

Campus Wireless LAN Reference Design

May 2016

AVAYA

Table of Contents

Preface	1
Introduction	3
Campus Wireless LAN Design	4
Third Generation Wireless	4
Internal User Wireless Design Details	6
Management	7
Authentication and Encryption	7
Wireless Services	9
Network Integration	11
Hardware and Software	12
Deployment	13
Planning Your Site with Avaya Wi-Fi Designer	13
Deploying Wireless Orchestration System	16
Deploying the WOS Default Profile	21
Deploying Application Control in WOS	29
Deploying the Avaya Ignition Server	32
Deploying Guest Manager	42
Deploying Campus Switches for Access Points	52
Deploying Different Security Policies on the Same SSID	55
Glossary	61

Preface

Document Conventions

Tips



Notes contain additional information.



Cautions contain important information about preventing data loss or equipment damage.

Text

Bold text indicates either a value to be entered or a user interface element.

This design uses **4051** and **4052** for the backbone VLANs

Blue text in a procedure indicates a configuration variable that you need to substitute with a value appropriate for your network. That value will differ from the value shown in the procedure.

b0ad.aa42.b884

or

Right-click **example.org**, and click **New Host**.

Highlighted text indicates emphasis.

Port1/32 1 **UP** 7d 06:26:22 127 22 d4ea.0ece.3465

Configuration Variables



For command-line input (CLI), you need to substitute example configuration values (such as IP addresses and MAC addresses) with values appropriate for your network.

Depending on the number of devices you are configuring, you will perform some procedures multiple times. Those procedures begin with a “Configuration variables” table. In the below example, you would first perform the procedure on box 8201, substituting values appropriate for your network. Then you would repeat the procedure on box 8202, substituting values for the second device in your network.

Configuration variables

Value	8201	8202
SPBM instance	10	10
SPBM nick-name	1.82.01	1.82.02
Backbone VLANs	4051,4052	4051,4052
ISIS area	49.0010	49.0010

Diagrams

-  Red lines denote a shortest path bridging (SPB) link.
-  Black lines denote a non-SPB link.

You can also view a [glossary of the icons](#) used this guide.

Feedback

Please [send us](#) your comments and suggestions.

Introduction

The *Campus Wireless LAN Reference Design* discusses the design and deployment of a wireless local area network (LAN) in organizations occupying one or more buildings in close proximity. This guide discusses the choices available when designing a campus wireless LAN (WLAN) and how to decide between them. This guide also explains how to deploy the identity engines, wireless orchestration system, and access points, as well as how to integrate to an Avaya Fabric Connect network.

The information included in this guide is based on common customer requirements and provides a tested starting point for engineers to begin designing and deploying an Avaya network. This guide does not document every possible way to design and deploy a network but instead presents the tested and recommended options that will meet the majority of customer needs.

Campus Wireless LAN Design

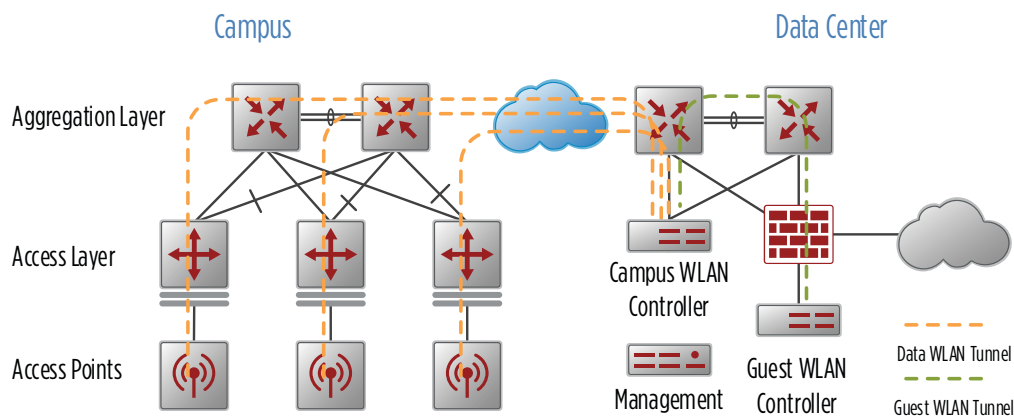
Third Generation Wireless

The Avaya 9100 series access points (APs) and WLAN Orchestration System (WOS) are third generation WLAN products that incorporate the best parts of the first and second generation. Coupled with an Avaya campus LAN based on Fabric Connect, the WLAN provides the availability, scalability, and visibility today's customers require.

First-generation WLANs used standalone APs that were mostly deployed in a few select locations, such as classrooms and conference rooms. As wireless networks became more pervasive and the applications relying on them grew, the shortcomings of the first-generation WLANs became apparent. In those first-generation networks, organizations found it difficult if not impossible to seamlessly roam between access points, to tune the radio frequency (RF) settings across all the access points (to provide optimal coverage and power levels), and to manage and upgrade the devices as a whole network.

Second-generation networks strove to solve the shortcomings of the first-generation networks through the introduction of the WLAN controller. Controllers provided a central point for device and RF management, and they provided a means for all the access points in the network to operate as a unit, allowing for fast roaming. However, as convenient as second-generation networks have been, their own shortcomings are emerging. Specifically, the need to tunnel all the wireless LAN traffic back to a centralized controller reduces availability, scalability, and visibility.

Figure 1 Controller based wireless network



The Avaya 9100 wireless system is a hybrid of the standalone and controller-based architectures. The capabilities that worked best centrally—specifically configuration, device management and visibility—are centralized in the WLAN orchestration system, and capabilities that have an advantage at the edge have been returned to the access point. These edge features include RF management, roaming key exchange, and advanced capabilities such as application control. You are able to move these features to the edge by using intelligent access points that have increased hardware capabilities compared to first or second-generation devices. However, intelligence access points

working alone can't replace the collective intelligence a controller has about the network. To solve this, Avaya 9100 series access points work together as one network by discovering access points in close RF-proximity and sharing relevant information.

The Avaya 9100 wireless system's availability does not rely on any central device. If WOS is taken offline, there is no effect on the existing wireless LAN traffic or on the ability to have new users join the network.

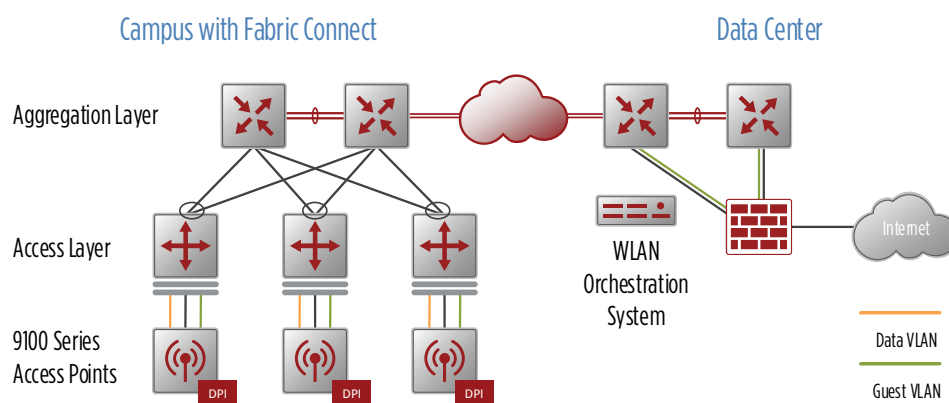
Moving the right features to the edge allows for a more scalable solution. For example, application control capabilities through deep packet inspection (DPI) scale linearly with the number of access points in the network. If that feature was centralized, its scale would be bound by the controller, and as access points were added or upgraded to a faster technology, the controller would have to as well. In controller-based networks, all traffic is tunneled to the centralized controller, putting extra traffic on the network, and scale is limited by the controller's capabilities. With Avaya's 9100 wireless system, traffic goes directly where it is destined instead of being backhauled to the controller. This provides a network that is easier to scale, because traffic isn't transmitted on devices and links that aren't part of the path between the two endpoints. Also, there is no controller that all wireless traffic traverses that must scale with the network.

Removing tunnels from the network increases visibility in the network. Security functions, quality of service, and troubleshooting tools like SPAN can all be applied consistently to wired and wireless traffic. This underscores the value of integrating the Avaya 9100 wireless system with a fully capable campus LAN infrastructure like the Avaya ERS and VSP devices.

One benefit of tunneling wireless traffic to a controller was an easy way to segment groups of users from each other. Specifically, guest traffic can be tunneled back to a controller in the DMZ. This ensures that guest users cannot access any internal resources and that they have access only to the Internet.

The Avaya 9100 wireless solution, working in conjunction with the Avaya Campus LAN running Fabric Connect, provides customers with the ability to continue to use segmentation as a means to separate user groups, both internal and guests. Customers can get the benefit of the hybrid architecture while still using central points of security control.

Figure 2 Avaya 9100 series wireless



Internal User Wireless Design Details

In this reference design, Avaya 9100 series APs deployed and managed through WOS provide access to two wireless networks, one for internal users and a second that provides guest access for visitors.

Avaya WLAN 9100 series include four indoor APs that cater to different deployment and client requirements. All 9100 series indoor APs have common software and feature sets, including:

- **Software defined radios**—Two radios configurable for both the 5GHz and 2.4GHz bands. You can reconfigure the number of radios in your network supporting the 5GHz band as the number of clients supporting that band increases over time.
- **Auto Cell Size**—Auto Cell Size is an automatic, self-tuning mechanism that balances transmit power between access points in order to help guarantee coverage while limiting the RF energy that could extend beyond the organizational boundary. Auto Cell uses communication between access points to dynamically set radio power so that complete coverage is provided to all areas, yet at the minimum power level required. This helps to minimize potential interference with neighboring networks. Additionally, access points running Auto Cell automatically detect and compensate for coverage gaps caused by system interruptions.
- **Spectrum Management**—In the automatic mode, channels are allocated dynamically, driven by changes in the environment. Access points perform Auto Channel assignment by scanning the surrounding area for RF activity on all channels, then automatically selecting and setting channels on the access point to the best channels available. You typically execute this function when initially installing access points in a new location, and you may optionally configure it to execute periodically to account for changes in the RF environment over time. Auto Channel selection has significant advantages, including that it more accurately tunes the RF characteristics of a wireless installation than a manual configuration does, because the radios themselves are scanning the environment from their physical location.
- **Air Cleaner Filters**—The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. You may select all of the air cleaner rules for the greatest effect, or only specific rules, such as broadcast or multicast, to eliminate only a particular source of traffic.

To choose between access points you must decide two things. Your first decision is whether you want 802.11ac to be enabled the day you install it or sometime in the future. If you choose an access point that doesn't support 802.11ac on day one, Avaya WLAN 9100 allows you to upgrade to 802.11ac (the latest WLAN industry standard that delivers gigabit throughput) with just a software upgrade—no need to touch the access point.

Secondly, you must determine whether wireless devices attaching to your network today or in the future can take advantage of a 3x3 MIMO access point. High-end laptops and business-class devices are best suited to take advantage of 3x3 MIMO access points. Tablets, phones, and Chromebooks typically support 2x2 or less.

Table 1 9100 Series Indoor Access Point Portfolio

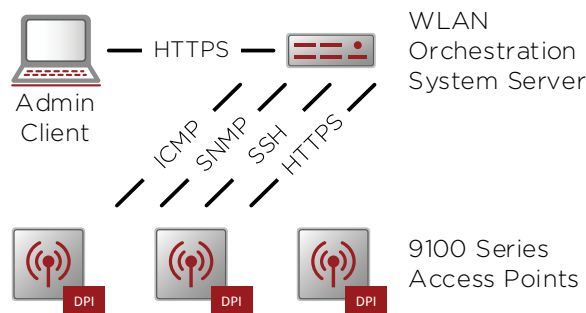
Access Point	802.11ac support	Spatial Streams
9122	With license	2x2
9123	With license	3x3
9132	Day one	2x2
9133	Day one	3x3
9144	Day one	4x4
9112	Day one	2x2
9114	Day one	2x2

Management

Avaya 9100 series access points are managed through the Wireless LAN Orchestration System. WOS is a wireless network management web application for managing Avaya access points. WOS provides centralized monitoring, configuration, reporting, and management functions for access points—either individually, by group, or for all access points. Administrators use WOS through a web interface. The WOS server is designed to be run on a virtual platform in the data center. The application package allows you to install and run the WOS server on your own virtual machine under VMware vSphere or Microsoft Hyper-V.

WOS allows IT administrators to simplify repetitive tasks by managing configurations, scheduling firmware upgrades across multiple wireless access points, and creating groups of wireless access points. All of these features allow the IT department to actively monitor and manage the health of their wireless network from anywhere, using a browser.

Figure 3 WOS and 9100 Series Access Points



Authentication and Encryption

Wireless clients are authenticated via the Avaya Identity Engines Ignition Server. Ignition Server is an 802.1X-capable RADIUS authentication, authorization, and accounting (AAA) server that permits or denies users access to a network based on policies. Access policies are stored on the Ignition Server while internal user accounts and groups are maintained on an existing user directory such as Microsoft's Active Directory.

The Ignition Server installs in your data center as a virtual appliance on VMware and is managed through a client application called Ignition Dashboard.

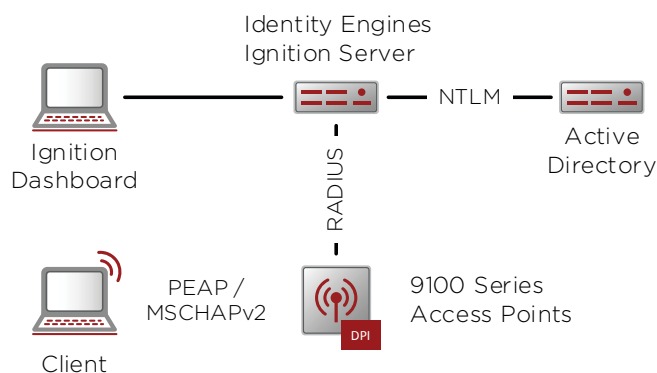
All access points will authenticate and authorize clients directly to the Ignition Server. However, each access point is not required to be defined in the Ignition Server authenticator list. One authenticator bundle for each wired aggregation block is defined to contain the amount of configuration required on the Ignition Server, and access points can obtain IP address information via DHCP.

Internal Wireless Network

The Avaya Ignition Server supports a number of extensible authentication protocols (EAP) methods, which include EAP-TLS, EAP-GTC, and PEAP. EAP-TLS is based on public key infrastructure (PKI) and leverages digital certificates issued to both the Ignition Server and users while EAP-GTC, and PEAP support credentials which can be validated against a backend user directory store such as Active Directory. In this reference design, the internal wireless network is configured to support PEAP and EAP-GTC.

EAP-GTC and PEAP each operate in a similar manner: Ignition Server establishes a secure transport layer security (TLS) session with the 802.1X client before the user's credentials are exchanged through the TLS tunnel. The main advantage of these EAP methods over EAP-TLS is that a signed certificate is only required on the Ignition Server. The 802.1X clients do not require a user certificate, which greatly simplifies implementation, deployment, and management of the authentication system.

Figure 4 Internal Wireless



Guest Wireless Network

In this reference design, the guest wireless network is not configured for wireless encryption. This allows visitors to easily connect. To ensure only authorized visitors are able to use the guest network, a captive portal provides an alternate mode of authentication to a wireless network. The captive portal blocks network traffic from a visitor until they are authenticated. The captive portal displays a login page when a user associates to the guest wireless network and opens a browser to any website. Once authenticated, the browser is redirected either to your specified landing page, if any, or else back to the originally requested website.

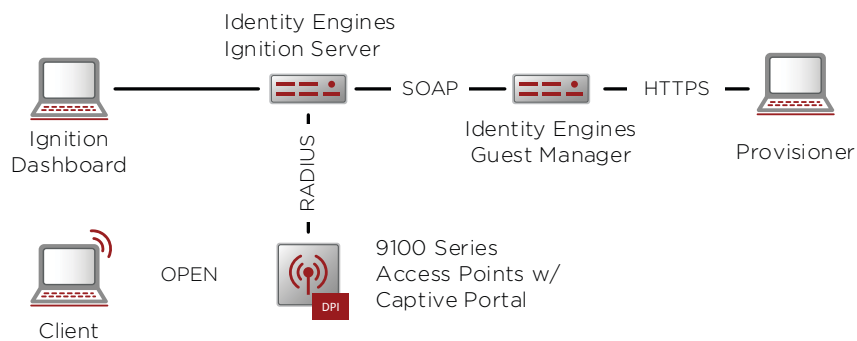
You can customize the captive portal's login page with any organization-specific content or site design.

In this reference design, each Avaya 9100 series access point in the network that is enabled for guest access has the internal captive portal service configured. Once authenticated, the guest user can roam between access points without being prompted to re-authenticate.

Avaya Identity Engines Ignition Guest Manager lets internal users create and manage temporary network accounts for visitors. Guest Manager installs as a web service on Microsoft Windows 2003 and 2008 server. In this reference design, provisioners are defined based on Active Directory group membership while the Guest Manager creates and manages the guest accounts in the internal user store of the Ignition Server appliance. When a guest attempts to authenticate via the captive portal, the access point sends the authentication request to the same Ignition Server as for internal clients, policy on the Ignition Server ensures guests cannot authenticate to the internal wireless network.

Guest Manager also requires access to a simple mail transfer protocol (SMTP) server. When guest accounts are created, the provisioner does not see the automatically-generated password; instead the credentials are emailed (or sent as an SMS) directly to the guest.

Figure 5 Guest Wireless



Wireless Services

The access point provides services at the edge of the network in order to enhance scalability and performance of the network.

Bonjour Support

Bonjour is Apple's "Zero Config" networking solution that facilitates simplified deployment of Apple devices.

Because Bonjour and specifically mDNS use *Link Local* multicast, this means that Apple devices in different virtual LANs (VLANs) do not discover each other and are unable to connect to each other's services. This is creating issues because Apple iOS applications that use mDNS (such as AirPlay and AirPrint, as well as Apple devices such as AppleTV) find their way into classrooms and meeting rooms, and their users expect them to work the same as they do in their home network environment.

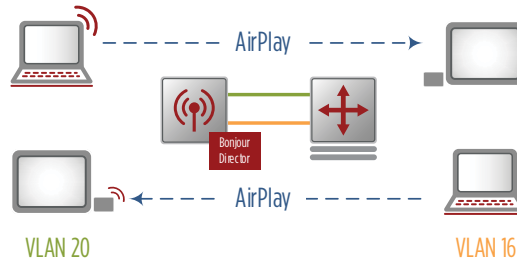
When the access point receives a multicast packet on a wireless interface SSID/VLAN, it will compare the destination multicast address to its multicast forwarding table to determine if the packet needs to be forwarded to any additional VLANs on the wired interface, or if it should just be bridged to the VLAN associated with the SSID.

If the multicast address is in the forwarding table, it will then check the Multicast VLAN Forwarding table to determine if there are specific VLAN entries configured. If there are, the packet will only be forwarded to those VLANs. If no entries are present, the packet is forwarded to all of the defined VLANs on the wired interface. If the multicast packet is mDNS, the access point will also check the MDNS filter table to determine if it should forward all mDNS packets, or if only specific services

should be forwarded. If there are no entries, all mDNS packets are forwarded. If there are specific services in the table, it will only forward those specific services.

For the access point to be able to forward and filter multicast packets, the local networks need to be accessible by the access point. For example, if you want to forward mDNS AppleTV service queries and responses between VLAN 16 and VLAN 20, both VLANs need to be connected to the access point. This is normally accomplished by trunking both VLANs over the same physical Ethernet connection using IEEE 802.1q, over a Gigabit Ethernet connection from the LAN switch to the access points Gigabit Ethernet port.

Figure 6 Bonjour support



Application Control

The Application Control feature available on the Avaya 9100 series access points provides real-time visibility and control of application usage by users across the wireless network.

The access point uses Application Control to determine what applications are being used and by whom, as well as how much bandwidth they are consuming. You can track application usage over time to monitor trends, with usage tracked by access point, VLAN, or station. Application Control recognizes many hundreds of applications groups them into a number of categories. It rates the applications by their degree of risk and productiveness and presents the results to you both graphically and in tables.

In addition to visibility, Application Control allows you to put filters in place in order to implement per-application policies. You can also restrict disruptive applications or increase the priority of important applications like VoIP and Scopia.

The distributed architecture of Avaya's 9100 series access points allows Application Control to scale naturally as you grow the network. Each access point performs application control locally, allowing the feature so scale linearly with the number of access points in the network.

Figure 7 Application Control

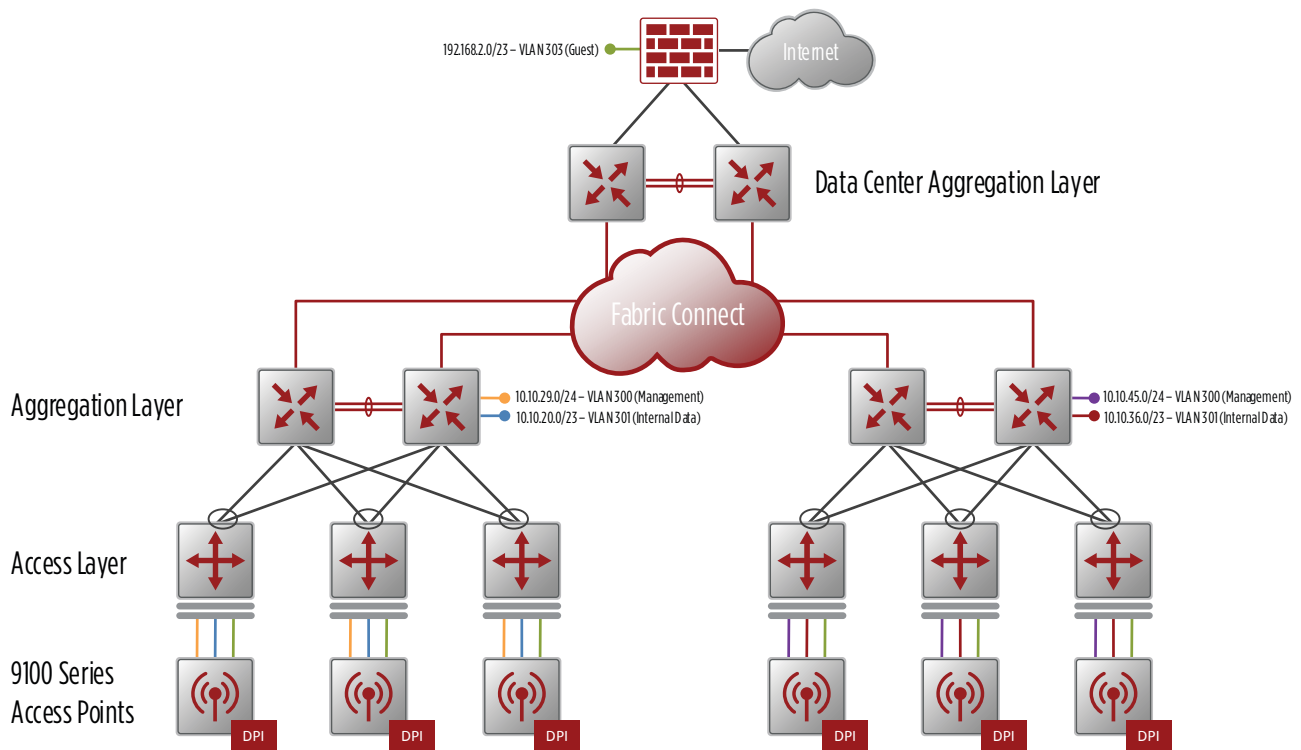


Network Integration

To maintain sessions for real-time data traffic, such as voice and video, users must be able to maintain the same IP address through the entire session. With traditional networks, VLANs and subnets should have boundaries at the aggregation layer switches. With Fabric Connect, you can extend Layer 2 anywhere in the network. The aggregation layer does not have to be a Layer 2/ Layer 3 boundary for network stability, as it would be in a traditional campus network.

With Avaya Fabric Connect, VLAN numbering is only locally significant within the aggregation block. However, WOS profiles contain information on VLAN numbering, so to simplify deployment use the same VLAN numbering across aggregation blocks. IP addressing should be unique at each aggregation block for the management and internal wireless networks. This allows for Layer 2 roaming within a building, and a contained management domain for the access points. Guest IP addressing will be common across the campus, terminating at the internet firewall.

Figure 8 Network Integration



Hardware and Software

The hardware and software validated while creating this guide.

Table 2 Validated Hardware and Software

Component	Platform	Software Version
Access layer switch	Avaya ERS 4850	5.8.1
Access point	Avaya 9122 Avaya 9123 Avaya 9132 Avaya 9133 Avaya 9144	7.6 8.1.1 (for AP 9144)
WLAN Orchestration System	VMWare 5.5	7.5.5
Ignition Server	VMWare 5.5	9.1
Ignition Guest Manager	Windows 2008 R2 64-bit	9.2.3
Ignition Dashboard	Windows 7	9.2.4
WiFi Designer	Windows 7	1.9

Deployment

Procedures

Planning Your Site with Avaya Wi-Fi Designer

- 1.1 Start the Plan
- 1.2 Draw Walls on the Map
- 1.3 Place Access Points on the Map
- 1.4 Analyze the Results

The Avaya Wi-Fi Designer is a laptop or tablet-based tool developed by Avaya for performing radio frequency (RF) site surveys. Use it to perform predictive designs and active surveys for design and verification of Wi-Fi deployments. It maps signal strength over an entire site, revealing areas that meet your specified design criteria, as well as those that fail to meet them. Using Wi-Fi Designer to plan a wireless deployment allows you to optimally predict the number, type, and location of Avaya wireless access points for a particular site, without having access to the site. Wi-Fi Designer allows you to ensure the desired wireless coverage with the minimum number of access points. A floor plan map is used to graphically position the access points and display coverage. Post-deployment, use Wi-Fi Designer to check coverage and fine-tune SSID and Radio (radio) assignments.

You use a planning (or predictive) project to initially calculate the number and placement of access points on a site, without needing physical access points or access to the site. Drag and drop one or more access points on your floor plan map. In this predictive mode, Wi-Fi Designer uses knowledge of access point performance and your selected environment conditions, as well as information that you provide about walls inside the building, to calculate the estimated RF coverage. The results of a planning project may be used as a starting point for selecting initial access point positions for a Device Centric Site Survey.

Avaya Wi-Fi Designer's planning mode is useful for helping you decide where to deploy access points in advance of performing a physical site survey. This is a practical first step to take before you perform a device-centric site survey. You start with a floor plan, refine the floor plan by drawing in walls of various construction types to make the RF coverage model more accurate, and then drag and drop the desired access point models onto the map.

1.1 Start the Plan

Step 1: Open Avaya Wi-Fi Designer.

Step 2: Select **File > New**.

Step 3: Under Project Types, click **Planning**. The Create New Avaya Wi-Fi Designer Project dialog appears.

Step 4: In the **Specify project name** box, enter WLAN Planning Project.

Step 5: In the **Select location for project** box, browse to the location you want to save the plan.

Step 6: In the **Select floor plan for project** box, browse to the saved floor plan image you want to use in planning.

Step 7: Under **Select Baseline Setting**, choose **Drawing Walls**, and then click **OK**.

It is important to set the scale of each map in order for the results to display accurately and for location information to be as precise as possible.

It is very easy to set the scale. Before you start, measure the actual length of a wall or other feature represented on the map. The longer the object being measured is, the more accurate the scale will be.

Step 8: Measure a wall or other feature that is represented accurately on the map.

Step 9: In the Floor Plan ribbon, click **Scale Floor Plan**. The mouse pointer will change to a calibration tool.

Step 10: On the map, position the mouse pointer at one end of the wall or other feature that you measured and click. Move the mouse pointer to the other end of the feature and click again. The **Complete Floor Plan Scale** dialog box appears.

Step 11: Enter measured length of the feature, in feet and inches, and then click **OK**.

1.2 Draw Walls on the Map

Many buildings have a combination of types of construction materials, each which provide different levels of attenuation of RF signals. By drawing walls, you can specify a type of wall construction, and then draw the walls, windows, and doors on your floor plan.

Step 1: In the Walls ribbon, click the construction type. The **Wall Properties** dialog box appears.

Step 2: For **Material**, choose **Interior Hollow Wall**, and then click **OK**.

Step 3: Click the **Draw Walls** button. The mouse pointer changes to the Walls pointer.

Step 4: Use the mouse to move the Walls pointer to the starting point of a wall. Click and drag to the desired end point, and release the mouse button to terminate the line segment.

Step 5: Repeat this process to enter as many walls of the same material as you need.

Note If you end a wall very close to the endpoint of another wall, they will snap together to form a corner. This snap feature is only active for connecting two endpoints.



Step 6: If you have additional walls constructed of a different material, change the material as explained in Step 2, and proceed to draw the new walls.

Step 7: When you are done working with walls, click the **Draw Walls** button again to exit walls mode.

1.3 Place Access Points on the Map

Planning a deployment involves placing one or more access points on the map. Wi-Fi Designer allows you to specify settings for individual radios on access points. You may enable and disable radios, designate the monitor radio, select operating bands, and adjust transmit power. These settings will be taken into account when the project heatmap is computed. The heatmap and RSSI lines will show antenna patterns for your radio settings.

Step 1: In the Survey ribbon, click the **Add Source** button. The **New Installed Wi-Fi Source Properties** dialog box is displayed.

Step 2: For **WIFI Source Type**, choose **WAP9133**.

Step 3: The new access point is placed at the upper left hand corner of the map. Move the access point to the desired location.

Step 4: Double-click the access point to show its radio view. Each radio is represented by a labeled wedge.

Note The wedges are displayed in the following colors:

Blue—Radio is on and operating in the 5 GHz band. Transmit power is also shown.

Green—Radio is on and operating in the 2.4 GHz band. Transmit power is also shown.

White—Radio is designated as the monitor radio and thus not available to wireless clients, or radio is off (disabled).



Step 5: Right-click on the wedge for the desired radio to display the drop-down menu. This menu allows you to:

- **Make Monitor**—Make this radio a monitor radio. Note that if a different radio was previously the monitor, that radio will lose its monitor status and will be switched off.
- **Turn 2.4 GHz On/Turn 5 GHz On**—Set this radio to the 2.4 GHz or 5 GHz band and turn it on.
- **Turn Off**—Disable this radio.
- To change **Tx Power** (1 to 20 dBm), right-click the wedge for the desired radio and from the drop-down menu, select **Properties**.

Step 6: Adjust the orientation of the access point by clicking and holding the green dot located

beneath the **radio1** label. Use it to rotate the access point until the direction that radio2 is facing on the map is the desired direction for deployment. This generally means that the monitor radio is facing in the direction of least desired wireless coverage.

1.4 Analyze the Results

Step 1: In the Analyze ribbon, click **Heatmap**.

Step 2: In the Source ribbon, click **Select All**.

Step 3: On the right hand side of the screen, click the **Settings** tab. The settings pane expands.

Step 4: For **Frequency Band**, choose **5 GHz**.

Next, select a number of overlapped sources for which to check. For example, if you select the number 4, then areas that have wireless coverage from at least 4 separate access points will display regularly. Areas that have coverage from fewer sources are displayed in gray tones. If you do not wish to consider how many wireless sources are available at any location, select **None**.

Step 5: For **overlapped sources**, choose **2**.

Next, select the acceptable signal strength.

Step 6: Click in the palette or drag the slider underneath until the value reads **-67dbm**.

The map shows areas that do not meet this criterion (that is, that have unacceptable signal strength) in gray tones.

Step 7: Move or add access points to the map until the desired coverage is achieved.

Procedures

Deploying Wireless Orchestration System

- 2.1 Add WOS DNS Record
- 2.2 Deploy the WOS OVA
- 2.3 Configure WOS Appliance
- 2.4 Configure WOS

You should fully deploy and configure WOS prior to deploying access points. In this reference design we use VMWare vSphere for deployment.

2.1 Add WOS DNS Record

The 9100 Series access points use the **avaya-wos** DNS record to locate and register to the wireless orchestration system. A DNS record is also configured to make it easy for administrators to contact the WOS server

Table 3 Configuration variables

Value	All aggregation switches
DNS domain	avaya.test
Appliance hostname	wos
WOS IP address	172.16.1.14

Step 1: On the Windows 2012 server, open DNS Manager.

Step 2: Expand the server.

Step 3: Expand **Forward Lookup Zones**.

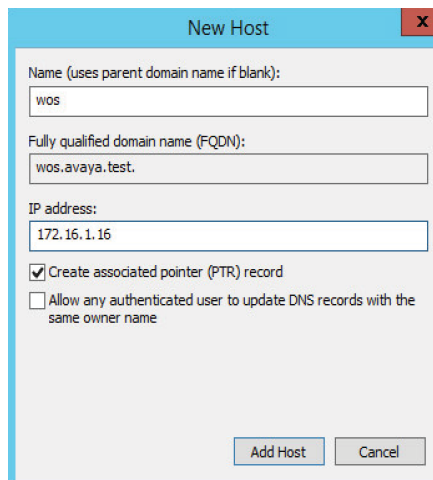
Step 4: Right click **avaya.test**, and click **New Host (A or AAAA)**.

Step 5: In the New Host window, in the **Name** box, enter **wos**.

Step 6: In the **IP address** box, enter **172.16.1.14**

Step 7: Select **Create associated pointer (PTR) record**.

Step 8: Click **Add Host**.



Step 9: In DNS Manager, right-click **avaya.test**, and click **New Alias (CNAME)**.

Step 10: In the New Resource Record window, in the **Alias name** box, enter **avaya-wos**.

Step 11: In the **Fully qualified domain name (FQDN) for target host** box, enter **wos.avaya.test**.

Step 12: Click **OK**.

The screenshot shows a 'New Resource Record' dialog box. It has a title bar with the text 'New Resource Record' and a close button (X). The dialog contains the following fields and controls:

- Alias (CNAME):** A text input field containing 'avaya-wos'.
- Fully qualified domain name (FQDN):** A text input field containing 'avaya-wos.avaya.test'.
- Fully qualified domain name (FQDN) for target host:** A text input field containing 'wos.avaya.test' and a 'Browse...' button to its right.
- Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.**
- OK** and **Cancel** buttons at the bottom.

2.2 Deploy the WOS OVA

Step 1: Open the VMWare vSphere Web Client.

Step 2: Select any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host.

Step 3: Select **Actions** > **All vCenter Actions** > **Deploy OVF Template**.

Step 4: In the **Deploy OVF Template** window, under **Select source**, select **Local file**, and click **Browse**.

Step 5: Select the wos ova, and then click **Open**.

Step 6: Click **Next**.

Step 7: Under **Review details**, click **Next**.

Step 8: Under **Select name and folder**, in the **Name** field, enter a name for the virtual machine. (Example: wos-vm)

Step 9: Select a folder or datacenter for the virtual machine to be located, and then click **Next**.

Step 10: Under **Select a resource**, select a host on which to run the virtual machine, and then click **Next**.

Step 11: Under **Select storage**, select a datastore as the virtual machine destination, and then click **Next**.

Step 12: Under **Setup networks**, for **Destination** choose the network connected to the data center, and then click **Next**.

Step 13: Select **Power on after deployment**, and then click **Finish**.

2.3 Configure WOS Appliance

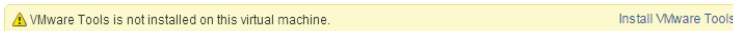
You must complete the initial setup of the appliance, including IP addressing information, prior to configuring WOS.

Table 4 Configuration variables

Value	All aggregation switches
WOS IP address	172.16.1.14/24
WOS default gateway	172.16.1.1
Admin password	Example9100password

Step 1: In the vSphere Web Client, in the WOS virtual machine, click the **Summary** tab.

Step 2: Click **Install VMWare Tools**, and then click **Launch Console**.



Step 3: In the WOS console, login with a username and password of **admin**.

Step 4: Install VMWare tools, configure the network interface, and change the cli admin password.

```
vm-tools install
config t
interface ethernet 0
  ip address 172.16.1.14 255.255.255.0
  exit
route
  add default 172.16.1.1
  exit
admin
  edit admin plain Example9100password
save
```

2.4 Configure WOS

Configure WOS with your licenses and adjust the polling rate based on the number of access points in your network.

Step 1: Open the WOS website at <https://wos.avaya.test:9443>

Step 2: Log in to WOS with the default username and password of **admin**.

Step 3: If you are prompted to run through the steps to discover access points, click **no**.

Step 4: In **Settings > General > WOS License**, enter your **License Key**, and then click **Apply**.

Step 5: In **Settings > WOS Users > Manage Users**, select the checkbox next to **admin**.

Step 6: Click **Change Password**. The Change Password window appears.

Step 7: In the **Old Password** box, enter **admin**.

Step 8: In the New and Confirm Password boxes, enter **Example9100password**, and then click **OK**.

Step 9: If WOS will be managing more than 100 access points, change the polling rate.

Step 10: In **Settings > Application > Polling**, in the **Polling Rate** list, choose **MEDIUM** for 100 - 250 access points, and **SLOW** for 250 and above.

Access Points are periodically polled by WOS to gather statistical information. A Fast rate can provide near real-time data about Avaya Access Points for smaller networks while a Slow rate is more suitable for a large network of Access Points. ([More Info](#))

Polling Rate

Optional Pollers

- Ethernet Statistics
- Interface Settings
- Interface MAC Information
- Radio Statistics
- Radio Settings
- Station Statistics
- VLAN Statistics
- WDS Statistics
- System Information
- Temperature Statistics
- Rogue Detection
- Rogue Control
- IDS Events (Enabling this poller may result in lower performance of the system)
- Station Assurance Events (Enabling this poller may result in lower performance of the system)
- Environment Control Statistics
- Application Control Statistics
- Application Control Station Statistics (Enabling this poller may result in lower performance of the system)
- Ethernet Statistics for AOS Lite devices
- System Information for AOS Lite devices
- Interface Settings for AOS Lite devices
- Station Statistics for AOS Lite devices
- Radio Settings for AOS Lite Devices

Deploying the WOS Default Profile

- 3.1 Create the profiles and configure global settings
- 3.2 Configure Profile SSID/VLANS
- 3.3 Configure External RADIUS
- 3.4 Configure Profile Support for Bonjour
- 3.5 Configure Profile Access Point Software Version

A profile allows you to specify a set of access points and manage them as a group. After creating a profile and defining it as the default profile, you define the configuration and software version. With the introduction of WLAN 9100 AOS-Lite Operating System software, which is suitable for access points such as 9112 and 9114, an AOS-Lite default profile has to be created separately. As new access points are discovered, they will automatically be added to the default profile.

3.1 Create the profiles and configure global settings

Table 5 Configuration variables

Value	All aggregation switches
Default profile name	Default_Profile
Timezone	GMT - 8
NTP server hostname	ntp.avaya.test
SNMP RO community	roexample
SNMP RW community	rwexample
Access point password	examplepassword
Filter list name	Default

First, create a new profile.

Step 1: In **Configure > Access Point Configuration > Profiles**, click **Add AOS Profile**. The Add New Profile window appears.

Step 2: In the **Profile Name** box, enter **Default_Profile**, and then click **OK**.

The screenshot shows a dialog box titled "Add New AOS Profile". Inside the dialog, there is a label "Profile Name:" followed by a text input field. The input field contains the text "Default_Profile" and is highlighted with a blue border.

Step 3: Select the box next to the name of the profile you just created, and then click **Default**.

Step 4: You are asked if you are sure you want this Profile set to default, click **OK**.

Step 5: Click the name of profile you just created, **Default_Profile**.

Step 6: Click the **Configuration** tab.

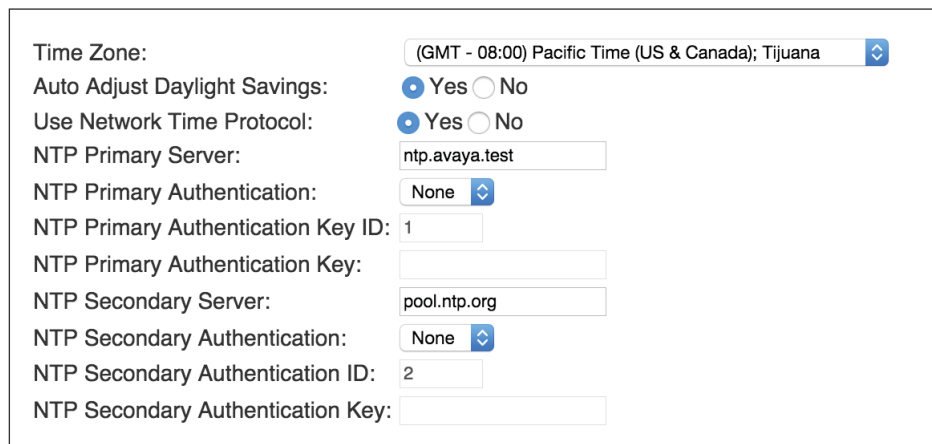
Next, enable network time protocol (NTP) to ease troubleshooting and log comparison between devices.

Step 7: In **Services > Time**, in the **Time Zone** list, choose **GMT – 08:00**.

Step 8: Next **Auto Adjust Daylight Savings**, select **Yes**.

Step 9: Next to **Use Network Time Protocol**, select **Yes**.

Step 10: In the **NTP Primary Server** box, enter **ntp.avaya.test**.



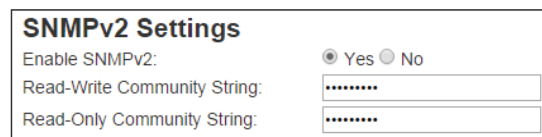
The screenshot shows the NTP configuration interface with the following settings:

- Time Zone: (GMT - 08:00) Pacific Time (US & Canada); Tijuana
- Auto Adjust Daylight Savings: Yes No
- Use Network Time Protocol: Yes No
- NTP Primary Server: ntp.avaya.test
- NTP Primary Authentication: None
- NTP Primary Authentication Key ID: 1
- NTP Primary Authentication Key: [empty field]
- NTP Secondary Server: pool.ntp.org
- NTP Secondary Authentication: None
- NTP Secondary Authentication ID: 2
- NTP Secondary Authentication Key: [empty field]

Next, enable SNMP to allow the access points to be managed by WOS.

Step 11: In **Services > SNMP**, in the **Read-Write Community String** box, enter **rwexample**.

Step 12: In the **Read-Only Community Sting** box, enter **roexample**.



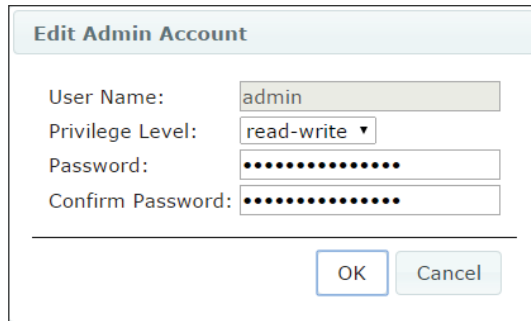
The screenshot shows the SNMPv2 Settings interface with the following settings:

- Enable SNMPv2: Yes No
- Read-Write Community String: [masked field]
- Read-Only Community String: [masked field]

Next, change the access point admin password from the default setting.

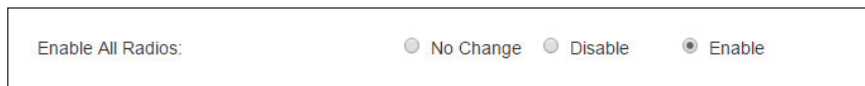
Step 13: In **Security > Admin Management**, select **admin** and then click **Edit**.

Step 14: In the **Password** and **Confirm Password** box, enter **examplepassword**.



Next, configure radio settings.

Step 15: In **Radios > Radio Settings**, for **Enable All Radios**, select **Enable**.

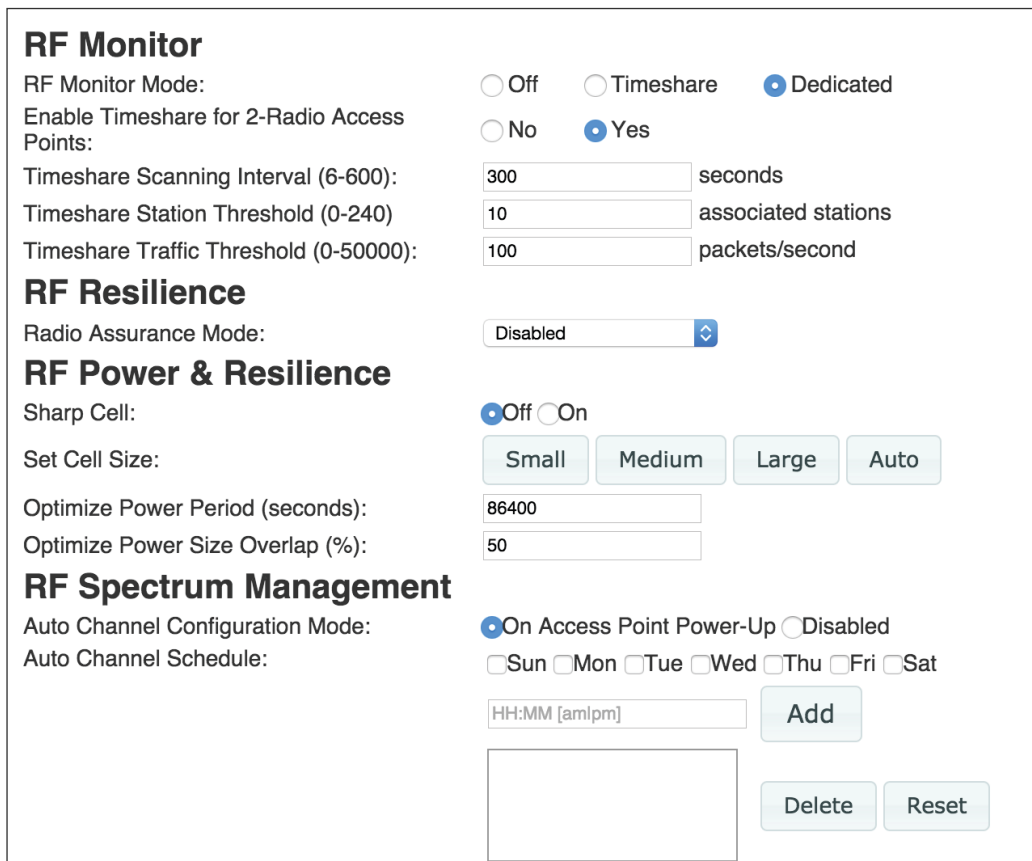


Step 16: Select your country.

Next, set optimal radio power to be calculated and negotiated with neighboring access points once a day.

Step 17: In **Radios > Advanced RF Settings**, in the **Optimize Power period** box, enter **86400**.

Step 18: In the **Optimize Power Size Overlap** box, enter **50**.



RF Monitor

RF Monitor Mode: Off Timeshare Dedicated

Enable Timeshare for 2-Radio Access Points: No Yes

Timeshare Scanning Interval (6-600): seconds

Timeshare Station Threshold (0-240): associated stations

Timeshare Traffic Threshold (0-50000): packets/second

RF Resilience

Radio Assurance Mode:

RF Power & Resilience

Sharp Cell: Off On

Set Cell Size:

Optimize Power Period (seconds):

Optimize Power Size Overlap (%):

RF Spectrum Management

Auto Channel Configuration Mode: On Access Point Power-Up Disabled

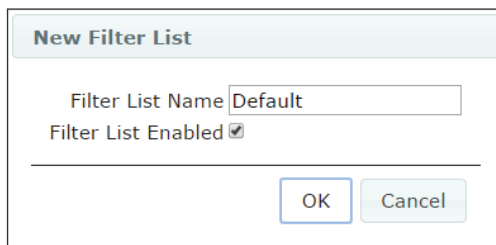
Auto Channel Schedule: Sun Mon Tue Wed Thu Fri Sat

Finally, enable the air cleaner filters which eliminate unnecessary wireless traffic.

Step 19: In **Filters > Filter Lists**, click **Add**. The New Filter List window appears.

Step 20: In the **Filter List Name** box, enter **Default**.

Step 21: Select **Filter list Enabled**, and then click **OK**.



Caution Do not use the pre-defined Global filter. It will negatively affect access point performance.



Step 22: In **Filters > Filter Management**, in the **Filter List** list, choose **Default**.

Step 23: Click **Add Preset Filters**. The Add Preset Filters window appears.

Step 24: In the **Select Preset Filters** list, choose **All air cleaner filters**, and then click **OK**.

3.2 Configure Profile SSID/VLANS

Configure two networks, one for internal data clients and a second for guest access to the internet.

Table 6 Configuration variables

Value	All aggregation switches
Data VLAN name	Data VLAN
Data VLAN id	301
Voice VLAN name	Voice VLAN
Voice VLAN id	302
Guest VLAN name	Guest VLAN
Guest VLAN id	303
Captive portal landing page	www.avaya.test
DNS server	172.16.1.20

First, configure the VLANs for internal users, voice handsets, and guests..

Step 1: In **VLAN > VLAN Management**, select **Enable Vlan Configuration For This Profile**.

Step 2: Click **Add**. The New VLAN window appears.

Step 3: In **Name** box, enter **Data VLAN**.

Step 4: In the **VLAN ID** box, enter the VLAN number **301**.

Step 5: Repeat Step 1 through Step 4 for the voice and guest VLANs, as shown in Table 6.

Step 6: In **SSIDs > SSID Management**, in the Add SSID box enter **Data**, and then click **Add SSID**.

Step 7: In the General Setting pane, select **Enabled**.

Step 8: Select **Broadcast**.

Step 9: In the **Vlan** list, choose **Data VLAN**.

Step 10: In the **Filter List** list, choose **Default**.

The screenshot shows the 'General Settings' configuration window for a new SSID. The settings are as follows:

Setting	Value
Name:	Data
Enabled	<input checked="" type="checkbox"/>
Broadcast	<input checked="" type="checkbox"/>
Band	Both
Vlan	Data VLAN
QoS	0
Filter List	Default
Avaya Roaming	L2
Fallback	None
Mobile Device Management	None

Additionally, the 'Vlan Number' is set to 301.

Step 11: Expand **Authentication/Encryption**.

Step 12: In the **Encryption/Authentication** list, choose **WPA2/802.1x**.

Next, configure the wireless network for guest users and setup the captive portal.

Step 13: In **SSIDs > SSID Management**, in the Add SSID box enter **Guest**, and then click **Add SSID**.

Step 14: Expand the General Settings pane, and then select **Enabled**.

Step 15: Select **Broadcast**.

Step 16: In the **Vlan** list, choose **Guest VLAN**.

Step 17: In the **Filter List** list, choose **Default**.

Step 18: In the **QoS** list, choose **1**.

Step 19: In the **Avaya Roaming** list, choose **L2 & L3**.

General Settings	
Name:	Guest
Enabled	<input checked="" type="checkbox"/>
Broadcast	<input checked="" type="checkbox"/>
Band	Both
Vlan	Guest VLAN
Vlan Number	303
QoS	2
Filter List	Default
Avaya Roaming	L2 & L3
Fallback	None
Mobile Device Management	None

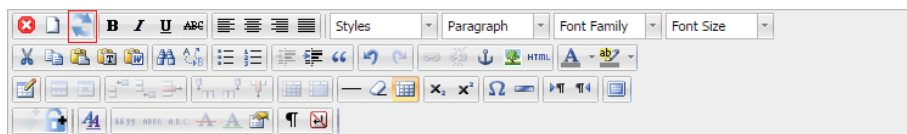
Step 20: Expand the Captive Portal pane.

Step 21: In the **Server** list, choose **Internal Login**.

Step 22: In The **RADIUS Authentication Type** list, choose **CHAP**.

Create the login page, which resides on the access point, using the captive portal editor. The HTML editor can add text and images and insert a section containing fields to capture user credentials, or you may insert a default login page and customize it.

Step 23: In the captive portal editor, click the default splash page button.



Finally, remove the default wireless network.

Step 24: In the **Currently select SSID** list, choose **avaya**, and then click **Delete select SSID**.

3.3 Configure External RADIUS

In this reference design, the Avaya Ignition Server provides client RADIUS authentication. Clients on the Data SSID authenticate against Active Directory, and clients on the guest SSID authenticate to the internal user store managed by the Avaya Ignition Guest Manager. Management authentication on the access point is provided by the local account. Configure the access points to contact the Ignition Server for all client authentication.

Table 7 Configuration variables

Value	All aggregation switches
Ignition server IP address	172.16.1.16
RADIUS shared secret	examplesecret

Step 1: In **Security > External RADIUS**, in the **Primary Server IP Address** box, enter **172.16.1.16**.

Step 2: In the **Shared Secret** box, enter **examplesecret**.

External RADIUS Settings

Enable External RADIUS: Yes No

Timeout (seconds):

DAS Port:

DAS Event-Timestamp: Optional Required

DAS Time Window:

External RADIUS Primary Server

Host Name / IP Address:

Port Number:

Shared Secret / Verify Secret:

External RADIUS Secondary Server

Host Name / IP Address:

Port Number:

Shared Secret / Verify Secret:

RADIUS Attribute Formatting

Called-Station-Id Attribute Format: BSSID BSSID:SSID

Station MAC Format: Lower case [xxxxxxxxxxxx] Upper case [XXXXXXXXXXXXXX] Lower case hyphenated [xx-xx-xx-xx-xx-xx] Upper case hyphenated [XX-XX-XX-XX-XX-XX]

Accounting

Enable RADIUS Accounting: Yes No

3.4 Configure Profile Support for Bonjour

Bonjour support allows Apple clients to use functions such as AirPlay and AirPrint. Configure the profile to support AirPlay to an Apple TV.

Table 8 Configuration variables

Value	All aggregation switches
Wired data VLAN name	Wired Data VLAN
Wired data VLAN id	198

If some of your Apple clients are connected to the wired network, add that wired VLAN to the profile.

Step 1: In **VLAN > VLAN Management**, click **Add**. The New VLAN window appears.

Step 2: In **Name** box, enter **Wired Data VLAN**.

Step 3: In the **VLAN ID** box, enter the VLAN number **198**, and then click **OK**.

Next, configure multicast forwarding between the networks to enable Bonjour support.

Step 4: In **Radios > Global Settings**, in the **Multicast Forwarding** box enter **224.0.0.251**, and then click **Add**.

Step 5: In the **Multicast VLAN Forwarding** list, choose **Data VLAN**, and then click **Add**.

Step 6: In the **Multicast VLAN Forwarding** list, choose **Wired Data VLAN**, and then click **Add**.

Step 7: In the **MDNS Filter** list, choose **Apple TV**, and then click **Add**.

Step 8: Click **Apply Config**.

3.5 Configure Profile Access Point Software Version

WOS does not include software images for the access points. Prior to beginning this procedure, download the access point software from support.avaya.com.

Step 1: Navigate to **Configure > Access Point Configuration > Profiles**.

Step 2: Select the box next to the name of the default profile, and then click **Set Access Point OS Version**.

Step 3: Select **WOS SCP Server**, and then click **Next**.

Step 4: For System Software, click the ellipsis (...). The Import System Software image window appears.

Step 5: Click **Choose file**. The open file dialog box appears.

Step 6: Browse to the saved AOS image on your computer, and then click **Open**.

Step 7: Click **Upload**. When the upload is complete, the System Software list will show the uploaded image.

Step 8: Click **Next**.

Step 9: Click **Finished**. A message appears, saying that there are no access points that require a new access point OS version. Ignore this message because there are no access points associated to the profile at this point. Access points will be upgraded as they are associated to the profile.

Deploying Application Control in WOS

- 4.1 Enable Application Control
- 4.2 Limit Traffic by Using Application Control
- 4.3 Deny Traffic by Using Application Control

Application Control is a licensed feature on the access points. Access points with application control enabled use Deep Packet Inspection (DPI) to determine what applications are being used and by whom, as well as how much bandwidth they are consuming. Additionally, you can configure bandwidth limits and deny traffic based on the application. Before beginning these procedures, install the application control licenses on the access points.

4.1 Enable Application Control

First, enable WOS to collect per-station application control statistics.

Step 1: In **Settings > Application > Polling**, select **Application Control Station Statistics**, and then click **Save**.

Access Points are periodically polled by WOS to gather statistical information. A Fast rate can provide near real-time data about Avaya Access Points for smaller networks while a Slow rate is more suitable for a large network of Access Points. ([More Info](#))

Polling Rate: MEDIUM

Optional Pollers:

- Ethernet Statistics
- Interface Settings
- Interface MAC Information
- Radio Statistics
- Radio Settings
- Station Statistics
- VLAN Statistics
- WDS Statistics
- System Information
- Temperature Statistics
- Rogue Detection
- Rogue Control
- IDS Events (Enabling this poller may result in lower performance of the system)
- Station Assurance Events (Enabling this poller may result in lower performance of the system)
- Environment Control Statistics
- Application Control Statistics
- Application Control Station Statistics (Enabling this poller may result in lower performance of the system)
- Ethernet Statistics for AOS Lite devices
- System Information for AOS Lite devices
- Interface Settings for AOS Lite devices
- Station Statistics for AOS Lite devices
- Radio Settings for AOS Lite Devices

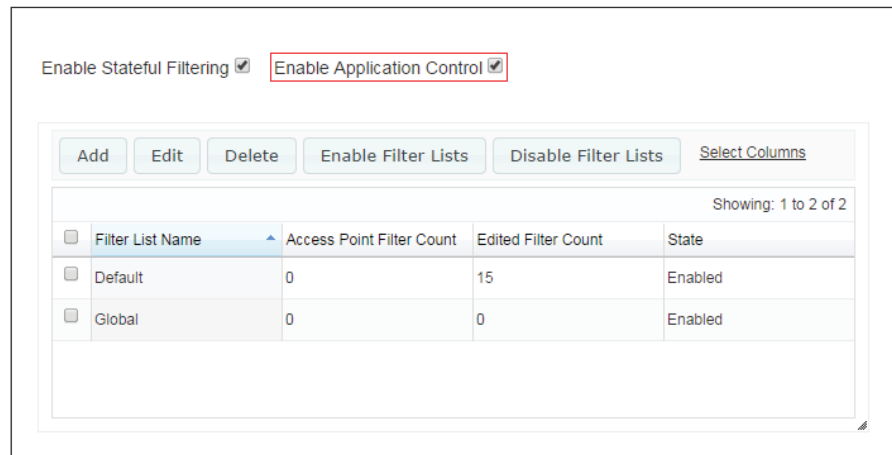
Save

Next, in the default profile, enable application control.

Step 2: In **Configure > Access Point Configuration > Profiles**, click the name of the default profile.

Step 3: Click the **Configuration** tab.

Step 4: In **Filters > Filter Lists**, select **Enable Application Control**.



4.2 Limit Traffic by Using Application Control

Add a new filter to the filter list you created and applied to the SSIDs in the section “Deploying the WOS Default Profile.” You can set limits to traffic for all stations concurrently or on a per-station basis. You can apply application control to a whole application category in one rule or to a single application. This example limits iTunes traffic, which includes app updates, on a per-station basis to 100Kbps.

Step 1: In **Filters > Filter Management**, in the **Filter List** list, choose **Default**.

Step 2: Click **Add**. The New Filter window appears.

Step 3: In the **Filter Name** box, enter **Apple App Store**.

Step 4: In the **Layer** list, choose **Layer 3**.

Step 5: Select **Enable**.

Step 6: In the **Traffic Limit Type** list, choose **Per Station Kbps**.

Step 7: In the **Traffic Limit** box, enter **100**.

Step 8: In the Application Control **Category** list, choose **Streaming Media**.

Step 9: In the **Application** list, choose **iTunes**, and then click **OK**.

New Filter

Filter List Name: Default

Filter Name: Apple App Store

Layer: Layer 3

Enable:

Type: Allow

Traffic Limit Type: Per Station Kbps

Traffic Limit: 100

Protocol: ANY

Port: ANY

Source: ANY Not

Destination: ANY Not

DSCP: <None>

QoS: <None>

VLAN: <None>

Application Control

Category: Streaming Media Application: iTunes

Filter Log

OK Cancel

4.3 Deny Traffic by Using Application Control

Add a new filter to the filter list you created and applied to the SSIDs in the section “Deploying the WOS Default Profile.” You can apply application control to a whole application category in one rule or to a single application. This example denies Instagram.

Step 1: In **Filters > Filter Management**, in the **Filter List** list, choose **Default**.

Step 2: Click **Add**. The New Filter window appears.

Step 3: In the **Filter Name** box, enter **Instagram**.

Step 4: In the **Layer** list, choose **Layer 3**.

Step 5: Select **Enable**.

Step 6: In the **Type** list, choose **Deny**.

Step 7: In the Application Control **Category** list, choose **Social Networking**.

Step 8: In the **Application** list, choose **Instagram**, and then click **OK**.

New Filter

Filter List Name: Default

Filter Name: Instagram

Layer: Layer 3

Enable:

Type: Deny

Traffic Limit Type: None

Traffic Limit: 10

Protocol: ANY

Port: ANY

Source: ANY Not

Destination: ANY Not

DSCP: <None>

QoS: <None>

VLAN: <None>

Application Control

Category: Social Networking Application: Instagram

Filter Log

OK Cancel

Finally, apply the configuration changes to the profile.

Step 9: Click **Apply Config**.

Procedures

Deploying the Avaya Ignition Server

- 5.1 Configure the Appliance
- 5.2 Configure Active Directory
- 5.3 Configure Virtual Groups
- 5.4 Configure Access Policy
- 5.5 Configure Authenticators

5.1 Configure the Appliance

Table 9 Configuration variables

Value	All aggregation switches
IDE IP address	172.16.1.16/24
Default gateway	172.16.1.1
Admin password	ExampleIDepassword
Site name	Example Organization
NTP server	172.16.1.1

Step 1: Login with a username and password of **admin**.

```
interface admin ipaddr 172.16.1.16/24
set password
Enter Current Admin Password:
Enter New Admin Password:
Re-Enter New Admin Password:
route add 0.0.0.0/0 172.16.1.1 admin
```

Step 2: Open the dashboard application.

Step 3: Install Base License

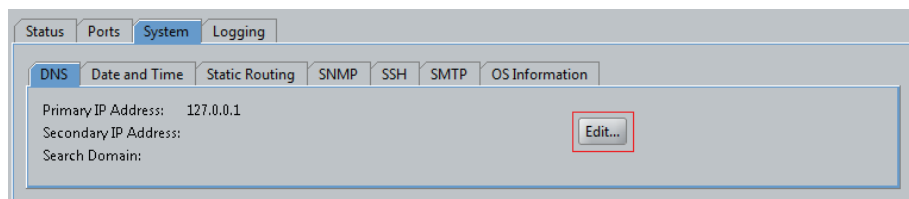
Step 4: Yes to Certificate warning

Step 5: In the Configuration pane, right-click **Site 0**, and then click **Rename Site**. The Rename Site window appears.

Step 6: In the **Site Name** box, enter **Example Organization**, and then click **OK**.

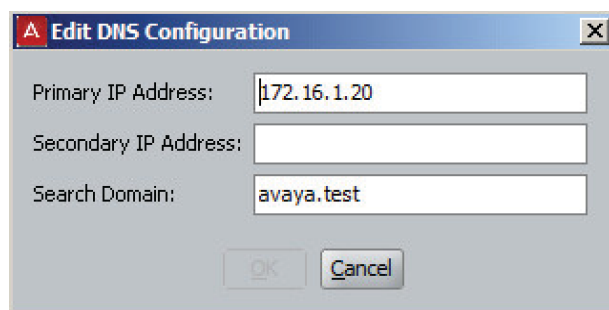
Step 7: Click the IP address of the server. The Nodes pane opens.

Step 8: Click the **System** tab and the **DNS** sub-tab, and then click **Edit**.



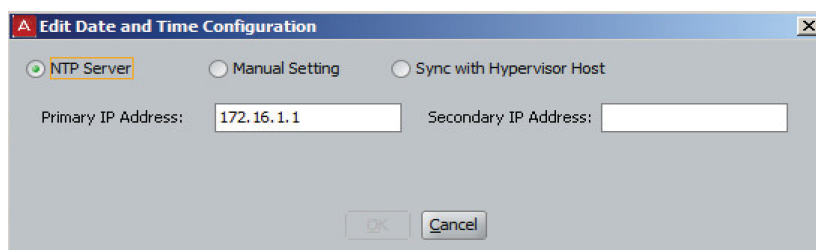
Step 9: In the **Primary IP Address** box, enter **172.16.1.16**.

Step 10: In the **Search Domain** box, enter **avaya.test**, and then click **OK**.



Step 11: Click the **Date and Time** tab, and then click **Edit**. The Edit Date and Time Configuration window appears.

Step 12: Select **NTP Server**, in the **Primary IP Address** box, enter **172.16.1.1**, and then click **OK**.



5.2 Configure Active Directory

Prior to integrating the Ignition server to Active Directory, you must create a service account in Active Directory that is a member of the Domain Admins group. Also, both the Ignition server and Active Directory server must be synced to the same NTP time source.

Table 10 Configuration variables

Value	All aggregation switches
AD domain name	avaya.test
Service account username	administrator
Service account password	idepassword
Directory name	Active Directory

Step 1: In **Site Configuration > Directories > Directory Services**, click **New**.

Step 2: On the Choose Service Type page, select **Active Directory**, and then click **Next**.

Step 3: On the Service Configuration Options page, select **Automatically Configure**, and then click **Next**.

Step 4: In the **AD Domain Name** box, enter **avaya.test**.

Step 5: In the **Service Account Name** box, enter **administrator**.

Step 6: In the **Service Account Password** box, enter **idepassword**, and then click **Next**.

Step 7: If IP address of Active Directory is not found, on the Connect to Active Directory page, manually enter the **IP address** of the Active Directory, and then click **Next**.

Step 8: In the **Name** box, enter **Active Directory**.

Step 9: Click **Test Configuration**. The Test Results window appears.

Step 10: Next to NETBIOS Server Name, click the flashlight icon.

Step 11: Click **OK**, and then click **Next**.

Step 12: Review the information shown on the **Created Active Directory Summary** page, and then click **Finish**.

Step 13: In **Site Configuration > Directories > Directory Sets > default set**, click **Edit**.

Step 14: Click **Add**. The Directory Set Entry window appears.

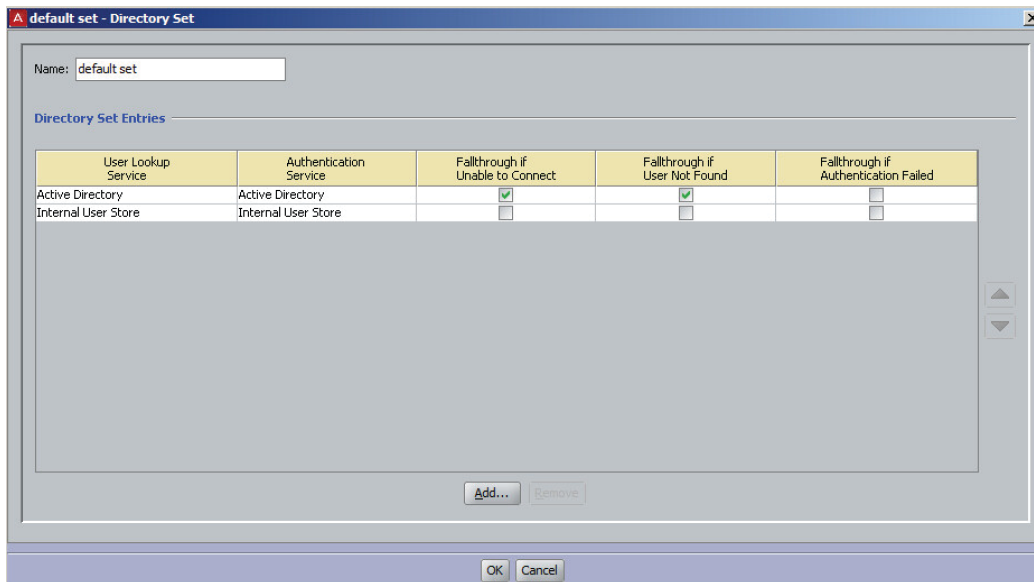
Step 15: In the User Lookup Service list, choose **Active Directory**.

Step 16: In the Authentication Service list, choose **Active Directory**, and then click **OK**.

Step 17: Click the Active Directory row, and move it to the top of the list by clicking the **up arrow**.

Step 18: In the Active Directory row, select **Fallthrough if Unable to Connect**.

Step 19: In the Active Directory row, select **Fallthrough if User Not Found**, and then click **OK**.



5.3 Configure Virtual Groups

This procedure assumes all internal user accounts in Active Directory are a member of a pre-existing group named Employees.

Step 1: In **Site Configuration > Directories > Virtual Mapping > Virtual Groups**, click **Actions > Add A New Virtual Group**. The Add Virtual Group window appears.

Step 2: In the **Virtual Group Name** box, enter **Employees**, and then click **OK**.

Step 3: Click **Add**. The Map Groups window appears.

Step 4: In the **Directory Service** list, choose **Active Directory**.

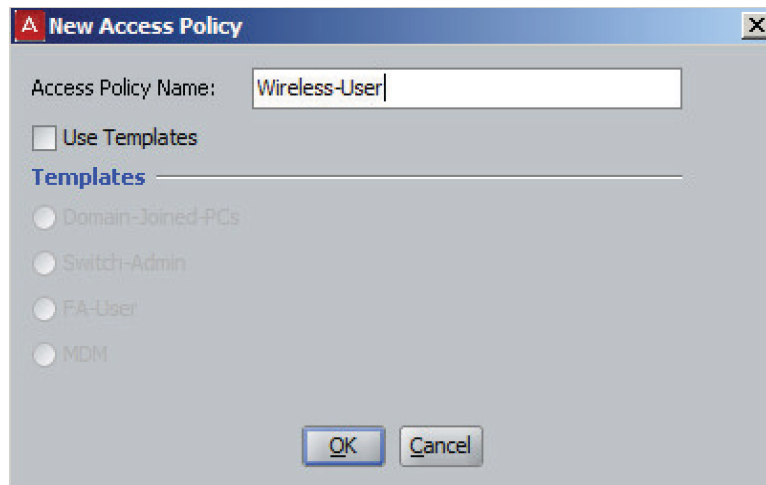
Step 5: Expand the Active Directory tree, select the **Employees** group, and then click **OK**.

5.4 Configure Access Policy

The *access policy* defines what set of authentication parameters are accepted, as well as the authorization rules that define who is allowed to access the network.

Step 1: In **Site Configuration > Access Policies > RADIUS**, click **New**. The New Access Policy window appears.

Step 2: In the **Access Policy Name** box, enter **wireless-user**, and then click **OK**.

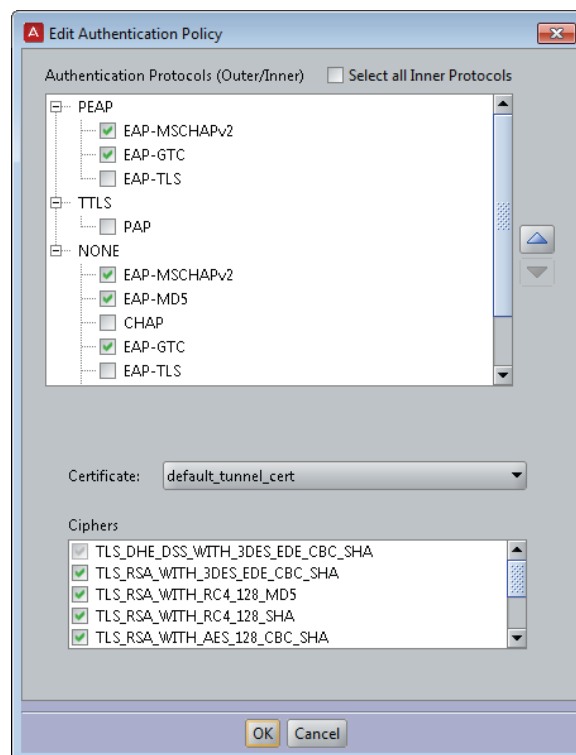


Step 3: In **Site Configuration > Access Policies > RADIUS > wireless user**, click the **Authentication Policy** tab.

Step 4: Click **Edit**.

Step 5: Expand **PEAP**, and then select **EAP-MSCHAPv2** and **EAP-GTC**.

Step 6: Expand **NONE**, and then select **EAP-MSCHAPv2**, **EAP-MD5** and **EAP-GTC**.



Note Your default installation includes sample certificate files that allow you to use the system without immediately installing your own certificates, but Avaya strongly recommends that you install your own certificates before deploying Ignition Server on a production network.



Step 7: Click the **Identity Routing** tab, and then click **Edit**. The Edit Identity Routing Policy window appears.

Step 8: Select **Enable Default Directory Set**, and then click **OK**.

Step 9: Click the **Authorization Policy** tab.

Step 10: Click the **Edit** button to the right of **RADIUS Authorization Policy**. The Edit Authorization Policy window appears.

Step 11: Click **Add**. The New Rule window appears.

Step 12: In the **Name** box, enter **Employees**, and then click **OK**.

Step 13: Click **New**. The Constraint Details window appears.

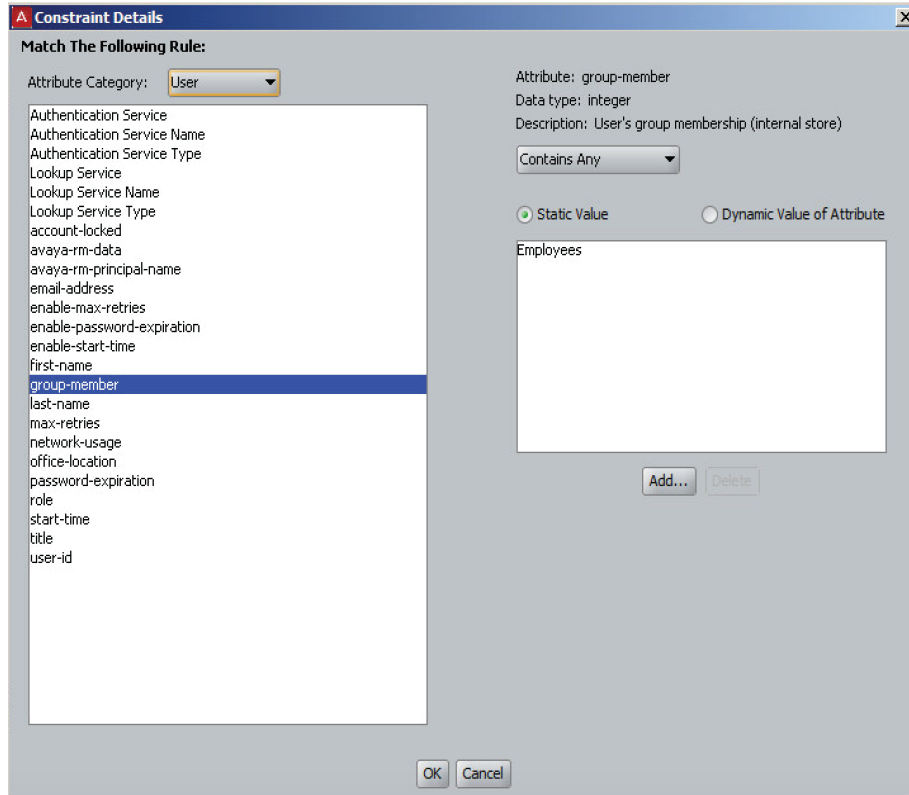
Step 14: In the **Attribute Category** list, choose **User**.

Step 15: Select **group-member**.

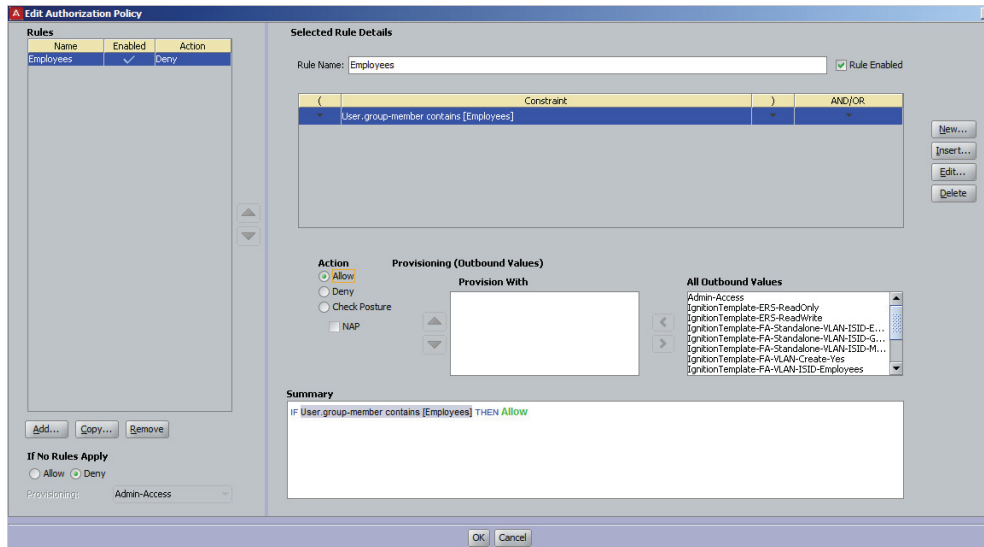
Step 16: Click **Add**. The Add Value window appears.

Step 17: In the **Add Group** list, choose **Employees**, and then click **OK**.

Step 18: Click **OK**.



Step 19: For Action, select **Allow**, and then click **OK**.



5.5 Configure Authenticators

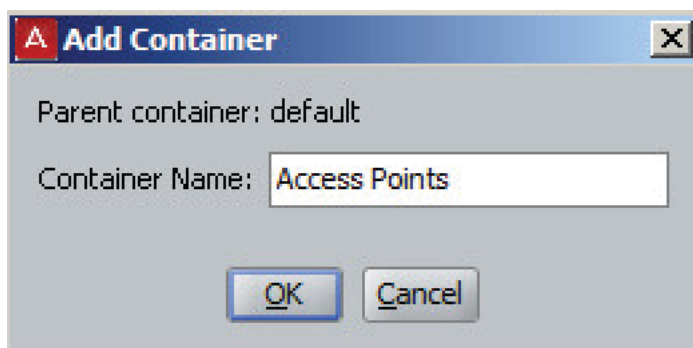
Define the per aggregation block management networks to which the access points are connected as authenticators. This allows access points to obtain IP addressing through DHCP and simplifies policy configuration.

Table 11 Configuration variables

Value	All aggregation switches
AP management subnet	172.16.2.0/24
Access policy name	wireless-user

Step 1: In **Site Configuration > Authenticators**, right-click **default**, and then click **Add Container**. The Add Container window appears.

Step 2: In the **Container Name** box, enter **Access Points**, and then click **OK**.



Step 3: In **Site Configuration > Authenticators > default > Access Points**, click **New**. The Authenticator Details window appears.

Step 4: In the **Name** box, enter **Aggregation Block 1 Access Points**.

Step 5: Select **Bundle**.

Step 6: In the **IP Address** box, enter **172.16.2.0/24**.

Step 7: In the **Vendor** list, choose **Avaya-WLAN**.

Step 8: In the **Device Template** list, choose **generic-avaya-wlan**.

Step 9: In the **RADIUS Shared Secret** box, enter **examplesecret**.

Step 10: In the **Access Policy** list, choose **Wireless-User**, and then click **OK**.

Authenticator Details

Name: Aggregation Block 1 Access Points Enable Authenticator

IP Address: 172.16.2.0 / 24 Bundle

Container: default.Access Points

Authenticator Type: Any

Vendor: Avaya-WLAN Device Template: generic-avaya-wlan

RADIUS Settings CoA Settings TACACS+ Settings

RADIUS Shared Secret: [masked] Show

Enable RADIUS Access

Access Policy: Wireless-User

Enable MAC Auth

Access Policy: default-radius-device

Use MAC Address as Password

Do Not Use Password

Use RADIUS Shared Secret As Password

Use This Password [] Show

OK Cancel

Step 11: In **Site Configuration > Authenticators > default > Access Points > Aggregation Block 1 Access Points**, click **New**.

Step 12: In the **Name** box, enter **Wireless Users**.

Step 13: In the **Authenticator Attribute** list, choose **Inbound-NAS-Port-Type**.

Step 14: In the **Attribute Value** box, enter **19**.

Step 15: In the **Access Policy** list, choose **Wireless-User**, and then click **OK**.

A Sub Authenticator Details

Name:

Authenticator Attribute:

Attribute Value:

Sub Authenticator Type:

Access Policy:

Enable MAC Auth

Use MAC Address as Password

Do Not Use Password

Use RADIUS Shared Secret As Password

Use This Password

Access Policy:

Procedures

Deploying Guest Manager

- 6.1 Configure Active Directory
- 6.2 Configure Ignition Server for Guest Manager
- 6.3 Update IDE Policy for Guests
- 6.4 Configure Guest Manager
- 6.5 Create Guest User Accounts

Avaya Identity Engines Ignition Guest Manager lets internal users create and manage temporary network accounts for visitors. Guest Manager installs as a web service on Microsoft Windows 2003 and 2008 server. In this reference design, provisioners are defined based on Active Directory group membership while the Guest Manager creates and manages the guest accounts in the internal user store of the Ignition Server appliance. When a guest attempts to authenticate via the captive portal, the access point sends the authentication request to the same Ignition Server as for internal clients, policy on the Ignition Server ensures guests cannot authenticate to the internal wireless network.

6.1 Configure Active Directory

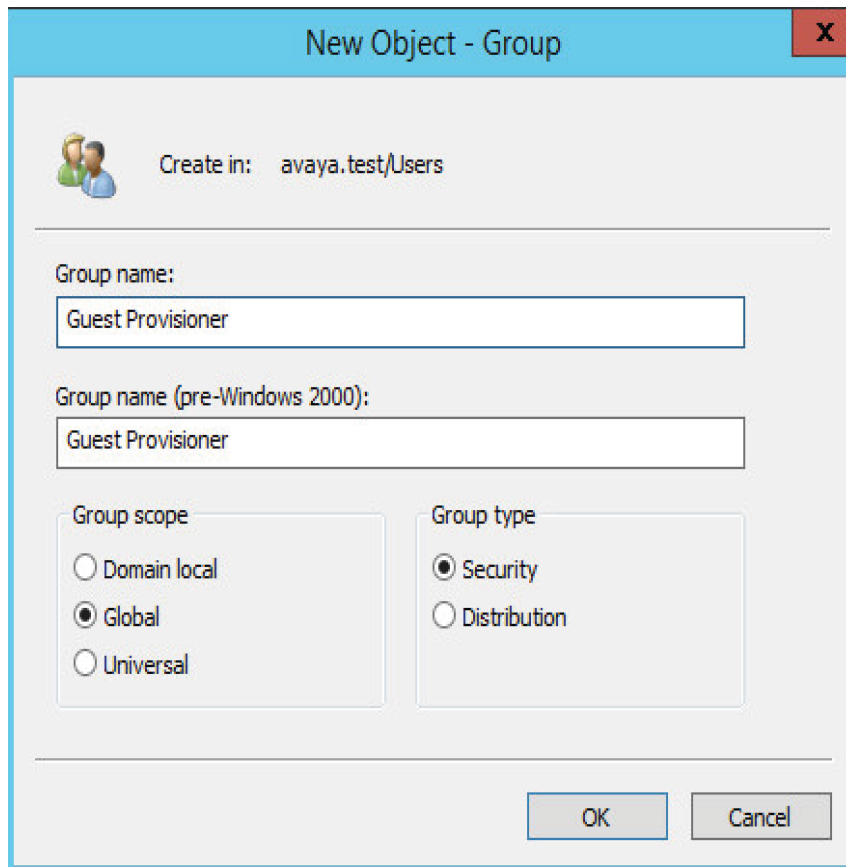
In Active Directory, create a group in which all provisioners will be a member. Assign appropriate users to the group.

Step 1: Open Active Directory Users and Computers

Step 2: Expand example.org, and then right-click **Users**.

Step 3: Click **New > Group**. The New Object - Group window appears.

Step 4: In the **Group name** box, enter **Guest Provisioner**, and then click **OK**.



The screenshot shows the 'New Object - Group' dialog box. The title bar is blue with the text 'New Object - Group' and a red close button. Below the title bar, there is a user icon and the text 'Create in: avaya.test/Users'. The 'Group name:' field contains 'Guest Provisioner'. The 'Group name (pre-Windows 2000):' field also contains 'Guest Provisioner'. There are two sections for group configuration: 'Group scope' with radio buttons for 'Domain local', 'Global' (selected), and 'Universal'; and 'Group type' with radio buttons for 'Security' (selected) and 'Distribution'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Step 5: Right-click the user, and then click **Add to a group**. The Select Groups window appears.

Step 6: In the object names box, enter **Guest Provisioner**.

Step 7: Click **Check Names**, and then click **OK**.

6.2 Configure Ignition Server for Guest Manager

The Ignition Server works in conjunction with the Guest Manager and stores the guest accounts in its internal user store. The Ignition Server also provides the policy that maps provisioners from the Active Directory group to the correct permissions in Guest Manager.

Table 12 Configuration variables

Value	All aggregation switches
SOAP username	soapadmin
SOAP password	soappassword
Guest Manager IP address	172.16.1.17
RADIUS shared secret	examplesecret

Step 1: Launch Ignition Dashboard and log into your Ignition Server as **admin**.

Step 2: In Dashboard's Configuration Hierarchy panel, click **Example Organization**.

Step 3: In the Sites panel, click the **Licenses** tab. Make sure the licenses list contains a license called "Guest Manager."

Step 4: In the Sites panel, click the **Services** tab, and then click the **SOAP** tab.

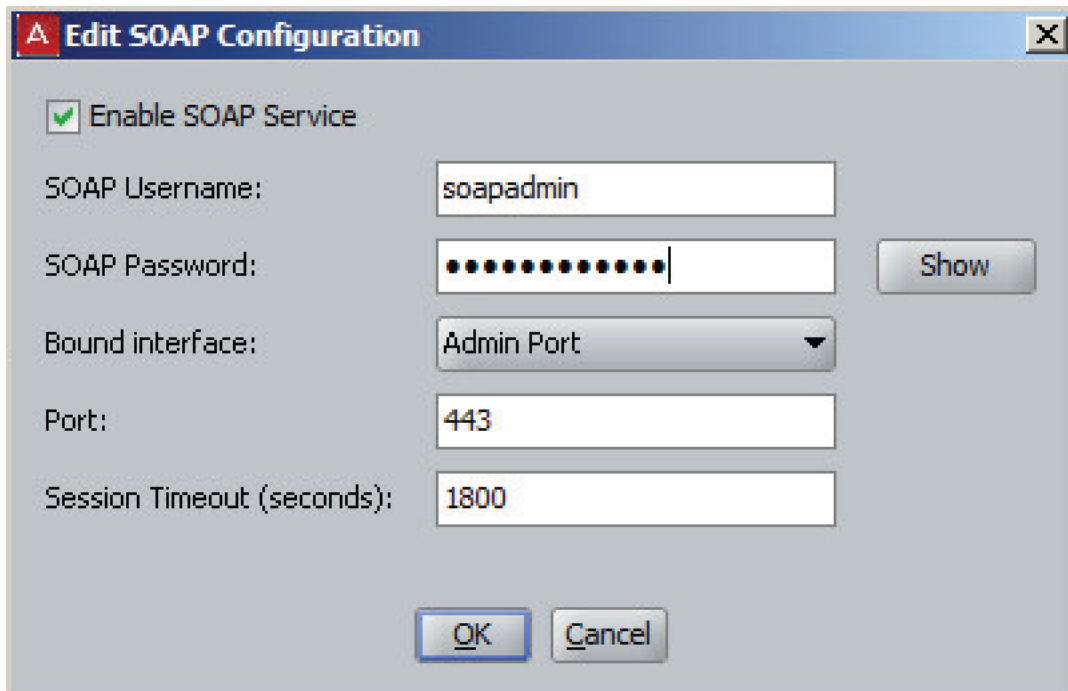
Step 5: Click the **Edit** button. The Edit SOAP Configuration appears.

Step 6: Select **Enable SOAP Service**.

Step 7: In the **SOAP Username box**, enter **soapadmin**.

Step 8: In the **SOAP Password box**, enter **soappassword**.

Step 9: In the **Bound interface** list, choose **Admin Port.**, and then click **OK**.



Step 10: In **Site Configuration > Directories > Virtual Mapping > Virtual Groups**, click **Actions > Add A New Virtual Group**.

Step 11: In the **Virtual Group Name** box, enter **Provisioners**, and then click **OK**.

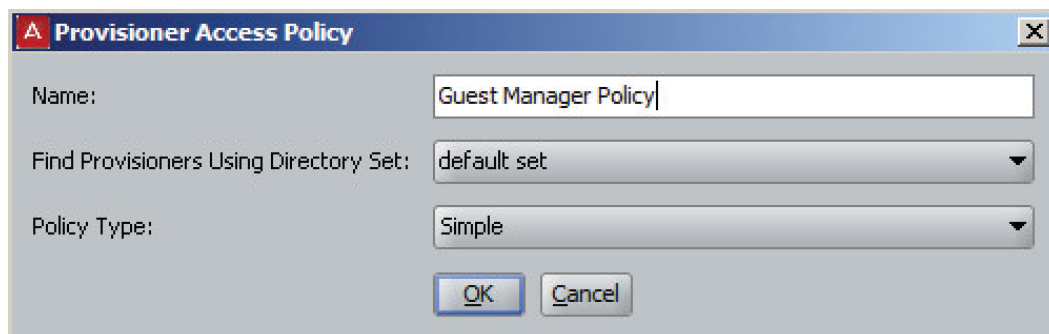
Step 12: Click **Add**. The Map Groups window appears.

Step 13: In the **Directory Service** list, choose **Active Directory**.

Step 14: Expand the Active Directory tree, select the **Guest Provisioner** group, and then click **OK**.

Step 15: In **Site Configuration > Guest Manager > Provisioner Access Policies**, click **New**.

Step 16: In the **Name** box, enter **Guest Manager Policy**, and then click **OK**.

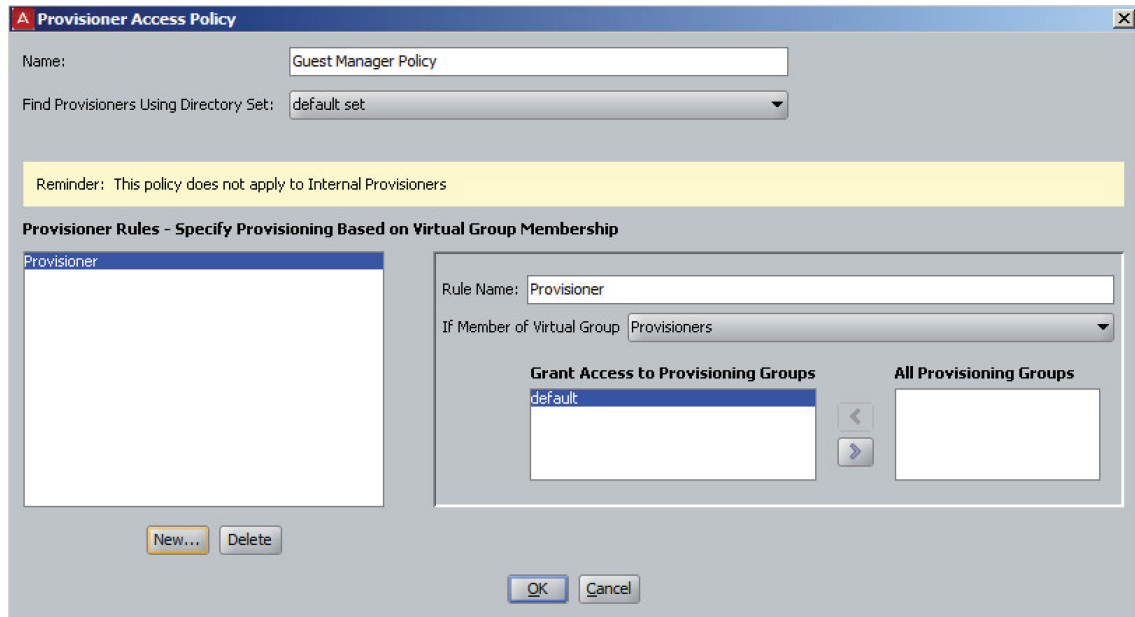


Step 17: Click **New**.

Step 18: In the **Rule Name** box, enter **Provisioner**, and then click **OK**.

Step 19: In the **If Member of Virtual Group** list, choose **Provisioners**.

Step 20: Click **default** and move it the **Grant Access to Provisioning groups** list, and then click **OK**.



Step 21: Click **OK**.

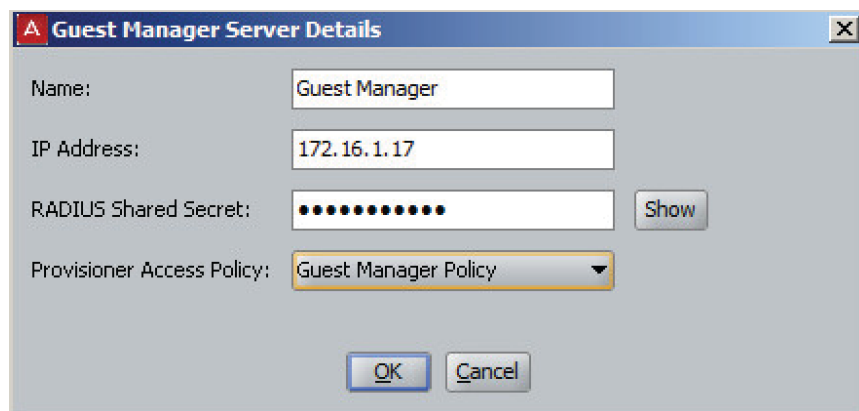
Step 22: In **Site Configuration > Guest Manager > Guest Manager Servers**, click **New**. The Guest Manager Server Details window appears.

Step 23: In the **Name** box, enter **Guest Manager**.

Step 24: In the **IP Address** box, enter **172.16.1.17**.

Step 25: In the **RADIUS Shared Secret** box, enter **examplesecret**.

Step 26: In the **Provisioner Access Policy** list, choose **Guest Manager Policy**, and then click **OK**.

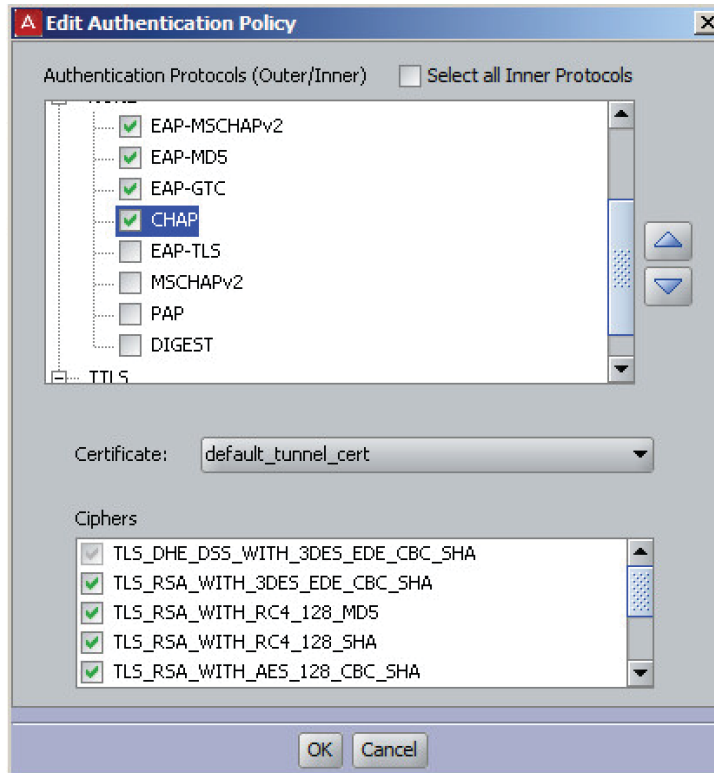


6.3 Update IDE Policy for Guests

Step 1: In **Site Configuration > Access Policies > RADIUS > wireless user**, click the **Authentication Policy** tab.

Step 2: Click **Edit**. The Edit Authentication Policy window appears.

Step 3: Select **CHAP**, and then click **OK**.



Step 4: Click the **Authorization Policy** tab.

Step 5: Click the **Edit** button to the right of **RADIUS Authorization Policy**. The Edit Authorization Policy window appears.

Step 6: Click **Add**. The New Rule window appears.

Step 7: In the **Name** box, enter **Guest**, and then click **OK**.

Step 8: Click **New**. The Constraint Details window appears.

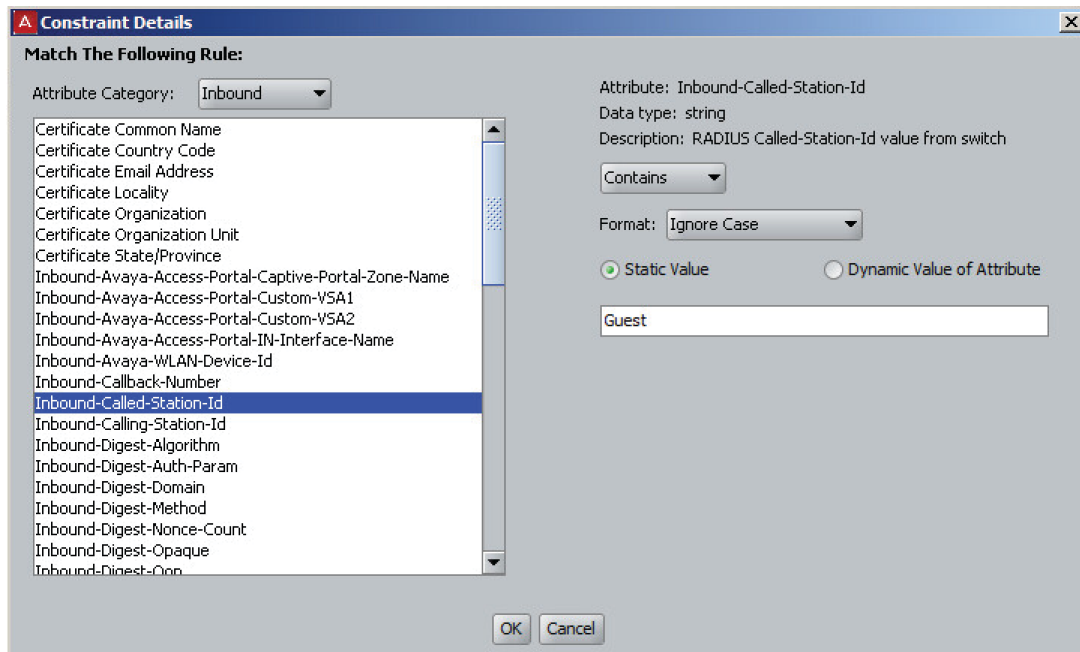
Step 9: In the **Attribute Category** list, choose **Inbound**.

Step 10: Select **Inbound-Called-Station-Id**.

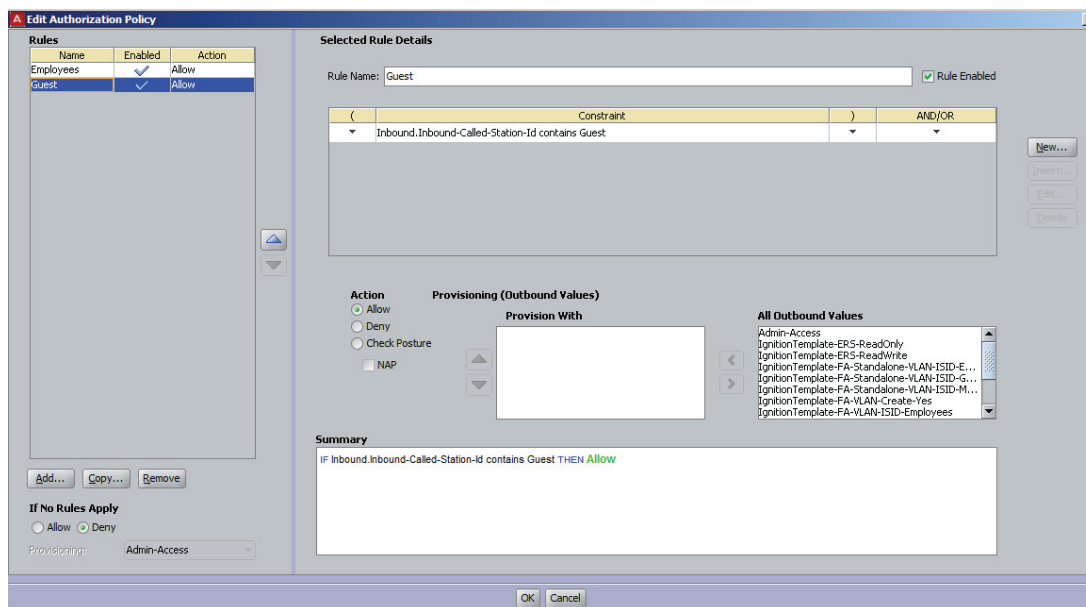
Step 11: Choose **Contains**.

Step 12: In the **Format** list, choose **Ignore Case**.

Step 13: In the box, enter **Guest**, and then click **OK**.



Step 14: For Action, select **Allow**, and then click **OK**.



6.4 Configure Guest Manager

Table 13 Configuration variables

Value	All aggregation switches
Ignition Guest Manager IP address	172.16.1.17
Ignition server IP address	172.16.1.16
SOAP username	soapadmin
SOAP password	soappassword
RADIUS shared secret	examplesecret
SMTP server	smtp.avaya.test

Step 1: Install Guest Manager on the VMWare.

Step 2: Login with a username and password of **admin**.

```
interface admin ipaddr 172.16.1.17/24
route add 0.0.0.0/0 172.16.1.1 admin
dns server primary 172.16.1.20
dns domain avaya.test
passwd
Password:
Reenter Password:
```

Step 3: Restart the virtual machine

```
reboot
```

Step 4: In the DNS server, set up a DNS record for the Guest Manager's IP address.

Step 5: Open the Guest Manager Administrator Application by browsing to <https://gm.avaya.test/GuestManager/admin/>

Step 6: Enter the Guest Manager login credentials (admin/admin), and then click **Login**.

Step 7: Click **Administration > Account**.

Step 8: Next to Administrator Password, click **Change**.

Step 9: In the **Current Password** box, enter **admin**.

Step 10: Enter and confirm the new password, **ExampleGMPassWord**, and then click **Submit**.

The screenshot shows a web form titled "Administrator Account". It contains the following fields and controls:

- Administrator User Name:**
- Administrator Password:** [Cancel](#)
- Current Password:**
- New Password:**
- Confirm Password:** (This field is highlighted with a blue border)
- Administrator Idle Timeout (min.):** (1 - 60)

At the bottom of the form are two buttons: **Submit** and **Reset**.

Step 11: Click **Administration > Connection > Appliance**.

Step 12: In the **IP Address** box, enter **172.16.1.16**.

Step 13: In the **User Name** box, enter **soapadmin**.

Step 14: In the **Password** box, enter **soappassword**, and then click **Connect**.

The screenshot shows a web form titled "Login to Appliance". It contains the following fields and controls:

- IP Address:**
- SOAP Port:**
- User Name:**
- Password:** (This field is highlighted with a blue border)

At the bottom of the form is a button: **Connect**.

Step 15: Click **Administration > Connection > RADIUS**.

Step 16: In the **Shared Secret** box, enter **examplesecret**, and then click **Submit**.

Step 17: Click **Administration > Notification > E-mail**.

Step 18: Select **Enable Sending of Email Notification**.

Step 19: In the **From Address** box enter **guestmanager@avaya.test**

Step 20: In the **SMTP Server** box, enter **smtp.avaya.test**.

Step 21: If your SMTP server requires authentication, then select the User Authentication check box and, in the SMTP Server User Name and Password fields, type the login credentials of the SMTP server user.

Step 22: Click **Submit**.

Email SMTP Configuration

Enable Sending of Email Notification

From Address:

Server:

Use SSL: Yes No

SSL Certificate: Custom System +

Port Number:

User Authentication

User Name:

Password: [Cancel](#)

New Password:

Confirm Password:

6.5 Create Guest User Accounts

Step 1: Open the Guest Manager Provisioner Application by browsing to <https://gm.avaya.test/GuestManager/>

Step 2: In the Login screen, enter your provisioner Username and Password.

Step 3: Click **Sign In**.

Step 4: Click the **Guest Users > New** button.

Next, in the Create Guest User screen, you provide the account details

Step 5: In the **Group Membership** list, choose the provisioning group to which this guest will belong. Each provisioning group imposes certain account guidelines (maximum validity period, allowable access zones, and so on), so the fields and defaults of the window may change after you choose a provisioning group.

Step 6: Type the user's **First Name** and **Last Name**. The window creates a default user name that you can edit. The user name must be unique before you can save the user.

Step 7: If you have login instructions for the user, type them in the **Comments** field. Later when you send the user a notification e-mail, or print the user's login information sheet, the comments will be included.

Step 8: Click **Submit**. The Guest Manager application creates the guest user account and e-mails notifications to the people you specified in the Send Notifications section.

Procedures

Deploying Campus Switches for Access Points

- 7.1 Add Wireless Networks to Campus Aggregation Block
- 7.2 Add Guest Network to Campus Aggregation and Data Center Devices
- 7.3 Configure Access Layer ERS 4800s

The switch configurations shown in this reference design build upon the information contained in the *Campus LAN Reference Design* and assume that the campus LAN and data center switches are already operational and configured with Avaya Fabric Connect between all aggregation and core devices.

7.1 Add Wireless Networks to Campus Aggregation Block

Configure two networks for wireless: one dedicated for the management interfaces of the access points in the campus, and the second for clients attached to the internal data wireless network. All access points within a campus aggregation block, regardless of the access layer closet to which they are attached, connect to the same network.

Access point management interfaces obtain IP addresses through DHCP. DHCP addressing allows for a quick deployment of the access points. Static IP addressing is not required, because the access point self-discovers WOS through a DNS lookup, and IDE uses the AP management network range to allow authentication.

Table 14 Configuration variables

Value	agg1-8200-1	agg2-8200-2
Management VLAN id	300	
Management VLAN name	WLAN-Mgmt	
Management VLAN IP address	172.16.1.1/24	172.16.1.2/24
Data VLAN id	301	
Data VLAN name	WLAN-Data	
Data VLAN IP address	172.16.3.1/23	172.16.3.2/23
DHCP server	172.16.1.20	

Step 1: On the first campus aggregation switch (agg1-8200-1), create the wireless VLANs.

```
vlan create 300 name WLAN-Mgmt type port-mstprstp 1
vlan create 301 name WLAN-Data type port-mstprstp 1
vlan i-sid 300 1000300
vlan i-sid 301 1000301
```

Step 2: Add an IP address to the VLAN interface and enable RSMLT for gateway redundancy.

```
interface Vlan 300
  ip address 172.16.1.1 255.255.255.0
  ip rsmlt
  ip rsmlt holdup-timer 9999
exit
interface Vlan 301
  ip address 172.16.3.1 255.255.254.0
  ip rsmlt
  ip rsmlt holdup-timer 9999
  ip dhcp-relay
  ip dhcp-relay fwd-path 172.16.1.20
  ip dhcp-relay fwd-path 172.16.1.20 enable
exit
```

Step 3: Configure the peer aggregation switch.

```
vlan create 300 name WLAN-Mgmt type port-mstprstp 1
vlan create 301 name WLAN-Data type port-mstprstp 1
vlan i-sid 300 1000300
vlan i-sid 301 1000301
interface Vlan 300
  ip address 172.16.1.2 255.255.255.0
  ip rsmlt
  ip rsmlt holdup-timer 9999
exit
interface Vlan 301
  ip address 172.16.3.2 255.255.254.0
  ip rsmlt
  ip rsmlt holdup-timer 9999
  ip dhcp-relay
  ip dhcp-relay fwd-path 172.16.1.20
  ip dhcp-relay fwd-path 172.16.1.20 enable
exit
```

Step 4: Repeat this procedure on each aggregation block in the campus. Keep the VLAN id the same at all aggregation blocks, but provide them with unique IP subnets.

7.2 Add Guest Network to Campus Aggregation and Data Center Devices

Configure one network for guest access that stretches across all aggregation blocks in the campus. All access points, regardless of the access layer closet to which they are attached, connect to the same network. The guest network stretches into the data center where the internet firewall's DMZ interface is connected to the guest network. The firewall serves as the default gateway for all clients in the guest network. Aggregation switches internal to the network must not be configured with an IP address on that VLAN.

Table 15 Configuration variables

Value	All aggregation switches
Guest VLAN id	303
Guest I-SID id	1000303
Guest VLAN name	WLAN-Guest
Access layer SMLT id	110
Firewall interface	10

Step 1: On the campus aggregation VSP 8200s, create a wireless management VLAN, map it to an I-SID, and assign it to the SMLT connected to the access layer device.

```
vlan create 303 name WLAN-Guest type port-mstprstp 1
vlan i-sid 303 1000303
vlan mlt 303 110
```

Step 2: Repeat this procedure on each aggregation block in the campus. Keep the VLAN id and I-SID.

Step 3: On the data center access layer VSP 7000, which runs SPB, connect the firewall to the guest network.

```
vlan create 303 name WLAN-Guest type port
vlan i-sid 303 1000303
vlan members add 303 10
```

7.3 Configure Access Layer ERS 4800s

The Avaya ERS 4850 series switch is used in the access layer to provide edge services to clients and access points. It provides the access points power through IEEE 802.3at PoE+.

Table 16 Configuration variables

Value	All aggregation switches
Access point interfaces	1/48, 2/48
Uplink MLT interfaces	1/50,3/50
Wired data VLAN id	16

Step 1: On the access layer switch, create the wireless VLANs

```
vlan create 300 name WLAN-Mgmt type port
vlan create 301 name WLAN-Data type port
vlan create 303 name WLAN-Guest type port
```

Step 2: Assign the VLANs to the interface connected to the access point and to the uplink interfaces.

```
vlan ports 1/48 tagging untagPvidOnly pvid 300
vlan ports 2/48 tagging untagPvidOnly pvid 300
vlan member add 300 1/48,2/48,1/50,3/50
vlan member add 301 1/48,2/48,1/50,3/50
vlan member add 303 1/48,2/48,1/50,3/50
```

Step 3: If support for Bonjour forwarding is required on wired networks, add those VLANs to the access point interface as well.

```
vlan member add 16 1/48,2/48
```

Step 4: Repeat this procedure on each access switch with access points attached in the campus.

Procedures

Deploying Different Security Policies on the Same SSID

- 8.1 Create a Filter to Limit Access to Internal Devices
- 8.2 Create the Contractors Group
- 8.3 Assign the Outbound Values

8.1 Create a Filter to Limit Access to Internal Devices

Step 1: In **Configure > Access Point Configuration > Profiles**, click **Default_Profile**.

Step 2: Click the **Configuration** tab.

Step 3: In **Filters > Filter Lists**, click **Add**.

Step 4: In the **Filter List Name** box, enter **Contractors**.

Step 5: Select **Filter List Enabled**, and then click **OK**.

First, allow contractors to reach their internal server

Step 6: In **Filters > Filter Management**, in the **Filter List** list, choose **Contractors**.

Step 7: Click **Add**. The New Filter window appears.

Step 8: In the **Filter Name** box, enter **Internal Server**.

New Filter

Filter List Name

Filter Name

Layer

Enable

Type

Traffic Limit Type

Traffic Limit

Protocol

Port

Source Not

Destination Not

IP

Mask

DSCP

QoS

VLAN

Application Control

Category Application

Filter Log

OK Cancel

Step 9: In the **Layer** list, choose **Layer 3**.

Step 10: Select **Enable**.

Step 11: In the **Destination** list, choose **IP Address**.

Step 12: In the **IP** box, enter **172.16.3.100**, and then click **OK**.

Next, block contractors from reaching other internal devices.

Step 13: In **Filters > Filter Management**, in the **Filter List** list, choose **Contractors**.

Step 14: Click **Add**. The New Filter window appears.

Step 15: In the **Filter Name** box, enter **Deny Internal**.

New Filter

Filter List Name

Filter Name

Layer

Enable

Type

Traffic Limit Type

Traffic Limit

Protocol

Port

Source Not

Destination Not

IP

Mask

DSCP

QoS

VLAN

Application Control

Category Application

Filter Log

Step 16: In the **Layer** list, choose **Layer 3**.

Step 17: Select **Enable**.

Step 18: In the **Type** list, choose **Deny**.

Step 19: In the **Destination** list, choose **IP Address**.

Step 20: In the **IP** box, enter **172.16.4.0**.

Step 21: In the **Mask** box, enter **255.255.255.0**, and then click **OK**.

8.2 Create the Contractors Group

Step 1: In **Groups > Group Management**, click **Add**.

Step 2: Select **Enabled**.

Add User Group

Settings

Enabled:

Name:

RADIUS ID:

Device ID:

Vlan Name: Vlan Number:

QoS:

Filter:

Avaya Roaming:

Fallback:

Captive Portal:

Limits

Stations:

Traffic: Packets/Sec Unlimited

Kbps Unlimited

Traffic per Station: Packets/Sec Unlimited

Kbps Unlimited

Days Active: Everyday Sun Mon Tue Wed Thu Fri Sat

Time Active: Always Time On: Time Off:

OK Cancel

Step 3: In the **Name** box, enter **Contractors**.

Step 4: In the **RADIUS ID** box, enter **Contractor Group**.

Step 5: In the **QoS** list, choose **0**.

Step 6: In the **Filter** list, choose **Contractors**, and then click **OK**.

Step 7: Click **Apply Config**.

8.3 Assign the Outbound Values

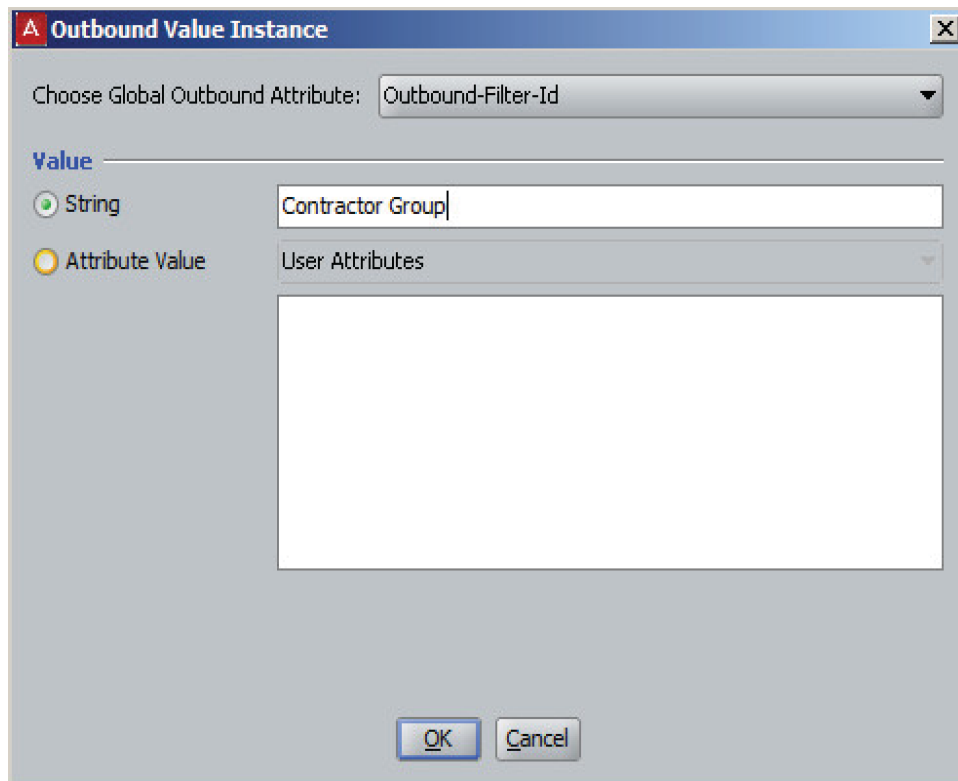
Step 1: In **Example Organization > Site Configuration > Provisioning > RADIUS > Outbound Values**, click **New**.

Step 2: In the **Outbound Value Name** box, enter **Contractors**.

Step 3: Click **New**. The Outbound Value Instance window appears.

Step 4: In the **Global Outbound Attribute** list, choose **Outbound-Filter-Id**.

Step 5: In the **String** box, enter **Contractor Group**, and then click **OK**.



Step 6: Click **OK**.

Step 7: In **Site Configuration > Directories > Virtual Mapping > Virtual Groups**, click **Actions > Add A New Virtual Group**. The Add Virtual Group window appears.

Step 8: In the **Virtual Group Name** box, enter **Contractors**, and then click **OK**.

Step 9: Click **Add**. The Map Groups window appears.

Step 10: In the **Directory Service** list, choose **Active Directory**.

Step 11: Expand the Active Directory tree, select the **Contractors** group, and then click **OK**.

Step 12: In **Site Configuration > Access Policies > RADIUS > wireless user**, click the **Authorization Policy** tab.

Step 13: Click the **Edit** button to the right of **RADIUS Authorization Policy**. The Edit Authorization Policy window appears.

Step 14: Click **Add**. The New Rule window appears.

Step 15: In the **Name** box, enter **Contractors**, and then click **OK**.

Step 16: Click **New**. The Constraint Details window appears.

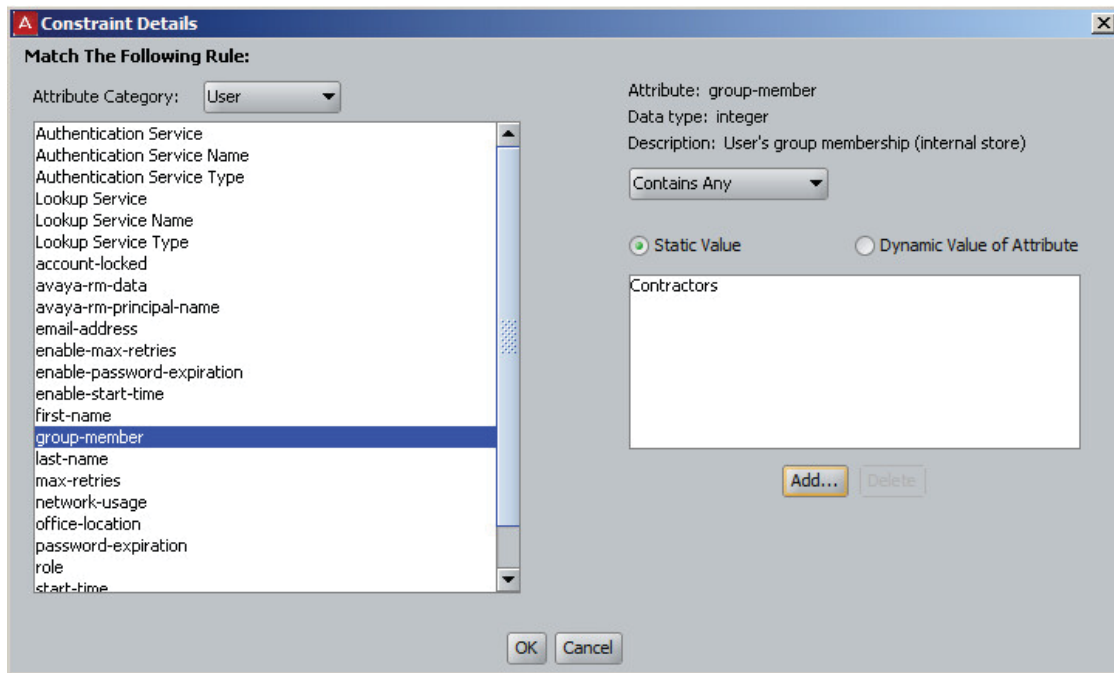
Step 17: In the **Attribute Category** list, choose **User**.

Step 18: Select **group-member**.

Step 19: Click **Add**. The Add Value window appears.

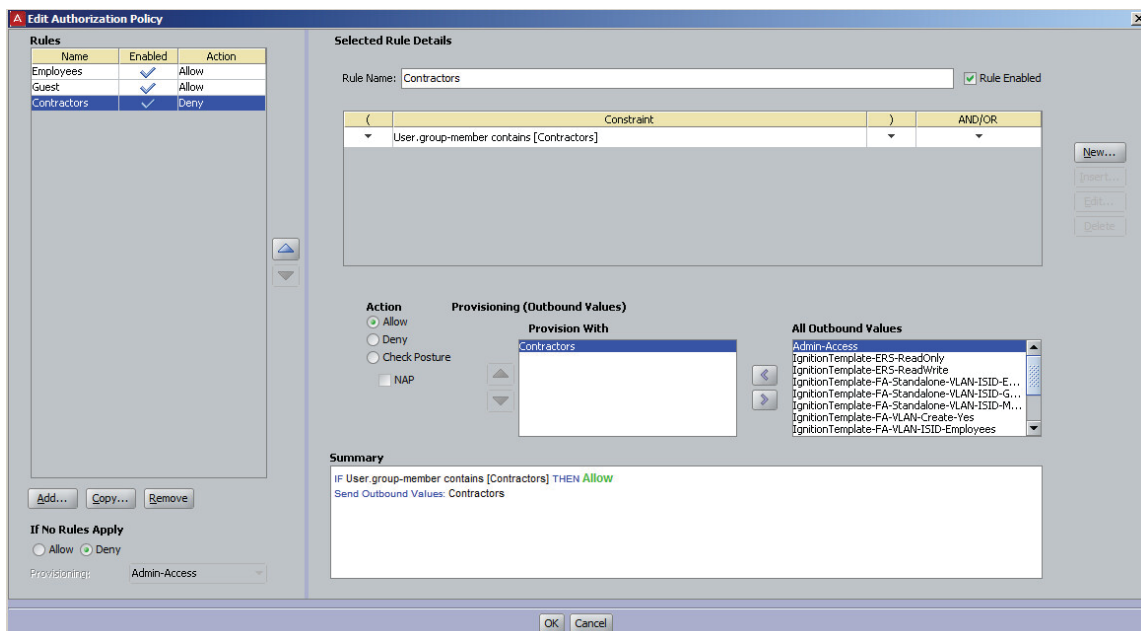
Step 20: In the **Add Group** list, choose **Contractors**, and then click **OK**.

Step 21: Click **OK**.



Step 22: For Action, select **Allow**.

Step 23: Move **Contractors** from **All Outbound Values** to **Provision With**, and then click **OK**.



Glossary

AAA server authentication, authorization, and accounting server

AP access point

DPI deep packet inspection

EAP extensible authentication protocols

LAN local area network

NTP network time protocol

PKI public key infrastructure

RF radio frequency

SMTP simple mail transfer protocol

TLS transport layer security

vLAN virtual local area network

WLAN wireless local area network

WOS wireless local area network orchestration system



[Send us](#) your comments and suggestions.

© 2016 AVAYA All Rights Reserved.

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation 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 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.