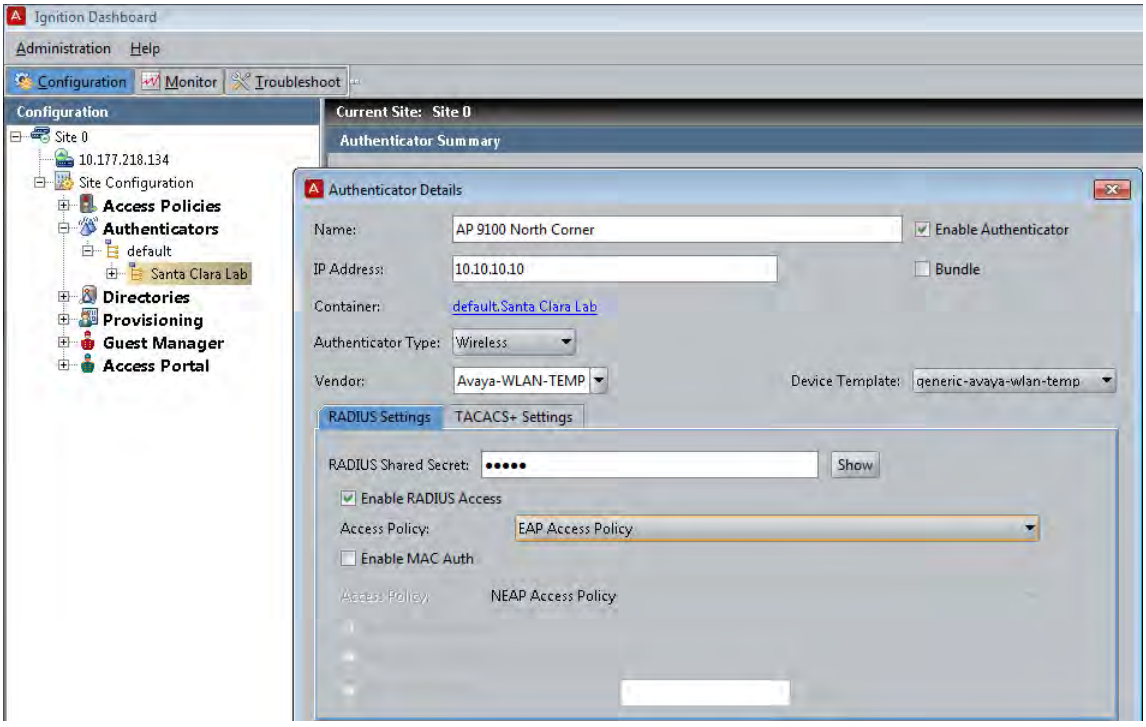
  The **Add Container** window displays.

- Enter the Container name (for example, Building 8) and click **OK**.

3. In the navigation pane, click the Container for the APs.

   The **Authenticator Summary** window displays.

4. Enter a name for the AP; for example, *AP 9100 North Corner*.
5. Enter the AP's IP address.
6. From the **Vendor** drop-down list, select **Avaya-WLAN-TEMP**.
7. From the **Device Template** drop-down list, select the appropriate template created in Configuring the Device Template on page 16.
8. In the **RADIUS Shared Secret** field, enter the password.



9. Click OK.

   The AP is displayed in the **Authenticator Summary** window.

10. To add another AP as an Authenticator, click **New.....** in the Authenticator Summary window, and repeat Step 4 to Step 8.

Related Links

Ignition Server configuration for WLAN 9100 Series APs on page 13

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*.

Related Links

Ignition Server configuration for WLAN 9100 Series APs on page 13