

Ignition Server Ignition Guest Management Wireless LAN 8100

Engineering

 Ignition Guest Management for Wireless LAN 8100 Technical Configuration Guide

Avaya Data Solutions Document Date: July 2011 Document Number: NN48500-615 Document Version: 1.1



© 2011 Avaya Inc. All Rights Reserved.

Notices

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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 Web sites referenced within this site or documentation(s) 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 this product. 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 Web site: http://www.avaya.com/support Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER, AND 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").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) 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. 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.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

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

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support.



Abstract

This Technical Configuration Guide outlines the configuration steps required to create an authenticated network infrastructure for wireless guest users. The main components include the Avaya Wireless LAN 8100, access control provided by the Avaya Ignition Server and guest user provisioning provided by the Ignition Guest Manager.

The audience for this Technical Configuration Guide is intended to be Avaya Sales teams, Partner Sales teams and end-user customers.

Revision Control

No	Date	Version	Revised By	Remarks
1	17 Dec 2010	1.0	KLM	Initial Draft
2	5 July 2011	1.1	KLM	Minor Correction in Section 2.3.1.1



Table of Contents

Figu	res		5
Tabl	es		5
Conv	ventic	ons	6
1.	Over	rview	7
1.	1	Solution Components	8
1.	2	Hardware & Software	9
2.	Conf	iguration Example	11
2.	1	Ignition Server	11
	2.1.1	Ignition Server Login	11
	2.1.2	Licenses	13
	2.1.3	Directory Sets	15
	2.1.4	Groups	18
	2.1.5	Access Policies	20
	2.1.6	Authenticators	31
	2.1.7	Guest Manager	34
2.	2	Ignition Guest Manager	56
	2.2.1	Ignition Guest Manager Login	56
	2.2.2	Basic Administration	57
	2.2.3	Connections	58
	2.2.4	Provisioning Groups	60
	2.2.5	Internal Provisioners	67
2.	3	Wireless LAN 8180 Controller	70
	2.3.1	Preliminary Configuration	70
	2.3.2	Captive Portal	74
	2.3.3	RADIUS Profiles	76
	2.3.4	Network Profiles	77
	2.3.5	AP Profiles	78
2.	4	Verification	80
	2.4.1	Internal Provisioners Authentication	80
	2.4.2	External Provisioners Authentication	82
	2.4.3	Captive Portal Authentication	84
3.	Refe	Prence Documentation	88



Figures

Figure 1.0 – Avaya Wireless Guest Management Solution	7
Figure 1.1 – Topology	9
Figure 2.1.3.1 – Directory Set	
Figure 2.1.4.1 – Internal Groups	
Figure 2.1.5.1 – Access Policy	
Figure 2.1.6.1 – Access Policy	
Figure 2.1.7.1.1 – SOAP Service	
Figure 2.1.7.2.1 – Guest Manager Server	
Figure 2.1.7.3 – External Provisioners	
Figure 2.2.5 – Provisioning Groups	60

Tables

Table 1.1 – Hardware and Software1	10
------------------------------------	----

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols



Tip – Highlights a configuration or technical tip.



Note - Highlights important information to the reader.



Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# show running-config

Output examples from Avaya devices are displayed in a Lucida Console font:

```
ERS5520-48T# show sys-info
```

Operation Mode:	Switch
MAC Address:	00-12-83-93-в0-00
POE Module FW:	6370.4
Reset Count:	83
Last Reset Type:	Management Factory Reset
Power Status:	Primary Power
Autotopology:	Enabled
Pluggable Port 45:	None
Pluggable Port 46:	None
Pluggable Port 47:	None
Pluggable Port 48:	None
Base Unit Selection:	Non-base unit using rear-panel switch
sysDescr:	Ethernet Routing Switch 5520-48T-PWR
	HW:02 FW:6.0.0.10 SW:v6.2.0.009
	Mfg Date:12042004 HW Dev:H/W rev.02

ΑνΑγ

1. Overview

Guest access is one of the most pervasive applications of wireless networking and most wireless infrastructure vendors offer guest access features. However most wireless guest access solutions are impractical as they either require dedicated resources such as front desk personnel or IT helpdesk staff to provision accounts or require privileged access into the infrastructure devices opening the core network to potential security risks.

To eliminate the management overhead many enterprises deploy 24x7 open networks which are susceptible to abuse or authenticated networks with fixed credentials which over time are shared and diluted. Neither approach is optimal or recommended as they provide no means of identifying the end-user nor do they provide the means of offering tier services to differing classes of users.

The Avaya guest management solution outlined in this guide provides enterprises with an easy to deploy and manage suite of products and applications that allows:

- 1) Authenticated wireless access using a captive-portal for guest users or temporary staff using notebook PCs, tablets, PDAs or smart phones.
- 2) Simplified guest user provisioning by corporate end-users (sponsors) which offloads the task of creating and managing guest user accounts from front-desk personnel or IT staff.
- Ability assign specific network access or restrictions based different guest user classes such as visitors, contractors or temporary employees.



Figure 1.0 – Avaya Wireless Guest Management Solution

AVAYA

1.1 Solution Components

The Avaya wireless guest management solution consists of the following software and hardware components:

- 1. Configuration and Management:
 - Ignition Dashboard Application A Windows based application used to configure and manage the Ignition Server that provides RADIUS authentication, authorization and accounting.
 - Guest Manager Administrator Application A web-based application for administrators to manage provisioner users, templates and optionally perform bulk updates for guest users.
 - Guest Manager Provisioner Application A web-based application for corporate end-users (sponsors) to create and manage guest user accounts without IT or front-desk personnel intervention.
- 2. Access Control:
 - *Ignition Server* Authenticates and authorizes guest users who wish to connect to the network and captures accounting information.
 - Optional External User Directory Active Directory or LDAP user store which can be queried by the Ignition Server to authenticate and authorize corporate end-users who wish to create guest user accounts.
- 3. Authenticator:
 - Avaya Wireless LAN 8100 Provides captive-portal authentication for the guest users which is authenticated using RADIUS against the Ignition Server where the guest user accounts reside.



1.2 Hardware & Software

The following diagram depicts the hardware and software components and the topology used to create this guide:





The following table highlights the hardware and software outlined above used to create this guide:

Hardware and Software Components

Dell PowerEdge D610 Server – VMWare ESXi Version 4.1.0:

- Avaya Ignition Server Version 07.00.00.020468
- Microsoft Windows Server 2003 Enterprise Edition with Service Pack 2:
 - Avaya Ignition Guest Manager Version 07.00.00.020468
- Microsoft Windows Server 2003 Enterprise Edition with Service Pack 2:
 - Active Directory Services
 - o DNS Services

Avaya Secure Router 2330 – Version 10.3

Avaya Ethernet Routing Switch 5520-48T-PWR - Version 6.2.0.009

Avaya WLAN 8100 Series – Version 1.0.1.007

- 1 x WLAN Controller 8180
- 3 x WLAN Access Point 8120

IBM Thinkpad T60 – Windows 7 Enterprise:

- Java Runtime Version 6 Update 20 (Standard Edition)
- Ignition Dashboard Version 7.0
- Mozilla Firefox Version 3.6.10
- Internet Explorer Version 8.0

Table 1.1 – Hardware and Software



2. Configuration Example

2.1 Ignition Server

The following sections outline the configuration steps required to configure the Avaya Ignition Server for Guest Access:

2.1.1 Ignition Server Login

The Avaya Ignition Server is configured using an Ignition Dashboard application that is installed on a Windows PC. The Ignition Dashboard can communicate with the Ignition Server using an IP Address assigned to the *Admin Port* (default) or *Service Port* (optional). All configuration & management tasks are performed using this application.

To use the Ignition Dashboard application the Ignition Server must be pre-configured with an IP address, subnet mask and default route. If IP addressing has not been defined on the Ignition Server, please follow the configuration steps provided in the *Avaya Identity Engines Ignition Server Getting Started* guide which is available on the Avaya support site http://support.avaya.com.

To access and login to the Ignition Server using the Ignition Dashboard:

1 Launch the *Ignition Dashboard* application then enter the administrative *Username* and *Password*. In the Connect To field enter the *IP address* assigned to the *Admin Port* or *Service Port* then click *OK*:

Administration Help	
🏶 Configuration 📓 Monitor 🗙 Insubleshoot	
Login User Name: Password: Connect To: 192108.10.52 Connect To: 192108.10.52	
	707



The default username and password for the Ignition Server is admin / admin.

2 A Site Configuration window with the recommended configuration sequence will be displayed:



You may click on each heading in the Site Configuration window to quickly configure each component.



2.1.2 Licenses

The Ignition Server ships without any licenses pre-installed. To provide guest services the Ignition Server will require a *Base License* as well as a *Guest Manager License*. Other licenses such as *Posture License*, *TACACS+ License*, and *Ignition Reports License* may also be installed but are not required for guest services.



1

Evaluation licenses for the Ignition Server can be obtained from the main Avaya Site by visiting <u>http://www.avaya.com/usa/product/identity-engines-portfolio</u>.

To verify or install a Base License and Guest Manager License on Ignition Server:

Within the *Ignition Dashboard* select *Configuration* > *Site-Name* > *Licenses*. This will display all the purchased or evaluation licenses that have been installed on the Ignition Server:





2 To install a Base License or Guest Manager License on the Ignition Server:

- 1) Select *Browse* and select the path and filename of the license file to install. This will install all the evaluation or purchased licenses at one time.
- 2) Alternatively copy the license key to the Windows clipboard then select *Paste*. This will install one evaluation or purchased license at a time.

Click *OK* when completed:

License to Install:	License to Install:
BASE LICENSE	BEGIN IGNITION LICENSE CERTIFICATE MIIBOQTBS#CBLAIBABMbOXZheWEGSW55jLiwgU2PidG5gQ2xhcmEsfENBEwUzNDU2 NxIONjAxMDEXM2xNzQ5NDeTCKF2YXLhIExhYnMTC02FQVRVUkVfSUFSEg4yMDEw MTExhDaxMDExM5XNTExM2xMDAxMDACAQATES9u2S92XWFyIGxpY2Vuc2Uw DRILNTMxNDA2NjgyNjkKAQAEggEAXryMSI29EqQppfBlIcMFj0KqD2a0VcpiFN+2
MIIBogIBBSCBIQIBABNDOXZheWEgEWSJLzwgUZFUdEEgGZzhemEsIENBEWUZND U2 NAIONJAMNDEXMEAXNZQZNTATCKF2YX1hIExhYnMTDZZFQUWUUKY60kFTRRIOMJ Ax MDEXMEANMDAMDASDjIWHTEXHTMvMDAWDAXAgEAExBFbmUgWWVhciBsaWN1bn N1 MAOSCSUZMDQwNjY4MjYSCgEABIIBACZJcuLtxuW/Kt4U9FCalwn/AS77Xmbdt9 Vn	7ESdirUVic2N293/JTYVeHDDNSN12geU05Ds02ddmL2VbC/2UVgAgosTkJEWY8V SwCuMfrfmth/CGgloID1956dHTFOHTVUWuUUUSEseTSh62V35GQLNAWBqv2Ou 10Cb3rceqHCNaIfhBHIyjmFd2CLVu/pykJ6uWPyCCFJLF1Su5mgkHRbv4Tn3v8yo bJr1ozPnAitXyUGf2C6bj5KAhGCF2EfKUmMSg4VKpAjvngLGVq0Q91GK17320UiC glav189xAcMaIudpX0WIX5BgH74009/085Zn8UVbbH2XVNg== END IGNITION LICENSE CERTIFICATE Paste Browse.
Ty: Paste the license text into the above text area or use the Browse button to read in a license file.	Tip: Paste the license text into the above text area or use the Browse button to read in a license file.

3 The following shows an Ignition Server with the Base License and Guest Manager License installed:

ervices	Licenses	Certificates	Logging	Scheduled Backups	
icenses: Decelies				License Details:	
Guest Ma	inager			Select a license to view it's detail information.	
Ignition F NAP Post	ceports cure				
TACACS: TNC Post	+ :ure				
Ir	stall Ev	nort All	lete	Conv to Clinhoard	
1					



2.1.3 Directory Sets

Directory sets are an ordered list of user lookup services used by the Ignition Server when it processes an authentication request. The directory set determines where the user account information is located (i.e. local, Active Directory, LDAP etc.), which service is used to retrieve the user's account information, and which service is used to retrieve authorization data such as attributes and group membership.

When a guest user account is added by the Ignition Guest Manager, it is created in the internal store (local database) on the Ignition Server. To be able to authenticate guest users form the internal store, a directory set and identity routing policy must be created.

2.1.3.1 Configuration Steps

For this configuration step a directory set named *Internal* will be created that will authenticate guest users against the *Internal User Store*:



Figure 2.1.3.1 – Directory Set



1 Within the Ignition Dashboard select Configuration > Site Configuration > Directories > Directory Sets. Right click on Directory Sets then select New:

<u>A</u> dministration <u>H</u> elp		
Configuration Monitor 💥	Iroubleshoot	
Configuration	Current Site: Site 0	_
🖃 🚭 Site 0	Directory Sets	
🛁 ide.avayalabs.local	Name	
🖻 👑 Site Configuration	default set	
Access Policies		
Authenticators		
Directories		
🕀 🔊 Directory		
🕀 🔊 Internal Store		
🛓 🧩 Virtual Mapping		
🕀 🌌 Provisioning		
🗄 🍈 Guest Manager		
00000	New Edit Delete	
200000		

2 In the *Directory Set* window provide enter the name *Internal*. Click *Add*:

ory Set Entries				
User Lookup Service	Authentication Service	Fallthrough if Unable to Connect	Fallthrough if User Not Found	Fallthrough if Authentication Failed
		Add		



3 In the *Directory Set Entry* window set the *Lookup Service* and *Authentication Services* to *Internal User Store*. Click *OK*:

i Please select a directo	ry service and an authentication server for the directory set entry.	
User Lookup Service: Authentication Service:	Internal User Store 💌	
	<u>OK</u> <u>C</u> ancel	

4 A Directory Set Entry named Internal has now been created. Click OK:

Name: Internal					
Directory Set Entries					
User Lookup	Authentication	Fallthrough if	Fallthrough if	Fallthrough if	
Internal User Store	Internal User Store				
		<u>A</u> dd			
		OK Creat			

AVAYA

2.1.4 Groups

Each guest user account is assigned to an internal group in the internal store on the Ignition Server. Groups allow the Ignition Server to differentiate between different classes of guest users then apply different network permissions such as to authenticated sessions such as time-of-day, day-of-week or bandwidth restrictions.

2.1.4.1 Configuration Steps

For this configuration step two internal groups named **Contractors** and **Visitors** will be created. Both groups will have **Type** set to **accessType** which will display groups in Ignition Server Guest Manager Application allowing them to be assigned to provisioning groups:



Figure 2.1.4.1 – Internal Groups



1 Within the Ignition Dashboard select Configuration > Site Configuration > Directories > Directory Sets > Internal Groups. Right click on default then then select Add A New Internal Group:

<u>A</u> dministration <u>H</u> elp		
🖄 Configuration 🛃 Monitor 💥 Ir	oubleshoot	
Configuration	Current Site: Site 0	
Configuration Site 0 Site Configuration Configuration Site Configuration Configuration Site Configuration Configuration Site Configuration Configuration Site Configuration Configuration Site Configuration Configuration Site Configuration Configur	Current Site: Site 0 Internal Groups Actions	Internal Group Details re: default e: sers Devices Internal User Na First Name Last Name Account Disabled Pending/Expired New Add Existing Edt Pernove Refresh
	<u>ب</u>	,, ====

2 Enter the *Internal Group* name *Visitors* then set the group *Type* to *accessType*. Check the option *Automatically create a virtual group for this internal group* then click *OK*. Repeat for a second group called *Contractors*:

Parent internal group: default		Parent internal group:	default	
Internal Group Name: Visitors		Internal Group Name:	Contractors	
Type:		Туре:	accessType	
Automatically create a virtual group for this internal group		Automatically creat	te a virtual group for this internal group	
OK Cancel			<u>O</u> K <u>C</u> ancel	
	-			_



2.1.5 Access Policies

Access policies are a set of rules that governs user authentication, authentication protocol support, the search order for user lookups, session authorization and provisioning. Access policies control how users are permitted to use the network as well as how the authentication transaction is performed.

2.1.5.1 Configuration Steps

For this configuration step:

- 1) An access policy named *Internal* will be created with *PAP* support with a routing policy mapped to the directory set named *Internal* created in section 2.1.3.
- An authorization policy will be created for the group named *Visitors* which only permits access Monday – Friday from 8:00AM → 5:00PM.
- 3) An authorization policy will be created for the group named *Contractors* with no restrictions.



Figure 2.1.5.1 – Access Policy



1 Within the Ignition Dashboard select Configuration > Site Configuration > Access Policies. Right click on RADIUS then click New Access Policy:

<u>A</u> dministration <u>H</u> elp	
🐞 Configuration 🛃 Monitor 💥 I	roubleshoot
Configuration	Current Site: Site 0
⊡🕶 Site 0	Access Policies
🛁 ide.avayalabs.local	Access Policy Names
🖻 👘 Site Configuration	default-radius-user
Access Policies	Policy
Autrenticators	
🖶 🌌 Provisioning	
🗄 🍓 Guest Manager	
	New

2 Set the Access Policy Name to Internal then click OK.

Access Policy Name:
Internal
<u>OK</u>

avaya.com



3 In the Access Policies window, right click on the new access policy then select Edit:

Configuration Current Site: Site 0 Access Policies Current Site: Site 0 Access Policies Current Site: Site 0 Access Policies Current Site: Site 0 Access Policy Current Site: Site 0 Access Pol	<u>A</u> dministration <u>H</u> elp	
Configuration Current Site: Site 0 Access Policies Access Policies Access Policies Access Policy Access Policies Access Policy Box Access Rename Directories Directories Directories Directories Box Access Delete	🔨 Configuration 🛃 Monitor 💥 I	roubleshoot
Access Policy Names detausystabs.local Access Policy Names default-radius-user Marchards Marchards Marchards Marchards Directories Provisioning Guest Manager Access Policy Names default-radius-user New Access Policy Names default-radius-user Delete Delete New Rename Edit Delete	Configuration	Current Site: Site 0
	Site 0 Configuration	Access Policies Access Policy Names default-radius-user Internal Rename Edit Delete New Rename Edit Delete

4 In the *Authentication Policy* window check *NONE/PAP* to enable PAP protocol support then click *Next*:

Authentication Policy	Authentication Policy i Indicate which inner/outer protocols will be supported in this Access Policy
Access Policy Summary	
	Authentication Protocols (Outer/Inner)
	P PEAP
	EAP-MSCHAPv2
	EAP-GTC
	EAP-TLS
	EAP-MSCHAPv2
	An Alfondaria - Alfondaria Interior
	Certificate: Ide.avayalabs.local
	Cinhers
	✓ TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_RC4_128_MD5
	✓ TLS_RSA_WITH_RC4_128_SHA
	▼ ILS_KSA_WITH_AES_IZ8_UBU_SHA
	Back Rext Finish Cancel



 Authentication Policy Identity Routing Policy Access Policy Summary 	Identity Routing Policy i You can setup authenticator container o selection, or you can simply use the defa Realm-Directory Set Mapping ✓ Enable Default Directory Set Directory Set: Internal	r realm-based rules for Directory S ult Directory Set	et	-
	Authenticator Container	Realm	Directory Set	
	New	Lung Edit Delete		
	Back Next	Finish Cancel		

6 The Access Policy Summary window will be displayed. Check the option Edit Authorization Policy When Wizard is Complete then click Finish:

 ✓ Authentication Policy ✓ Identity Routing Policy ✓ Access Policy Summary 	Access Policy Summary i The Access Policy will be updated with the for	ollowing settings.	_	
 Access Folicy summary 	Access Policy Name: Internal Authentication Policy NONE: PAP			
	Identity Routing			
	Default Directory Set: Internal			
	Authenticator Container	Realm	Directory Set	
	Edit Authorization Policy When Wizard is C	omplete		
	Back Next F	Finish Cancel		



In the Edit Authorization Policy window click Ad	k Add:
--	--------

1	Name Enab	ed Actio	on					
				Rule Name:			Rule Enabled	
				(Const	raint)	AND/OR	
				Action				
				Check Posture				
				NAP				
				Summary				
<u>A</u> dd	. <u>С</u> ору							
If No I	Rules Apply							
Brossie	iow 💿 Deny	oin-Access						
	Aur	Access						

8 Set the *Name* to *Visitors* then click *OK*:

Name:		
Visitors		
C	ОК	Cancel



9 Set the Action to Allow then click New:

Rules	Selected Rule Details				
Visitors Contraction	Rule Name: Visitors			Rule Enabled	
	(Constraint)	AND/OR	
					New
	Action Provisioning (Outbou	nd Values) Provision With	All Outbound Yalu	er.	
	O Deny O Check Posture		Admin-Access NAS-Prompt Sassion-Timeout	▲ 	
	TNC NAP	>	vlan40 vlan50 vlan70		
	Summary				
Add Copy Remove	IF THEN Allow				
If No Rules Apply Allow O Deny					
Provisioning: Admin-Access 👻					
	OK Cancel				

10 In the Constraint Details window set the Attribute Category to Authenticator. Select the attribute named Authenticator Type then set the value to Wireless. Click OK.

This will create an authorization rule that permits access if the authentication request originates from a *Wireless* device:

Match The Following Rule:		
Attribute Category: Authenticator Authenticator Authenticator Container Authenticator Device Template Authenticator Device Template Name	Attribute: Authenticato Data type: integer Description: Purpose lal Equal To	r Type bel for sub/authenticator in Ignition
Authenticator Name Authenticator Type	 Static Value 	O Dynamic Value of Attribute
Sub Authenticator Sub Authenticator Name Vendor Vendor Name	Wireless	
	OK Cancel	



11 Click New to create an additional rule. In the Constraint Details window set the Attribute Category to User. Select the attribute named group-member then set the match condition to Exactly Matches. Click Add then select the group named Visitors. Click OK:

This will create an authorization rule that permits access if the authenticating user is a member of the *Visitors* group:

terrore excelority	Data type: integer
Authentication Service	 Description: User's group membership (internal store)
Authentication Service Name	
Authentication Service Type	Exactly Matches 🔫
Lookup Service	
Lookup Service Name	
Lookup Service Type	Static Value Opynamic Value of Attribute
account-locked	Visitors
email-address	VISICOIS
enable-max-retries	600
enable-password-expiration	
enable-start-time	
first-name	
group-member	
last-name	
max-retries	
network-usage	Add Delete
office-location	
password-expiration	
role	
start-time	

12 Click *New* to create an additional rule. In the *Constraint Details* window set the *Attribute Category* to *System*. Select the attribute named *Time* then set the match condition to *Between*. Select the start time value *08:00:00* and the end time value *17:00:00*. Set the appropriate timezone then click *OK*.

This will create an authorization rule that permits access if the authentication request is received between 08:00AM \rightarrow 05:00PM:

Attribute Category: System Date Date and Time Falce Time	Data type: time Description: Current Ignition Server time Between
True Weekday	Static Value Dynamic Value of Attribute U8:00:00 America/New_York



13 Click New to create an additional rule. In the Constraint Details window set the Attribute Category to System. Select the attribute named Weekday then set the match condition to Week Day is Between. Select the start time day Monday and the end day Friday. Set the appropriate timezone then click OK.

This will create an authorization rule that permits access if the authentication request is received on Monday \rightarrow Friday:

Match The Following Rule:	
Attribute Category: System Date Date and Time False Time	Attribute: Weekday Data type: date Description: Weekday of Ignition Server Week Day is Between 💌
True Weekday	Static Value Opynamic Value of Attribute
	Monday 🔹 and Friday 🔹 America/New_York 🔹
O	Cancel

14 In the *Edit Authorization Policy* window click *Add* to create a new *Authorization Policy*:

Rules	Selected Rule Details			
Visitors Allow	Rule Name: Visitors		Rule Enabled	
Name Enabled Action Visitors Allow	Kule Name: Visitors (Constraint ((' Authenticator.Authenticator Type = Wireless User.group-member exactly matches [Visitors] System.Time between 8:00 AM and 5:00 PM System.Time between 8:00 AM and 5:00 PM Week day is between Monday and Friday Week day is between Monday and Friday Oneny Check Posture TNC NAP Summary (f (Authenticator.Authenticator Type = Wireless AND User non-member exactly matches Distors) \ AND	stbound Value	Rule Enabled AND AND AND AND AND AND AND AND AND AN	New Insert Edit Delete
If No Rules Apply Allow O Deny Provisionina:	User.group-member exactly matches [Visitors]) AND System.Time between 8:00 AM and 5:00 PM AND Week day is between Monday and Friday) THEN Allow	_		
	OK Cancel			



15 Set the Name to Contractors then click OK:

Name:	
Contractors	
ОК	Cancel

16 Set the *Action* to *Allow* then click *New*:

Rules	Selected Rule Details	
Name Enabled Action		
Contractors V Deny	Rule Name: Contractors	Rule Enabled
	(Constraint) AND/OR
		New
		Teco
	Action Provisioning (Outbound Values)	
	O Deny Admin-Acc	nd Values
	Check Posture	t IIII
	TNC Vian40	
	NAP Man30 Man70	•
	Summary	
Add Copy Remove		
If No Rules Apply		
○ Allow ⊙ Deny		
Provisioning: Admin-Access		
	OK Cancel	



17 In the Constraint Details window set the Attribute Category to Authenticator. Select the attribute named Authenticator Type then set the value to Wireless. Click OK.

This will create an authorization rule that permits access if the authentication request originates from a *Wireless* device:

Match The Following Rule: Attribute Category: Authenticator Authenticator Authenticator Container Authenticator Device Template Authenticator Device Template Name Authenticator Name	Attribute: Authentica Data type: integer Description: Purpose Equal To	tor Type label for sub/authenticator in Iqnition
Authenticator Type	 Static Value 	O Dynamic Value of Attribute
Sub Authenticator Sub Authenticator Name Vendor Vendor Name	Wireless	
	OK Cancel	

18 Click *New* to create an additional rule. In the *Constraint Details* window set the *Attribute Category* to *User*. Select the attribute named group-member then set the match condition to *Exactly Matches*. Click *Add* then select the group named *Contractors*. Click *OK*:

This will create an authorization rule that permits access if the authenticating user is a member of the *Contractors* group:

Authentication Service Authentication Service Name Authentication Service Type Lookup Service	Data type: integer Description: User's group membership (internal store) Exactly Matches	
Lookup Service Name Lookup Service Type account-locked email-address enable-max-retries enable-password-expiration enable-start-time first-name	Static Value Dynamic Value of Attri Contractors	ibute
group-member last-name max-retries network-usage office-location password-expiration role start-time	Add Delete	



19 Click OK:

Rules			Selected Rule Details		
Name	Enabled	Action			
Visitors	~	Allow	Rule Name: Contractors	Rule Enabled	
Contractors	\checkmark	Allow			
			(Constraint)	AND/OR	
			(Authenticator.Authenticator Type = Wireless	AND -	
			▼ User.group-member exactly matches [Contractors]) ▼	•	New
			Action Provisioning (Outbound Values) Allow Provision With Deny All Outbound Values) Check Posture Admin-Access TNC Van40 NAP Man J0	lues	
			Summary		
Add Con	Rem	ove	IF (Authenticator Authenticator Type = Wireless AND		
	<u>K</u> em		User.group-member exactly matches [Contractors]) THEN Allow		
if No Rules App	ly.				
🔿 Allow 🧿 Dei	ny				
	Admin-	Access			
			OK Const		

20 The Ignition Server will now have an authorization policy that supports PAP authentication using the Internal Store with the following authorization rules:

Access Policy: Internal

Authentication Policy

The following protocols are active:

Outer Protocol	Inner Protocol
NONE	PAP

Certificate

ide.avayalabs.local

Identity Routing

Default Directory Set Internal

Authorization Policy

Rule Name	Rule Summary		
Visitors	IF ((Authenticator .Authenticator Type = Wireless AND User.group-member exactly matches [Visitors]) AND System.Time between 8:00 AM and 5:00 PM AND Week day is between Monday and Friday) THEN Allow		
Contractors	IF (Authenticator.Authenticator Type = Wireless AND User.group-member exactly matches [Contractors]) THEN Atlow		

If No Rules Apply: Deny



2.1.6 Authenticators

Each network infrastructure device that uses the Ignition Server as a RADIUS server must be defined as an authenticator (i.e. RADIUS client). Each entry can be defined to support a single device (host IP address) or a group of devices (IP subnet & mask) and must include a RADIUS shared secret. In addition an access policy must also be assigned so that the Ignition Server knows how to process authentication requests originating from the device.

The authenticator entry also defines the device vendor and type which determines the RADIUS check and return attributes supported by the device.

2.1.6.1 Configuration Steps

For this configuration step an authenticator will be defined for the WC 8180 Wireless Controller with the following parameters defined:

- 1) The *Name* set to *wc8180-1.avayalabs.local* which is the hostname assigned to the WC 8180.
- 2) The IP Address set to 192.168.10.30 which is the host IP address assigned to the WC 8180.
- 3) The **RADIUS Shared Secret** set to **avayalabs** which matches the RADIUS shared secret assigned to the WC 8180.
- 4) The *Access Policy* is mapped to the Access Policy named *Internal* created in section 2.1.5.



Figure 2.1.6.1 – Access Policy



<u>A</u> dministration <u>H</u> elp								
S Configuration Monitor 💥 Iroubleshoot								
Configuration	Current Site: Site 0							
⊡== Site 0	Authenticator Summary						Actions 🔻	
E Site Configuration	Include descendants of selected container							
🗄 🖪 Access Policies	Name	IP Address	Bundle	Enabled	RADIUS	MAC Auth	TACACS+	Container
- W Authenticators								
E Directories								
🗄 🌌 Provisioning								
🖽 📵 Guest Manager								
			New					
		L	Coltan					
	J							

avaya.com



2 Enter the Name and IP Address of the WC8180 Wireless Controller then set the Authenticator Type to Wireless. Set the RADIUS Shared Secret to avayalabs then select the Access Policy named Internal. Click OK:

Name:	wc8180.avayalabs.com		Enable Authenticator					
IP Address:	192.168.10.30		Bundle					
Container:	<u>default</u>							
Authenticator Type:	Wireless 👻							
Vendor:	Default	Device Template:	generic-default 👻					
RADIUS Settings	TACACS+ Settings							
RADIUS Shared Sec	aret: •••••••	Sho	w					
Fnable RADIL								
	Enable RADIOS Access							
Access Policy:								
Enable MAC	Auth							
Access Policy:	default-radius-device		-					
O Do Not Use P								
O Use RADIUS S	Use RADIUS Shared Secret As Password							
O Use This Pass	word	Show						
	<u>0</u> K	<u>C</u> ancel						

3 The WC8180 has now been added as an authenticator and can now forward RADIUS access requests to the Ignition Server which will be authenticated against the Internal Store:

	IP Address	Bundle	Enabled	RADIUS	MAC Auth	+22A2AT	Container
180.avayalabs.com	192.168.10.30		~	\checkmark			default



2.1.7 Guest Manager

The Ignition Guest Manager Server provides a HTTP/HTTPS portal interface that allows provisioning users (sponsors) to provision temporary accounts for guest users. The Ignition Guest Manager communicates with the Ignition Server using SOAP over HTTPS.

The Guest Manager Server uses RADIUS to authenticate sponsor user's accounts against the Ignition Server. The provisioning account can be stored locally on the Ignition Server or centrally in LDAP or Active Directory user store.

Each provisioner user account maps to one or more provisioning groups that defines the guest user template and options each provisioner can create.

2.1.7.1 SOAP Service

Guest user and internal provisioner accounts are created by the Ignition Guest Manager on the Ignition Server over a SOAP interface. All communications over the SOAP interface are secured using TLS. For the Ignition Guest Manager Server to communicate with the Ignition Server the SOAP interface must be enabled on the Ignition Server and a SOAP username & password defined.

2.1.7.1.1 Configuration Steps

For this configuration step the SOAP service will be enabled on the Ignition Server with the following parameters defined:

- 1) The SOAP Username set to soapuser.
- 2) The SOAP Password set to avayalabs.
- 3) The SOAP Service set to Enabled.
- 4) The Bound interface will be set to the Admin Port.







1 Within the Ignition Dashboard select Configuration > Site-Name > Services > SOAP. Click Edit:

<u>A</u> dministration <u>H</u> elp		
🖄 Configuration 🕺 Monitor 💥 Ir	oubleshoot	
Configuration	Current Site: Site 0	
Er 🚾 Site 0	Sites	Actions 🔻
Site Configuration	Name: Site O	
Authenticators	Services Licenses Certificates Logging Scheduled Backups	
	RADIUS TACACS+ SOAP	
	SOAP Service: Disabled Edit SOAP Username: Bound interface:	
	Port: Session Timeout (seconds): SOAP Certificate: default_soap_cert Modify	

2 Check the option *Enable SOAP Service*. Set the *SOAP Username* to *soapuser* and the *SOAP Password* to *avayalabs*. Select the *Bound interface* named *Admin Port* then click *OK*:

Enable SOAP Service		
SOAP Username:	soapuser	
SOAP Password:	•••••	Show
Bound interface:	Admin Port 🔹	
Port:	443	
Session Timeout (seconds):	1800	
	<u>QK</u> <u>C</u> ancel	



2.1.7.2 Internal Provisioners

Internal provisioners authenticate to the Ignition Server using RADIUS and there accounts are stored locally on the Ignition Server. When an internal provisioner attempts to access the Ignition Guest Manager, the Ignition Guest Manager verifies the provisioner's credentials on the ignition server using RADIUS.

Each internal provisioner can be assigned to one or more provisioning groups which in-turn assigns guest users to an internal group on the Ignition Server. When the internal provisioner account is created on the Ignition server, the internal account includes the provisioning group names that the provisioners account has been assigned.

2.1.7.2.1 Configuration Steps

For this configuration step a Guest Manager Server Entry will be created for the Guest Manager server with the following parameters defined:

- 1) The *Name* set to *w3kserver-guest.avayalabs.local* which is the hostname assigned to the Ignition Guest Manager server.
- 2) The *IP Address* set to **192.168.10.55** which is the host IP address assigned to the Ignition Guest Manager server.
- 3) The *RADIUS Shared Secret* set to *avayalabs* which matches the RADIUS shared secret defined on the Ignition Guest Manager server.
- 4) The Provisioner Access Policy set to *Internal Provisioners Only* which authenticates provisioner accounts locally on the Ignition Server.




1 Within the Ignition Dashboard select Configuration > Site Configuration > Guest Manager > Guest Manager Servers. Right click on Guest Manager Servers then select New:

Administration <u>H</u> elp			
🖄 Configuration 🛃 Monitor 💥	Iroubleshoot		
Configuration	Current Site: Site 0		
⊡🖏 Site 0	Guest Manager Server Summary		
ide.avayalabs.local	Server Name	IP Address	Access Policy
E-B Site Configuration			
Access Policies			
🖻 🍓 Guest Manager			
🔂 Guest Manager Se	TV/		
📲 🕌 Provisione 🛛 Ne	w		
		New Edit Delete	
	>		

2 Enter the *Name* and *IP Address* for your Ignition Guest Manager server then set the *RADIUS Shared Secret* to *avayalabs*. Set the *Provisioner Access Policy* to *Internal Provisioners Only* then click *OK*:

Name:	w3kserver-guest.avayalabs.com	
IP Address:	192.168.10.55	
RADIUS Shared Secret:		Show
Provisioner Access Policy:	Internal Provisioners Only 🛛 👻	

avaya.com



3 A *Guest Manager Server* entry to support internal provisioners has now been created:

Guest Manager Server Summary		
Server Name	IP Address	Access Policy
w3kserver-guest.avayalabs.com	192.168.10.55	Internal Provisioners Only



2.1.7.3 External Provisioners (Optional)

External provisioners authenticate to the Ignition Server using RADIUS and there accounts are stored on an external user directory such as Active Directory or LDAP. When an external provisioner attempts to access the Ignition Guest Manager, the Ignition Guest Manager verifies the credentials on the Ignition Server using RADIUS which is verified against the external user directory.

Each external provisioner can be assigned to one or more provisioning groups which in-turn assigns guest users to an internal group on the Ignition Server. External provisioners are mapped to provisioning groups using provisioning access policies and virtual groups defined on the Ignition Server.



Figure 2.1.7.3 – External Provisioners

2.1.7.3.1 Directory Services

When external provisioning accounts are required, the directory store where provisioning user the accounts are located needs to be defined as a directory service on the on the Ignition Server. The directory service is then tied to a directory set so that the Ignition Server knows where to locate the provisioning users when they attempt to authenticate to the Ignition Guest Manager server.

2.1.7.3.1.1 Configuration Steps

For this configuration step a Microsoft Windows Server 2003 Domain Controller will be added to the Directory Services on the Ignition Server with the following parameters defined:

- 1) The *Name* will be set to *Active Directory* to match the directory type.
- 2) The **Service Account Name** will be set to **ide** which is a user account for the Ignition Server defined in Active Directory.
- 3) The *Service Account Password* will be set to *avayalabs* which matches password for the ide user account predefined in Active Directory.
- 4) The *NetBIOS Domain* will be set to *AVAYALABS* which matches the NetBIOS domain name for the Active Directory Domain.



- 5) The *AD Domain Name* will be set to *avayalabs.local* which matches the Active Directory Domain name.
- 6) The *Directory Root DN* will be set to the default value *DC=avayalabs,DC=local*.
- 7) The User Root DN will be set to the default value DC=avayalabs, DC=local.
- 8) The *Primary Server IP Address* will be set to **192.168.10.50** which is the host IP address assigned to Microsoft Windows Server 2003 Domain Controller.
- 9) The *Port* will be set to the default value 389.
- 10) The **NETBIOS Server Name** will be set to **W3KSERVER-DC1** which matches the NetBIOS name assigned to the Microsoft Windows Server 2003 Domain Controller.
- 1 Within the Ignition Dashboard select Configuration > Directories > Directory Services. Right click on Directory Services then select New:

Administration Help				
Sonfiguration Monitor 💥 Ir	oubleshoot			
Configuration	Current Site: Site 0			
⊡ 🚟 Site 0	Directory Services			
ide.avayalabs.local	Name		Directory Type	
Access Policies	Internal User Store	Internal Dat	abase	
🕀 🚿 Authenticators				
🖻 🔊 Directories				
Directory Sets				
The sectory New.				
🕀 🧩 Virtual Ma 🛛 Direct	ory Service Status			
🕀 🌆 Provisionin 🛛 Direct	ory Service Debugger			
🖻 🍈 Guest Manager				
Guest Manager Serve				
		New		
	J			



2 In the Choose Service Type window select Active Directory then click Next:



Choose Service Type Service Configuration Options Configure Active Directory Configure Token Service Configure RSA Service Configure RSA Service Manually configure

Cancel

Back 🕨 Next

3



4 In the Connect To Active Directory window enter the AD Domain Name, Service Account Name and Password. Click Next:

 ✓ Choose Service Type ✓ Service Configuration Options ➢ Connect To Active Directory Connect To Active Directory Configure Active Directory Created Active Directory Summary 	Connect To Active Directory j Please provide the following information needed to connect to the active directory. AD Domain Name: avayalabs.local Service Account Name: Service Account Password:
	(A) Make sure the appliance has been configured with a DNS server.
	4, Back P. Net Finish Cance

To communicate with Active Directory DNS must be enabled and configured on the Ignition Server.

In this example an Active Directory account called *ide* with the password *avayalabs* has been pre-defined in Active Directory and is a member of the *Domain Users* group. Account options have also been set to lock the account password so that it does not change.

Properties	? ×
Remote control Terr Member Of Dial-in General Address Account	minal Services Profile COM+ Environment Sessions Profile Telephones Organization
User logon name:	
ide	@avayalabs.local
User logon name (pre- <u>W</u> indows 20	000):
AVAYALABS\	ide
Logon Hours Log On	<u>I</u> o
Account options:	
User must change password User cannot change password Password never expires Store password using revers	a at next logon
Account expires • Never • End of: Sunday	, January 09, 2011 💌
	OK Cancel Apply

ide Properties ? 🗙
Remote control Terminal Services Profile COM+ General Address Account Profile Telephones Organization Member Of Dial-in Environment Sessions
Member of:
Name Active Directory Folder Domain Admins avayalabs.local/Users Domain Users avayalabs.local/Users
Add <u>R</u> emove
Primary group: Domain Users Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK Cancel Apply



5 In the *Connect to Active Directory* window select the *Security Protocols* type *Simple* then enter the *IP address* of the *Active Directory Domain Controller*. Click *Next*:

 Choose Service Type Service Configuration Options Connect To Active Directory Configure Active Directory Configure Active Directory Summary 	Connect To Active Directory No IP addresses were foun Please provide the followin Service Account Name: Service Account Password: Security Protocol: IP Address:	d in the specified domain. Ig information needed to connect to the Active Di ide Simple 192.168.10.50	rectory.
	Port:	389	
	4. Back	Next Finish Cancel	

6 In the *Configure Active Directory Window* set the *Name* to *Active Directory*. Click the icon next to the *NETBIOS Server Name* field to resolve the NETBIOS server name. Verify the Active Directory configuration by selecting *Test Configuration*:

✓ Choose Service Type ✓ Service Configuration Options	Configure Active Directory i Successfully joined the do Please provide the require	main. d information needed to config	gure the active directory.
 Connect To Active Directory Connect To Active Directory Configure Active Directory Created Active Directory Summary 	Settings Name: Active I Security Protocol: Simple	Directory	
	Joined Domain As		
	NetBIOS Domain:	AVAYALABS	8
	AD Domain Name:	avayalabs.local	8
	Service Account Name:	ide	8
	Service Account Password	•••••	8
	Primary Server		Secondary Server
	IP Address: 19	2.168.10.50	IP Address:
	Port: 38	9 🔒	Port: 389
	NETBIOS Server Name: W	3KSERVER-DC1 🔽 🔀	NETBIOS Server Name: 📃 🖌
		Test Conf	figuration
	DN Configuration		
	Directory Root DN:	DC=avayalabs,DC=local	Browse
	User Root DN:	DC=avayalabs,DC=local	Browse
	Netlogon Account Root DI	N:	Browse
	Accept all users in the f	orest	
	🛃 Back	Next Finish Cancel]

avaya.com



7 If the Active Directory configuration is correct and the test successful, the following dialog message will be displayed. Click *OK* then *Next*:



8 A summary of the Active Directory configuration will be displayed. Click *Finish*:



9 An Active Directory service has now been added to the Ignition Server:

Directory Services	
Name	Directory Type
Internal User Store	Internal Database
Active Directory	Active Directory



2.1.7.3.2 Directory Sets

A directory set is required to tell the Ignition Server where to locate the provisioner user accounts and how to authenticate them. When a provisioning user attempts to authenticate, a RADIUS authentication request will be generated by the Ignition Guest Manager to the Ignition Server. The Ignition Server will use a provisioner access policy to determine which directory set to use to locate and authenticate the provisioning user accounts.

2.1.7.3.2.1 Configuration Steps

For this configuration step a Directory Set will be created with the following parameters defined:

- 1) The *Name* will be set to *Provisioners* to match the directory type.
- 2) A directory set for external provisioners will be defined that:
 - a. Assigns the User Lookup Service to the directory service named Active Directory.
 - b. Assigns the Authentication Service to the directory service named Active Directory.
- 3) A directory set for internal provisioners will be defined that:
 - a. Assigns the User Lookup Service to the directory service named Internet User Store.
 - b. Assigns the Authentication Service to the directory service named Internet User Store.
- 1 Within the Ignition Dashboard select Configuration > Site Configuration > Directories > Directory Sets. Right click on Directory Sets then select New:

<u>A</u> dministration <u>H</u> elp		
Configuration Monitor 💥 <u>I</u>	roubleshoot	
Configuration	Current Site: Site 0	
⊡ 🕶 Site 0	Directory Sets	
ide.avayalabs.local	Name	
E-Site Configuration	default set	
	Internal	
in Cale Directory Sets		
🕼 Inte New		
🦾 🕼 default set		
🕀 🔊 Directory Services		
🕀 🏭 Internal Store		
🗄 🤗 Virtual Mapping		
Provisioning		
🖽 🐨 🐨 Guest Manager		
	New	
		=00=



2 In the Directory Set window enter the name Provisioners then click Add:

ame: Provisioners					
irectory Set Entries User Lookup Service	Authentication Service	Fallthrough if Unable to Connect	Fallthrough if User Not Found	Fallthrough if Authentication Failed	
		Add			

3 In the Directory Set Entry window set the Lookup Service and Authentication Services to Active Directory. Click OK:

i Please select a directory service and an authentication server for the directory set entry.	
User Lookup Service: Active Directory 🔽	
Authentication Service: Active Directory	

4 Click Add. In the *Directory Set Entry* window set the *Lookup Service* and *Authentication* Services to Internal User Store. Click OK:

i Please select a directory service and an authentication server for the directory set entry.		
User Lookup Service: Internal User Store 🔻		
Authentication Service: Internal User Store 💌		
<u>QK</u> <u>Cancel</u>		



5 A *Directory Set* named *Provisioners* with two directory service entries has now been created. Click *OK*:



The previous example demonstrates how to create a directory set that supports both internal and external provisioners. If support for internal provisioners accounts is not required, the second directory set entry does not need to be defined.

2.1.7.3.3 Virtual Groups

i

The provisioning templates available to each provisioner is determined using a provisioner access policy and is based on group membership. When external provisioning accounts are used, the Ignition Server has to be able to associate the external user to a group so that authorization can be performed and permissions applied.

Virtual groups provide a mechanism that allows the Ignition Server to map external groups stored in Active Directory or LDAP to a virtual group within the Ignition Server. An authorization policy can then reference the virtual group to determine if the user is authorized to access the system and then assign the appropriate template access.

2.1.7.3.3.1 Configuration Steps

For this configuration step a Virtual Group called **Domain Users** will be created that maps to the Active Directory group called **Domain Users**. This will permit all Active Directory users to be able to access the Ignition Guest Manager Server and provision guest user accounts:



1 Within the Ignition Dashboard select Configuration > Site Configuration > Directories > Virtual Mapping > Virtual Groups. Select Actions > Add A New Virtual Group:

Administration Help							
Configuration Monitor 💥 Iro	ubleshoot						
Configuration	Current Site: Site 0	_	_	_	_	_	
⊡Site 0	Virtual Groups	Actions 🔻	Virtual Group Details				
ide.avayalabs.local	Name	Add A N	lew Virtual Group				
E- 🚯 Site Configuration	Visitors	Rename	Virtual Group				
	Contractors	Delete V	irtual Group				
E Directory Sets			D	irecton, Service		Group DN	
E B Directory Services			Internal User Store	incectory service	Visitors	oroup biv	
🕀 🄊 Internal Store							
🖃 🧩 Virtual Mapping							
🚟 User Virtual Attril							
🔤 🔤 Device Virtual At							
Provisioning							
🗄 📵 Guest Manager							
					Add Delete		
	•			100000			
							=00=

2 Set the Virtual Group Name to Domain Users then click OK:

Virtual Group Name: Domain Users	
<u>QK</u> <u>Cancel</u>	

avaya.com



3 A *Virtual Group* named Domain Users has now been created. Click *Add* to map the *Virtual Group* to the Active Directory *Domain Users* group:



4 In the *Map Groups* window select the *Directory Service* named *Active Directory*. Browse the tree then select the Active Directory group named *Domain Users*. Click *OK*:



avaya.com



5 A *Virtual Group* and *Active Directory* group mapping has now been created:



2.1.7.3.4 Provisioner Access Policy

External provisioner users are authenticated and authorized using provisioner access policies. Each provisioner access policy determines the directory set to use to authenticate users against as well as authorization rules that determine the provisioning groups available to authorized users based on virtual group membership.

2.1.7.3.4.1 Configuration Steps

For this configuration step a Provisioner Access Policy will be created with the following parameters:

- 1) The *Name* will be set to *Provisioners*.
- 2) The *Find Provisioners Using Directory Set* value will be set to the directory set named *Provisioners*.
- 3) A simple authorization rule will be created with the following parameters:
 - a. The Rule Name set to Domain Users.
 - b. The *If Member of Virtual Group* value set to the virtual group called *Domain Users*.
 - c. The internal groups called **Contractors** and **Visitors** will be added to the **Grant Access to Provisioning Groups** list.



1 Within the Ignition Dashboard select Configuration > Site Configuration > Guest Manager > Provisioner Access Policy. Right click on Provisioner Access Policy then select New:

Administration Help						
🤹 Configuration 📈 Monitor 💥 Iroubleshoot						
Configuration	ion Current Site: Site 0					
Site 0 ide.avayalabs.local ide.avayalabs.local Site Configuration Site	Provisioner Access Policies Access policies you create here a you create here DO NOT poly to on his or her provisioning group Name	apply ONLY to external provisioners tha o provisioners stored in the Ignition interr membership. Directory Set	it is, provisioners stored in your LDA hal store. For an internally stored pr Rule(s)	AP or AD store. Access policies ovisioner, privileges depend solely Policy Type		
Provisioner Access						
		New Edit.				
	1 <i>7</i>					

2 Set the *Name* to *Provisioners* then select the directory set named *Provisioners*. Set the *Policy Type* to *Simple* then click *OK*:

Name:	Provisioners
Find Provisioners Using Directory Set:	Provisioners
Policy Type:	Simple
	<u>QK</u> <u>Cancel</u>



3 Click *New* to create a new access rule:

Name:	Provisioners
Find Provisioners Using Directory Set:	Provisioners
Reminder: This policy does not appl	y to Internal Provisioners
Provisioner Rules - Specify Provision	ing Based on Virtual Group Membership
New Delete	
	OK Cancel

4 Set the Rule Name to Domain Users then click OK:

Rule Name:		
Domain Users		
	<u>Q</u> K	

5 Set the *If Member of Virtual Group* value to *Domain Users*. Assign the *Visitors* and *Contractors* groups then click *OK*:

Name:	Provisioners
Find Provisioners Using Directory Set:	Provisioners
Reminder: This policy does not appl	ly to Internal Provisioners
Provisioner Rules - Specify Provision	ing Based on Virtual Group Membership
Domain Users	Rule Name: Domain Users If Member of Virtual Group Domain Users Grant Access to Provisioning Groups Asitors Sontractors
New Delete	
	QK



6 A Provisioner Access Policy and rule for has now been created on the Ignition Server:

Provisioner Access Policies					
Access policies you create here apply ONLY to external provisioners that is, provisioners stored in your LDAP or AD store. Access policies you create here DO NOT apply to provisioners stored in the Ignition internal store. For an internally stored provisioner, privileges depend solely on his or her provisioning group membership.					
Name	Directory Set	Rule(s)	Policy Type		
Provisioners	Provisioners	Domain Users	Simple		

2.1.7.3.5 Guest Manager Server

External provisioners authenticate to the Ignition Server using RADIUS and there accounts are stored externally to the Ignition Server. When an external provisioner attempts to access the Ignition Guest Manager server, the Ignition Guest Manager verifies the provisioner's credentials on the ignition server using RADIUS.

The Ignition Server determines which external user to directory to authenticate the provisioners session against using the directory set specified in the provisioner access policy. Once authenticated the provisioners session is authorized using authorization rules assigned to the provisioner access policy.

2.1.7.3.5.1 Configuration Steps

For this configuration step a Guest Manager Server Entry will be created for the Guest Manager server with the following parameters defined:

- 1) The *Name* set to *w3kserver-guest.avayalabs.local* which is the hostname assigned to the Ignition Guest Manager server.
- 2) The *IP Address* set to **192.168.10.55** which is the host IP address assigned to the Ignition Guest Manager server.
- The *RADIUS Shared Secret* set to *avayalabs* which matches the RADIUS shared secret defined on the Ignition Guest Manager server.
- 4) The Provisioner Access Policy set to **Provisioners** which tells the Ignition Server to authenticate provisioner accounts externally against Active Directory.



1 Within the Ignition Dashboard select Configuration > Site Configuration > Guest Manager > Guest Manager Servers. Right click on Guest Manager Servers then select New:

Administration Help						
😰 Configuration 🔣 Monitor 💥 Iroubleshoot						
Configuration	Current Site: Site 0					
⊡ 🕶 Site 0	Guest Manager Server Summary					
ide.avayalabs.local	Server Name	IP Address	Access Policy			
E-Site Configuration						
Authoritication						
Authenticators						
Provisioning						
🖻 🎍 Guest Manager						
🔓 Guest Manager Serv						
📲 Provisione 🛛 New						
		New Edit Dolate				
		New				

2 Enter the *Name* and *IP Address* for the Ignition Guest Manager server then set the *RADIUS Shared Secret* to *avayalabs*. Set the *Provisioner Access Policy* to *Provisioners Only* then click *OK*:

Name:	w3kserver-guest.avayalabs.local	
IP Address:	192.168.10.55	
RADIUS Shared Secret:		Show
Provisioner Access Policy:	Provisioners 🗸 🔫	

avaya.com



3 A *Guest Manager Server* entry that supports both internal and external provisioners has now been created:

Guest Manager Server Summary		
Server Name	IP Address	Access Policy
w3kserver-guest.avayalabs.local	192.168.10.55	Provisioners



Internal provisioners will still be able to authenticate and access the Ignition Guest Manager server once support for external provisioners has been enabled.



2.2 Ignition Guest Manager

The following sections outline the configuration steps required to configure the Avaya Ignition Guest Manager Server to support Guest Access:

2.2.1 Ignition Guest Manager Login

- 1 Using a supported web browser connect to the administrative portal on the Ignition Guest Manager server:
 - HTTP URL Example: http://<guest-manager-ip-address>:8080/GuestManager/Admin
 - HTTPS URL Example: https://<guest-manager-ip-address>:8080/GuestManager/Admin



2 Enter the administrative User ID and Password then click Login:

Guest Manager
Identity Engines Ignition Guest Manager Copyright 2010 Awaya Corporation and its licensers. All rights reserved. Ignition Guest Manager User ID: admin Password:

The default username and password for the Ignition Guest Manager is *admin / admin*.



2.2.2 Basic Administration

By default the administrative username and password is set to admin / admin. For security purposes it is recommended that you change the default password.

To change the default password on the Ignition Guest Manager Server:

avaya	Ignit	ion Guest Manager Administrator: admin Connected: 192.168.10.52	Log
Expand All Collapse All		Administrator Account	
Provisioning Groups			
Provisioners		Administrator User Name: admin	
Self-Service		Administrator Password Change	
Guest Users		Administrator Timeout (min.): 30	(1 - 60)
Devices		Cubrat Board	
🖻 🗁 Administration			
📑 Account 📄 Preferences			
Connection			
😰 Appliance			
RADIUS			
🔤 📄 Certificate			
P. 🗁 Notification			
- 📄 E-mail			
SMS Gateways			

2 Enter the *Current Password* then in the *New Password* and *Confirm Password* fields enter and confirm the New Password. Click Submit:



3 The admin password will now be changed:

Successful Account Update

Administrator User Name: admin Administrator Password: ********** Administrator Timeout (min.): 30



2.2.3 Connections

The Ignition Guest Manager Server must be connected to the Ignition Server using the SOAP service. In addition to authenticate internal and external provisioners the RADIUS shared secret must be defined.

2.2.3.1 Configuration Steps

For this configuration step the Ignition Guest Manager Server will be connected to the Ignition Server using the SOAP service:

- 1) The *IP Address* will be set to **192.168.10.52** which is the host IP address assigned to the Admin Port on the Ignition Server.
- 2) The **Username** will be set to **soapuser** which was defined on the Ignition Server in section 2.1.7.1.
- 3) The Password will be set to *avayalabs* which was defined on the Ignition Server in section 2.1.7.1.
- 4) The Shared Secret will be set to *avayalabs* which was defined on the Ignition Server in section 2.1.7.2 & 2.1.7.3.
- 1 Within the *Ignition Guest Manager* select *Administration* > *Connection* > *Appliance*. Enter the Ignition Server *IP Address* then set the SOAP *User Name* to *soapuser* and the SOAP *Password* to *avayalabs*. Click *Connect*:

	Ignition Guest Manager Administrator: admin Disconnected	Logout
Expand All Collapse All	Login to Appliance	
📄 Provisioning Groups		
😰 Provisioners	IP Address: 192.168.10.52	
	SOAP Port: 443	
🛅 Guest Users	User Name: soapuser	
📄 Devices	Password:	
Administration		
🕑 Account	Connect	
E Connection		
Appliance		
🗋 Certificate		
P. 🗁 Notification		
📄 E-mail		
SMS Gateways		
- 🔒 Logs		
🔮 Who's On		
User's Guide		

2 The Ignition Guest Manager will now connect to the Ignition Server using the SOAP service:

You have successfully connected to Ignition™ Server: 192.168.10.52.



3 Within the Ignition Guest Manager select Administration > Connection > RADIUS. Set the RADIUS Shared Secret to avayalabs then click Submit:



RADIUS configuration was successfully updated.



4

The RADIUS shared secret must match the RADIUS shared secret defined for the Guest Manager Server entry on the Ignition Server.



2.2.4 Provisioning Groups

Provisioning groups are containers that collect internal users, guest users, and devices and allow these items to be managed by one or more provisioners in the provisioning group. In addition, each provisioner belongs to a provisioning group. The provisioner's membership in the provisioning group determines his or her provisioner rights and Guest Manager application settings.

Each provisioning account can be assigned to one or more provisioning groups. Internal provisioning accounts are assigned to provisioning groups within the Guest Manager application while external provisioning users are assigned to provisioning groups using provisioner access policies defined on the Ignition Server.

2.2.4.1 Configuration Steps

For this configuration step a provisioning groups called *Contractors* and *Visitors* will be defined and mapped to internal groups created on the Ignition Server:

- 1) A provisioning group named *Visitors* be created on the Ignition Guest Manager server with the following parameters:
 - a. The *Name* will be set to *Visitors* which matches the *Visitors* internal group created in section 2.1.4 on the Ignition Server.
 - b. The *Access Type* will be set to *Visitors* which associates the provisioning group with the internal group on the Ignition Server.
- 2) A provisioning group named **Contractors** will be created Ignition Guest Manager server with the following parameters:
 - a. The *Name* will be set to *Contractors* which matches the *Contractors* internal group created in section 2.1.4 on the Ignition Server.
 - b. The *Access Type* will be set to *Contractors* which associates the provisioning group with the internal group on the Ignition Server.



Figure 2.2.5 – Provisioning Groups



1 Within the Ignition Guest Manager select Provisioning Groups. Select Actions > New Provisioning Group:

	Ignition Guest Manager	Administrator: admin Connected: 192.168.10.52	Logout
Expand All Collapse All		Provisioning Groups	
···· Provisioners	Check All Clear All		Actions 🔻
	Name	Guest User Rig	New Provisioning Group
🛅 Guest Users	default	Yes	Delete Provisioning Group Members
Devices Administration Account Preferences Connection PApliance RADIUS Certificate Notification SMS Gateways Logs Who's On	Check All Clear All		Delete Expired Guest Users Delete Provisioning Groups Export Guest Users Export Devices

2 Enter the group name *Visitors* then associate the provisioning group to the internal group on the Ignition Server named *Visitors*:

	Create Provisioning Group					
Common	Guest User	Device	Notification	Advanced		
Group N	ame: Visitors	ners in thi	s group can vie	ew and edit e	ach other's records	
Tempo	rary accounts	may be va	alid for up to:			
	8 (:	L-999) 🔘 r	minutes 💿 hour	rs 🔘 days		
Areas t Access Ty	to which guest ypes: Visitor	users/de s Contra	vices can be g actors	ranted access	5:	
			Submit	Reset		



3 Select the *Guest User* tab then modify the guest provisioning options as required. Click *Submit*:

Create Provisioning Group								
Common	Guest User	Device	Notification	Advan	ced			
Allow or do edit, assoc	low or deny provisioners in this provisioning group the right to manage (create, lit, associate) USERS:							
Guest N	otification: 📝 Er	nail 🔽 🤅	SMS 🛛 Display	Password				
₹ ₹ ₹	Password Complexity Check: 4-6 characters (min 4, max 30, single number or range. For example, 6-10) including Iower case upper case ✓ Auto-generated passwords for guest users ✓ Auto-generate guest user name with: ○ Firstname_Lastname (e.g., John Smith -> John_Smith) ④ firstinitiallastname (e.g., John Smith -> jsmith)							
	N	lo extra p	refix or suffix (Add pre	efix (Add suffix	with	
		Acces	sible to Provis	sioners [)efau	It Value	-	
Bulk	Load Guest Users	• Ye	s © No				-	
Devic	ce Association	9 Ye	s 🔍 No			A	-	
Delet		● Ye	s © No		9 Ye	s 🔍 No	-	
Cent	Phone	• Ye	s UNO				-	
Acco	unt Activation		ne 🔍 First Logi	n N	Any w	alidity duration	-	
Netw	ork Access Rights	e ve			ll net	work rights	-	
		1 e 1e	5 10	ľ]	
		Г	Submit	Reset				



4 A summary of the Provisioning Group and options will be displayed:

Succ	essful Provisioning Group Creation
New provisioning group "Visitors"	was successfully created with the following information:
Common	
Provisioners in this group can	view and edit each other's records
Group Name:	Visitors
Max Duration:	8 hours
Access:	Visitors
Guest User	
User Management Right:	Allow
Guest Notification:	Display Password
Password Complexity Check:	4-6 characters including number
Password Generation:	Yes
User Name Generation:	firstinitiallastname (e.g., John Smith -> jsmith), No extra prefix or suffix
Bulk Load Guest Users:	Yes
Device Association:	Yes
Delete on Expire	Yes, default value: Yes
Cell Phone:	Yes
Account Activation:	Time
Account Validity Duration:	Yes
Network Access Rights:	Yes
Device	
Device Management Right:	Deny
Notification	
SMS Template:	New guest user was successfully created. User Name: \$username Password: \$password
Email Template:	Subject: Guest user account Message: User Name: \$username
	Password: \$password First Name: \$firstname
	Last Name: \$lastname
	E-mail: \$email
	Comments: \$comment Start Time: \$starttime
	End Time: \$endtime
	Access: \$access
Print Info:	
Advanced	
Trusted Hosts	All hosts are trusted
Time Zone:	America/New_York
Idle Timeout (min.)	_



5 Within the Ignition Guest Manager select Provisioning Groups. Select Actions > New Provisioning Group:

AVAYA	Ignition Guest Manager Administra	tor: admin d: 192.168.10.52	Logout
Expand All Collapse All		Provisioning Groups	
📄 Provisioning Groups 😰 Provisioners	Check All Clear All	Actions 🗸	
	Name	Guest User Rig New Provisioning Group	
🛅 Guest Users	default	Yes Delete Provisioning Group Mem	embers bers
Devices	Visitors	Yes Delete Expired Guest Users	
- Contraction - Contraction - Contraction - Contraction - Contraction - Contraction - Contraction - Contraction	Check All Clear All	Export Devices	
Connection			
 Notification SMS Gateways Logs Who's On User's Guide 			

6 Enter the group name *Contractors* then associate the provisioning group to the internal group on the Ignition Server named *Contractors*:

	Create Provisioning Group					
Common	Guest User	Device	Notification	Advanced		
Group N	ame: Contracto Provision rary accounts 8 (:	ners iners in thi may be va 1-999) ⊙r	s group can vi alid for up to: ninutes () hou	ew and edit e rs ©days	ach other's records	
Areas t Access Ty	to which guest ypes: Visitor	users/de s 🕅 Contra	vices can be g actors	ranted acces	5:	
			Submit	Reset		



7 Select the *Guest User* tab then modify the guest provisioning options as required. Click *Submit*:

Create Provisioning Group								
Common	mon Guest User Device Notification Advanced							
Allow or de edit, assoc	llow or deny provisioners in this provisioning group the right to manage (create, dit, associate) USERS:							
Guest N	Guest Notification: 🖉 Email 🛛 SMS 🖉 Display Password							
Pass	Password Complexity Check: 4-6 characters (min 4, max 30, single number or range. For example, 6-10) including Volumer case Volumer case Inumber Special characters							
	uto-generate gu Fi fi N	est user irstname rstinitialli	name with: Lastname (e.g., astname (e.g., Jo prefix or suffix (, John Sm ohn Smith	ith -> i -> js efix (John_Smith) mith) D Add suffix	with	
		Acce	ssible to Provis	sioners [Defau	lt Value		
Bulk	Load Guest Users	© Y∈	s 🔘 No					
Devie	ce Association		s 🔘 No					
Delet	e on Expire	© Y∈	s 🔘 No		Ye	s 🔘 No		
Cell I	Phone	© Y∈	s 🔘 No					
Account Activation		© ті	me 🔘 First Logii	n				
Account Validity Duration		on 💿 Ye	Ves ONO		Max validity duration			
Network Access Rights		© Y∈	◎ Yes ◎ No		All network rights			
	Network Access Rights Ores No All network rights							

avaya.com



8 A summary of the Provisioning Group and options will be displayed:

Succ	essful Provisioning Group Creation
New provisioning group "Contracto	ors" was successfully created with the following information:
Common	
Provisioners in this group can	view and edit each other's records
Group Name	: Contractors
Max Duration	: 8 hours
Access	: Contractors
Guest User	
User Management Right	Allow
Guest Notification	: Display Password
Password Complexity Check	: 4-6 characters including lower case, upper case, number
Password Generation	: Yes
User Name Generation	: firstinitiallastname (e.g., John Smith -> jsmith), No extra prefix or suffix
Bulk Load Guest Users	: Yes
Device Association	Yes
Delete on Expire	: Yes, default value: Yes
Cell Phone:	Yes
Account Activation	: Time
Account Validity Duration	: Yes
Network Access Rights	: Yes
Device	
Device	- D
Device Hanagement Right	Deny
Notification	
SMS Template	New guest user was successfully created.
	User Name: \$username
Email Template	Password: Spassword
Email Template	Message: User Name: \$username
	Password: \$password
	First Name: \$firstname
	E-mail: \$email
	Comments: \$comment
	Start Time: \$starttime
	Access: \$access
Print Info	· · · · · · · · · · · · · · · · · · ·
Advanced	
Trusted Hosts	: All hosts are trusted
Time Zone:	: America/New_York
Idle Timeout (min.)	: 15

9 Provisioning Groups named *Visitors* and *Contractors* have now been created:

Provisioning Groups							
Che	ack All Clear All		Actions 🔻				
	Name	Guest User Rights	Device Rights				
	Contractors	Yes	No				
	default	Yes	No				
	Visitors	Yes	No				
Che	Check All Clear All Actions						



2.2.5 Internal Provisioners

A provisioner is a person who creates and manages guest user accounts and device records using the Guest Manager application.

Internal provisioner accounts are stored locally on the Ignition Server while external provisioner accounts are stored in the Active Directory or LDAP user store. When a provisioner account is created on the Ignition Guest Manager Server, the account will be created in the local store on the Ignition Server.



The Ignition Server can simultaneously supports internal and external provisioner accounts at the same time if required.

Each internal provisioner will use the Guest Manager application to create, modify, and delete guest user accounts. The provisioner owns the guest user accounts that he or she creates. If the provisioner's account is deleted, then the guest user accounts it owns are either transferred to other provisioners or deleted.

2.2.5.1 Configuration Steps

For this configuration step an internal provisioning account will be created and assigned to both the *Contractor* and *Visitor* provisioning groups:

1	Within the Ignition	Guest Manager select Provisioners.	Select Actions > New Provisioners:
	Αναγα	Ignition Guest Manager Administrator: admin Connected: 192.168.	3.10.52 Logout 🔒
	Expand All Collapse All Provisioning Groups Provisioners Self-Service Guest Users Devices	Provisioner Search Filters Provisioners: All Internal Provisioners All Specify Filter: Apply Filter	
	Administration Account Preferences Appliance RADUS Certificate SMS Gateways Gs User's Guide	Internal P	Provisioners
		Check All Clear All	Actions ▼
		No records found. Check All Clear All	List Mine List Rew Self-Provisioners Load Internal Provisioners Delete Expired Guest Users Delete Provisioners Export Guest Users Export Devices



2 Enter a name, password and email address then assign the *Contractors* and *Visitors* provisioning groups. Click *Submit*:

	Create Provisioner
User Name:	jdoe
First Name:	Jane
Last Name:	Doe
Password:	•••••
Confirm Password:	•••••
Email:	jdoe@example.com
Comments:	
Member of Provisioning Group(s):	Contractors default Visitors
	Submit Reset

3 An Internal Provisioning user account has now been created on the Ignition Server:

Successful Provisioner Creation
New provisioner " jdoe " was successfully created with the following information: User Name: jdoe
First Name: Jane Last Name: Doe
Password: ********** Email: jdoe@example.com
Comments: Member of Provisioning Visitors Group(s): Contractors



4 Within the *Ignition Dashboard* select *Configuration* > *Site Configuration* > *Directories* > *Internal Users*. The internal provisioning user account will be displayed:

Administration Help									
😰 Configuration 📈 Monitor 💥 Iroubleshoot									
Configuration	Current Site: Site 0								
Configuration	Internal Users O Get All Specify Criteria: User Name Starts With Apply Filter Viewing records: 1 - 1 of 1 Internal User Name Last Name Account Disabled Dending/Expired								
 ☐ Internal Users ☐ Internal Devices ⊖ ♥ Virtual Mapping ☐ ☐ Provisioning ☐ ☐ Guest Manager 									
	<u>New</u> <u>Copy</u> <u>Lat</u> <u>Delete</u> <u>Kefresh</u> <u>Import</u> <u>Export</u>								



2.3 Wireless LAN 8180 Controller

The following sections outline the configuration steps required to configure the Avaya WC8180 wireless controller to provide guest access using a Captive Portal that authenticates guest users against the Ignition Server:

2.3.1 **Preliminary Configuration**

The Avaya 8100 series Wireless Controller requires basic network configuration before it can provide wireless services to users. The Wireless Controller will be configured with the necessary management and user VLANs as well as the virtual IP addresses required for management, Access Point communications and captive-portal capture and re-direction. In addition wireless services need to be configured and enabled so that the Avaya 8100 series Wireless Controller can manage Avaya 8100 series Access Points and serve Wireless LANs.

2.3.1.1 Configuration Steps

For this configuration step a factory defaulted WC8180 Wireless Controller will be configured with the following basic parameters:

- 1. Management VLAN 10 and guest VLAN 14 will be created:
 - a. VLAN 10 will be assigned the IP address 192.168.10.30/24 and will be assigned to ports 1-11,13-16.
 - b. VLAN 14 will be assigned the IP address 192.168.14.30/24 and will be assigned to port 12.
 - c. IP routing will be *enabled*.
- 2. A static default route will be defined pointing to the **192.168.10.1** IP address assigned to the private internal interface on the firewall.
- 3. A valid license file will be uploaded.
- 4. Wireless services will be enabled:
 - a. The system-ip address will be set to the management IP address 192.168.10.30.
 - b. The WC8180 will be configured as *MDC capable* with the password *AvayaLabs12!*@ assigned.
 - c. The WC8180 will join the wireless domain named AVAYALABS.
 - d. The wireless domain will be configured with the country code US.
 - e. The wireless domain will be configured to automatically *promote-discovered-aps*.
 - f. A mobility VLAN named VLAN14 will be created and mapped to VLAN id 14.

2.3.1.1.1 AACLI

1 Using the AACLI access the global configuration context:

```
WC8180# configure terminal
```

```
WC8180(config)#
```



2 Create VLAN 10 and 14 and assign port membership:

WC81	80(config)# 1	vlan	create 10) name	VLAN10	type port			
WC81	80(config)# 1	vlan	create 14	l name	VLAN14	type port			
WC81	80(config)# 1	vlan i	members 1	emove	1 1-26				
WC81	WC8180(config)# vlan members add 10 1-11,13-26								
WC81	80(config)# 1	vlan i	members a	add 14	12				
WC81	80(config)# 1	vlan i	mgmt 10						
WC81	80(config)# s	show	vlan						
Id N	lame		Туре	Protoc	:ol	User PID	Active	IVL/SVL	Mgmt
1 V	/LAN #1		Port	None		0x0000	Yes	IVL	NO
	Port Member	rs: NC	DNE						
10 v	/LAN10		Port	None		0x0000	Yes	IVL	Yes
	Port Member	rs: 1-	-11,13-26						
14 v	/LAN14		Port	None		0x0000	Yes	IVL	NO
Port Members: 12									
Total	Total VLANS: 3								

3 Assign virtual IP addresses to VLAN 10 and VLAN 14 and mark VLAN 10 for management:

```
WC8180(config)# interface vlan 10
WC8180(config-if)# ip address 192.168.10.30 255.255.255.0
WC8180(config-if)# interface vlan 14
WC8180(config-if)# ip address 192.168.14.30 255.255.255.0
WC8180(config-if)# exit
WC8180(config)# show vlan ip
```

% Total of Primary Interfaces: 2

4 Globally enable *IP Routing*:

```
WC8180(config)# ip routing
WC8180(config)# show ip routing
```

IP Routing is enabled IP ARP life time is 21600 seconds



5 Define a static *Default Route* that points to the Firewalls IP Address on VLAN 14:

WC8180(config)# ip route 0.0.0.0 0.0.0.0 192.168.14.1 1

WC8180(config) # show ip route

Ip Route											
DST	MASK	NEXT	COST	VLAN	PORT	PROT	TYPE	PRF			
0.0.0.0	0.0.0.0	192.168.10.1	1	14	12	S	IB	5			
192.168.10.0	255.255.255.0	192.168.10.30	1	10		- c	DB	0			
192.168.14.0	255.255.255.0	192.168.14.30	1	14		- c	DB	0			
Total Routes: 3	3										

6 If necessary upload a license file. Once installed the WC8180 will need to be reset:

WC8180 (config) # copy tftp license address 192.168.10.6 filename license.dat

License successfully downloaded.

NOTE: system must be rebooted to activate license.

WC8180(config)# boot

7 Using the AACLI access the *wireless* configuration context. Set the *interface-ip* to the virtual IP Address assigned to VLAN *10* and enable wireless services:

```
WC8180> enable
```

WC8180# configure terminal

WC8180(config)# wireless

WC8180(config-wireless)# interface-ip 192.168.10.30

WC8180(config-wireless)# enable

WC8180(config-wireless)# **show wireless**

Status : Enabled Interface IP : 192.168.10.30 TCP/UDP base port : 61000

8 Configure the WC8180 as *MDC-Capable* and define a *password*:

```
WC8180 (config-wireless) # controller mdc-capable
```

% Domain password should be between 10-15 characters long. % Password must contain a minimum of 2 upper, 2 lowercase letters % 2 numbers and 2 special characters like !@#\$%^&*() Enter domain password: AvayaLabs12!@ Verify Domain password: AvayaLabs12!@


9 Create and join the *Wireless Domain* using the password defined in the previous step:

```
WC8180(config)# end
```

```
WC8180# wireless controller join-domain domain-name AVAYALABS mdc-address 192.168.10.30
```

Enter Domain Secret: AvayaLabs12!@

WC8180# show wireless controller domain-membership

Domain	Name	:	AVAYALABS
Domain	Role	:	Active MDC
Domain	Action Status	:	Join Success
Action	Failure Reason	:	None

10 Access the wireless configuration context. Create a Mobility VLAN for the guest users:

WC8180# configure terminal

WC8180(config)# wireless

WC8180(config-wireless# domain mobility-vlan VLAN14

WC8180 (config-wireless# show wireless domain mobility-vlan

Mobility VLAN Name Status default-MVLAN Active VLAN14 Active

11 Map the Mobility VLAN to the physical Guest VLAN Id:

WC8180(config-wireless# switch vlan-map VLAN14 lvid 14 WC8180(config-wireless# show wireless switch vlan-map

Mobility VLAN Name	LVID	Role	Weight	Track
VLAN14	14	None	1	NONE
default-MVLAN	0	None	1	NONE



12 Define a *country-code* and enable then option to *Automatically Promote Discovered APs*. Finally *synchronize* the configuration:

```
WC8180(config-wireless# domain
```

WC8180(config-wireless# country-code us

WC8180 (config-wireless# domain auto-promote-discovered-ap

WC8180(config-wireless# **end**

WC8180# wireless controller config-sync

WC8180# show wireless domain info

Country	:	US
AP QOS Mode	:	Disabled
Roaming Timeout	:	30 seconds
TSPEC Violation Report Interval	:	300 seconds
Auto Promote Discovered AP	:	Enabled
AP Image Update Download Group Size	:	5 %
AP Image Update Reset Group Size	:	5 %
AP Reset Group Size	:	5 %

2.3.2 Captive Portal

The Avaya 8100 series Wireless Controllers supports an integrated captive-portal feature that offers a simple way to provide secure authenticated access to users and devices using a standard web browser. Captive-portal authentication allows enterprises to offer authenticated access to the network for guest users by capturing and re-directing a web browsers session to a captive-portal login page hosted on the Avaya 8100 series Wireless Controllers.

The guest user must enter a valid username and password which is authenticated on the Ignition Server before being granted access to the network.

2.3.2.1 Configuration Steps:

For this configuration step the global captive-portal service parameters will be modified and a captive-portal profile created:

- 1. The global captive portal configuration will be modified with the following parameters:
 - a. The global state will be *Enabled*.
 - b. The *HTTP* redirection port redirection will be set to 8080.
- 2. A network profile will be created with the following parameters:
 - a. The Id will be set to 1.
 - b. The *Name* will be set to *AVAYA-GUEST* which will match the network profile name.
 - c. The Protocol Mode will be set to HTTP.

2.3.2.1.1 AACLI

1 Using the AACLI access the Wireless configuration context:

WC8180# configure terminal

WC8180(config)# wireless

2 Set the *HTTP* port to *8080*:

WC8180(config-wireless) # captive-portal http-port 8080

3 Globally enable the *Captive Portal*:

WC8180(config-wireless) # captive-portal enable

WC8180(config-wireless) # show wireless captive-portal info

Mode	:	Enabled
Additional HTTP Port	:	8080
Additional HTTPS Port	:	0
Statistics Reporting Interval	:	120
Authentication Timeout	:	300
HTTPS Certificate	:	Not present

4 Access the *Captive Portal Profile 1* configuration context:

WC8180(config-wireless)# captive-portal profile 1

5 Set the Profile Name to AVAYA-GUEST and the Protocol-Mode to HTTP:

```
WC8180(config-cp-profile) # profile-name AVAYA-GUEST
WC8180(config-cp-profile) # protocol-mode http
WC8180(config-cp-prodile) # show wireless captive-portal profile 1 detail
```

Captive Portal Profile ID: 1

Name	: AVAYA-GUEST
Protocol Mode	: http
User Logout Mode	: Enabled
Session Timeout (seconds)	: 0
Idle Timeout (seconds)	: 0
Max Bandwidth Up (bps)	: 0
Max Bandwidth Down (bps)	: 0
Max Input Octets (bytes)	: 0
Max Output Octets (bytes)	: 0
Max Total Octets (bytes)	: 0
Foreground Color	: #999999
Background Color	: #BFBFBF
Separator Color	: #B70024



2.3.3 RADIUS Profiles

The Avaya 8100 series Wireless Controller can authenticate guest users against one or more RADIUS servers assigned to a RADIUS profile. The RADIUS profiles are then assigned to one or more network profiles that require 802.1X, MAC or captive-portal authentication. The Avaya 8100 series Wireless Controller will then direct all RADIUS authentication requests to the available servers defined in the RADIUS profile.

2.3.3.1 Configuration Steps

For this configuration step a RADIUS authentication profile named *IDE* will be created with the Ignition Server added as a RADIUS server. The following RADIUS parameters will be defined:

- 1) The *IP Address* set to **192.168.10.52** which matches the *IP Address* assigned to the *Admin Port* on the *Ignition Server*.
- 2) The **RADIUS Shared Secret** set to **avayalabs** which matches the RADIUS shared secret assigned to the WC 8180 in section 2.1.6.

2.3.3.1.1 AACLI

1 Using the AACLI access the Wireless Security configuration context:

WC8180(config-cp-profile)# security

```
2 Create a RADIUS Profile with the id 1 named IDE and set the type to Auth:
```

WC8180 (config-security) # radius profile IDE type auth

WC8180(config-security) # show wireless security radius profile

Total radius profiles: 1, auth: 1, acct: 0

Radius Profile Type

----- -----

IDE

Authentication

3 Create a *RADIUS Server* entry with the *IP Address* assigned to the *Ignition Server* and assign it to the RADIUS Profile named *IDE*. When asked enter and confirm the secret *avayalabs*:

WC8180(config-security) # radius server 192.168.10.52 IDE secret

Enter server secret: **avayalabs**

Verify server secret: **avayalabs**

WC8180(config-security) # show wireless security radius server

Total radius servers: 1Server IPRadius ProfilePort# Priority192.168.10.52IDE18121





2.3.4 Network Profiles

Network Profiles define the wireless service parameters that radios advertise to wireless users. Each network profile defines the SSID name advertised to users, the mobility VLAN users are assigned, the authentication type and encryption ciphers. In addition the network profile defines the QoS mode and parameters for the wireless service.

2.3.4.1 Configuration Steps

For this configuration step *Network Profile 2* will be created with the following parameters will be defined:

- 1) The Profile Name set to AVAYA-GUEST which for consistency matches the SSID name.
- 2) The SSID set to AVAYA-GUEST which is advertised to wireless clients.
- 3) The *Mobility VLAN Name* set to *VLAN14* which is where the guest user's traffic will be forwarded.
- 4) User Validation set to RADIUS and the RADIUS profile named IDE assigned.
- 5) Captive Portal authentication Enabled and the Captive Portal Profile 1 assigned.

2.3.4.1.1 AACLI

1 Using the AACLI access the Wireless Network Profile 2 configuration context:

```
WC8180(config-security) # network-profile 2
```

2 Set the Profile Name and SSID Name to AVAYA-GUEST and define the Mobility VLAN name:

WC8180 (config-network-profile) # profile-name AVAYA-GUEST

WC8180 (config-network-profile) # ssid AVAYA-GUEST

```
WC8180(config-network-profile)# mobility-vlan VLAN14
```

3 Set the User Validation mode to RADIUS and assign the RADIUS Profile named IDE:

WC8180 (config-network-profile) # user-validation radius

WC8180 (config-network-profile) # radius authentication-profile IDE

4 Assign the Captive Profile Id 1 then enable Captive Portal:

```
WC8180(config-network-profile)# captive-portal profile-id 1
WC8180(config-network-profile)# captive-portal enable
WC8180(config-network-profile)# show wireless network-profile 2 detail
```

Ne

twork Profile ID: 2	
Name	: AVAYA-GUEST
SSID	: AVAYA-GUEST
Hide SSID	: NO
Mobility Vlan Name	: VLAN14
No Response to Probe Request	: Disabled
Captive Portal Mode	: Enabled
User Validation	: RADIUS
Captive Portal Profile Id	: 1
Local User Group	: Default
RADIUS Authentication Profile Name	: IDE
RADIUS Accounting Profile Name	:
RADIUS Accounting Mode	: Disabled
Security Mode	: open
MAC Validation	: Disabled
Wireless ARP Suppression	: Disabled

2.3.5 AP Profiles

Administrator's provision managed Access Points using AP profiles. AP profiles allow a common set of configuration parameters to be defined and applied to large groups of APs. Each AP profile is AP model specific and assigns radio profiles, network profiles and QoS mappings to Access Points assigned to the AP profile.

Each Access Point radio supports up to 16 Virtual Access Points (VAPs) each of with are assigned a unique MAC address and look like a single Access Point. Each radio can support a maximum of 16 network profile assignments.

2.3.5.1 Configuration Steps

For this configuration step *Network Profile 2* will be assigned to radios using the default *AP Profile 1*:

- 1) Network Profile 2 will be assigned to VAP 1 on Radio 1 (5GHz).
- 2) Network Profile 2 assigned to VAP 1 on Radio 2 (2.4GHz).

2.3.5.1.1 ACLI

```
1 Using the AACLI access the Wireless AP Profile 1 configuration context:
```

WC8180(config-wireless)# ap-profile 1

2 Assign Network Profile 2 to VAP 1 on Radios 1 & 2:

```
WC8180(config-ap-profile)# network 1 1 profile-id 2
WC8180(config-ap-profile)# network 2 1 profile-id 2
WC8180(config-ap-profile)# show wireless ap-profile network 1
```



AP Profile Id	Radio Id	VAP Id	Network Profile Id	Radio Operation
1	1	1	2	On
1	2	1	2	On

3 Connect the Avaya 8100 series Access Points to the network and verify they are *managed*:

WC8180(config-wireless) # **show wireless ap status**

ΑΡ ΜΑC	AP IP	Controller IP	Status	Need Image Upgrade
5C:E2:86:0F:A3:C0	192.168.11.104	192.168.10.30	Managed	NO
5C:E2:86:0F:C6:20	192.168.11.101	192.168.10.30	Managed	NO
5C:E2:86:10:4A:C0	192.168.11.100	192.168.10.30	Managed	NO

AVAYA

2.4 Verification

2.4.1 Internal Provisioners Authentication

Internal provisioning users are authenticated against the Ignition Servers internal user store. The following steps verify the internal provisioning user created in *Section 2.2.5* can successfully authenticate to the Ignition Server and is assigned the correct provisioning group assignments:

1	Using a supported v Manager server:	veb browser connect to the administrative portal on the Ignition Guest
	HTTP URL E	xample: http:// <guest-manager-ip-address>:8080/GuestManager/</guest-manager-ip-address>
	HTTPS URL	Example: https:// <guest-manager-ip-address>:8080/GuestManager/</guest-manager-ip-address>
	Eile Edit View Higtory E	ookmarks Iools Help
2	Enter the User Name 2.2.5 then click Log	e and <i>Password</i> of the internal provisioning account created in section in:
	Αναγα	Ignition Guest Manager
		Identity Engines Ignition Guest Manager
		Copyright 2010 Avaya Corporation and its licensers. All rights reserved.
		Ignition Guest Manager
		User Name: jdoe Password: •••••••• Login



3 Once successfully authenticated a dialog message will be displayed which provides the *Provisioning Groups* names the internal provisioning user is assigned:

AVAYA	Ignition Guest Manager Provisioner: jdoe	Logout
Expand All Collapse All	You have successfully signed in as jdoe. Member of Provisioning Group(s): Contractors Visitors	

4 You can verify authentication using the *Ignition Dashboard* application by clicking *Monitor* > *Site-Name* > *Guest Manager AAA Summary* > *Succeeded*:





2.4.2 External Provisioners Authentication

External provisioning users are authenticated through the Ignition Server but their credentials are stored externally in an Active Directory or LDAP user store. The following steps verify the external provisioning users can authenticated to the Ignition Server and are assigned the correct provisioning group assignments:

- 1 Using a supported web browser connect to the administrative portal on the Ignition Guest Manager server:
 - HTTP URL Example: http://<guest-manager-ip-address>:8080/GuestManager/
 - HTTPS URL Example: https://<guest-manager-ip-address>:8080/GuestManager/

<u>File Edit V</u> iew Hi <u>s</u> tory	<u>B</u> ookmarks <u>I</u> ools <u>H</u> elp	
🕙 - 🕑 🗙	▲ http://192.168.10.55:8080/GuestManager/provisioner/sign_in.jsp	÷
Getting Started		

2 Enter the User Name and Password of the Active Directory or LDAP account then click Login:

AVAYA	Ignition Guest Manager
	Identity Engines Ignition Guest Manager
	Copyright 2010 Avaya Corporation and its licensers. All rights reserved.
	Ignition Guest Manager
	User Name: kimarshali
	Password: Login



3 Once successfully authenticated a dialog message will be displayed which provides the *Provisioning Groups* names the internal provisioning user is assigned:

AVAYA	Ignition Guest Manager Provisioner: klmarshall	Logout
Expand All Collapse All	You have successfully signed in as klmarshall. Member of Provisioning Group(s): Visitors Contractors	

4 You can verify authentication using the *Ignition Dashboard* application by clicking *Monitor* > *Site-Name* > *Guest Manager AAA Summary* > *Succeeded*:

Administration Help					
Configuration Monitor	💥 <u>T</u> roubleshoot				
Monitor	Current Site: Site 0				2
E Site 0	RADIUS AAA Summary	TACACS+ AAA Summary	Guest Manager AAA Summary	User Accounting Learned Devices (via	AD)
······ 📷 ide.avayalabs.local	• User Authentication/	Authorization Activity (last 2	200 records)		🗹 Aut
	Succeeded Failed				
	Z010-12-17 09:42:22	kimarshall	Brouizioner	w3kserver-quest.avavalabs.local	Active Directory
			28228		

2.4.3 Captive Portal Authentication

Wireless users are authenticated using a captive-portal that captures and redirect users to a captiveportal login page hosted on the Avaya 8100 series Wireless Controller. When guest users associate to the AVAYA-GUEST wireless service, all traffic is blocked except DHCP, DNS and HTTP.

When the user launches their browser and attempts to connect to an external web-site, the WC 8180 captures the session and redirects the user to a login page hosted on the Avaya 8100 series Wireless Controller. The user must agree to the terms and conditions as well as enter valid credentials before being permitted access to the network:

1 Associate a wireless client to the *AVAYA-GUEST* SSID. Obtain and IP address from the DHCP server and verify IP addressing:

C:\>ipconfig

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix	. :	guest.avayalabs.local
Description	. :	Dell Wireless 1490 Dual Band WLAN Mini-Card
Physical Address	. :	00-1F-3A-02-AC-82
DHCP Enabled	. :	Yes
Autoconfiguration Enabled	. :	Yes
IPv4 Address	. :	192.168.14.101 (Preferred)
Subnet Mask	. :	255.255.255.0
Lease Obtained	. :	Friday, January 07, 2011 2:21:25 PM
Lease Expires	. :	Saturday, January 08, 2011 3:50:20 PM
Default Gateway	. :	192.168.14.1
DHCP Server	. :	192.168.14.1
DNS Servers	. :	208.67.222.222
		208.67.220.220
Primary WINS Server	. :	192.168.0.254
NetBIOS over Tcpip	. :	Enabled



In pre-authenticated state, the device will only be able to obtain an IP address, resolve hostnames and communicate with the captive portal. No other communications will be permitted.

(i)

In this example DHCP for the guest users is being provided by the firewall. The firewall has a DHCP scope defined with a pool of addresses in the 192.168.14.0/24 range which provides its guest interface IP address as the default gateway. Public DNS servers are also provided.

2 Launch a web-browser and attempt to connect to an external server (example *http://www.avaya.com*). The browsers session will be captured by the Avaya 8100 series Wireless Controller and redirected to the captive portal login page:

Captive Portal - Windows Internet Explorer	tml?pl=1&p2=1073&p3=3232238181	🔹 😒 🤧 🗶 🚰 Google	<mark>- ۵ - × -</mark>
😪 Favorites 🛛 🍰 🏉 Suggested Sites 👻 🔊 Web Slice Ga	illery ▼	💩 • 🔯 • 🖂 🖶 • Beg	je ▼ Safety ▼ T <u>o</u> ols ▼ 🕡 ▼ ³
Ανάγα	Welcome	to the Network	^
R	Acceptance Use Policy		1
Enter your Username. Username Password	Please allow pop-ups to display the logout WEB page.	X	
Connect To start using this service, enter your credentials and click the Connect button	Check here to indicate that	you have read and accepted the Accepta	nce Use Policy.
Done		👩 😌 Internet Protected Mode: On	- ≪ <u>ii</u> + €,100% +

3 Enter a valid *Username* and *Password* that you provisioned using the Ignition Guest Manager application. Check the option *Check here to indicate that you have read and accepted the Acceptance User Policy* then click *Connect*:

Captive Portal - Windows Internet Explorer	ptive_portal.html?p1=1&p2=1073&p3=323223818	1 🔹 😫 😽 🗙 🔏 Google	μ
🚖 Favorites 🛛 🚖 🏉 Suggested Sites 👻 👩	Web Slice Gallery 🕶		
🏀 Captive Portal		🖄 🕶 🖾 🐨 🖻 🖷 🖝 🗛	ge ▼ <u>S</u> afety ▼ T <u>o</u> ols ▼ 🔞 ▼
AVAYA	Welcon	ne to the Network	^
Enter your Username.	Acceptance Use Policy		*
Username guser Password	3		
To start using this service, enter you credentials and click the Connect bu	ir utton.	that you have read and accepted the Accepta	ance Use Policy.
Done		👩 🕥 Internet Protected Mode: On	√2 ▼ € 100% ▼



4 Once successfully authenticated the following message will be displayed:



5 View the captive portal sessions on the Avaya 8100 series Wireless Controller using the AACLI or EDM:

WC8180# show wireless captive-portal client status Total number of clients: 1 _____ Client Client Associated Mobility Status IP Address MAC Address Controller VLAN _____ 00:13:02:2E:78:82 192.168.10.101 192.168.10.30 VLAN10 Authenticated _____



AVAYA	EN	TERPRISE DEVIC	CE MANAGE	R			l	Help Se <u>G</u> u	<u>etup</u> Jide	
WC8180 - wc8180-1	~	Device Physical View	📰 Switch Summ	nary 🛎 🕅 🛅 A	ssociate Client 🗵	Captive Po	rtal 🗵			
▲		🔶 rofile 🔰 Status Group	Status Table	Network Stat	us Table Clien	t Status Table	Client Associate Table	Netwo	ork Client Associate	Table 🔶 🔶
Device		Apply R. Defree	h Devoort Dat							
Graph		V Apply Welles								
▷ 🚞 VLAN		MacAddress	InetAddress	UserName	ProtocolMode	VerificationMo	de AssocNetworkld	CPID	SessionTime	Switchl
IP Routing		00:13:02:2e:78:82	192.168.10.101	guser	http	radius	2	1	0d 00:01:52.00	00:1b:4f:
D QoS										
Serviceability										
System										
E Domain										
E Controller										
E Associate Client										
Profiles										
Security										
Mobity Switch										
T Managed AP										
E Managed Switch										
📰 RF Management										
Captive Portal										
		•								4
		Total Rows : 1 row(s)								
		Com		un All sinhte	essenced Devisi		10			
		Сору	ngne igi 2010 Ava	ya. An rights	reserved, Kevisi	on number: 204	10			

6 You can verify authentication using the *Ignition Dashboard* application by clicking *Monitor* > *Site-Name* > *RADIUS AAA Summary* > *Succeeded*:

Administration Help							
6 Configuration Monitor	💥 <u>T</u> roubleshoot						
Monitor	Current Site: Site 0	_	_	_	_	_	Ľ
🖃 🚟 Site 0	RADIUS AAA Summary	TACACS+ AAA Summary	Guest Manager AAA S	ummary L	Jser Accounting	Learned Devices (via AD)	
· ide.avayalabs.local	User Authentication/Authorization Activity (last 200 records)						
	Succeeded Failed						
	Timestamp 2010-12-17 15:15:21 guses	Ucer/MAC	Authenticator	Director Internal User	Auth Bro	Not Applicable	Docture Dr
	2010-12-17 15.15.21 guse		wcoloo-i.avayalabs	unternal Oser	Store NONE/PAP	Not Applicable	
	•		388				
							-00-



3. Reference Documentation

Publication Number	Document Title
NN47280-500	Avaya Identity Engines Ignition Server Configuration Guide
NN47280-501	Avaya Identity Engines Ignition Server Guest Manager Configuration
NN47251-102	Avaya WLAN 8100 Fundamentals
NN47251-500	Avaya WLAN 8100 Configuration - WC 8180 (CLI)
NN47251-501	Avaya WLAN 8100 Configuration - WC 8180 (GUI)

© 2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries. All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein. References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.