

Guest Access with ArubaOS

Version 1.0



Copyright

© 2012 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba will assume no responsibility for any errors or omissions.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License ("GPL"), GNU Lesser General Public License ("LGPL"), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an "as is" basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

Chapter 1:	Introduction	5
	Reference Material	5
Chapter 2:	ArubaOS or Amigopod for Visitor Management	6
Chapter 3:	Guest Networks with Captive Portal Authentication	9
	Captive Portal	9
	Captive Portal Authentication Process	9
	Guest Provisioning	11
	Licenses Required	11
	Certificates	11
Chapter 4:	Captive Portal Configuration	12
	Guest VLAN and Related DHCP Services	12
	Guest User Roles	17
	Network Destination Alias	18
	Defining Guest Access Policies	20
	Configuring the guest-logon Role	24
	Configuring the auth-guest Role	25
	Configuring the SSID Profile for Guest WLAN	27
	Configuring the Internal Database for Guest Authentication	29
	Configuring the Captive Portal Authentication Profile	30
	Configuring the AAA Profile for Guest WLAN	36
Chapter 5:	Guest Provisioning	37
	Configuring Guest Provisioning User	37
	Configuring the Guest-Provisioning Page	38
	Modifying Guest Fields on the GPP	38
	Modifying Page Design of the GPP	42
	Email Options for the GPP	42
	Creating Guest User Accounts	44
Chapter 6:	Optional Configurations for Guest Network	47
	Time Range	47
	Bandwidth Contracts	51
	Maximum User Sessions for Guest Role	54
	Walled Garden	56
	Prioritizing Employee Traffic Using Traffic Management Profile	58

Optional SSID and VAP Profile Parameters for Guest Network	58
Disabling lower Data Rates	58
Denying Inter User Traffic	60
Appendix A: Contacting Aruba Networks	61
Contacting Aruba Networks	61

Chapter 1: Introduction

Every organization, big or small, wants to provide some sort of network access to visitors. The visitors may be guests, contractors, auditors, or partners. The Aruba guest access solution provides role-based access to each category of visitors and secures the sensitive corporate resources. In typical Aruba guest access deployment, the guest users are prevented from accessing private network resources, and the contractors and partners can be give restricted access to some corporate resources. Managing visitor accounts has always been difficult for IT teams. The Aruba guest access solution simplifies guest provisioning by allowing authorized non-IT professionals, such as receptionists, to create and delete guest accounts. Additional features include customizable captive portal pages and the ability to gather detailed account information.

This guide explains the configuration of enterprise guest access using the captive portal capabilities of the base ArubaOS software.

Table 1 lists the current software versions for this guide.

Table 1 Aruba Software Versions

Product	Version
ArubaOS™ (mobility controllers)	6.1
ArubaOS (mobility access switch)	7.0
Aruba Instant™	1.1
MeshOS	4.2
AirWave®	7.3
AmigopodOS	3.3

Reference Material

This technical document assumes that the reader is familiar with the Aruba technology and knows how to set up a working WLAN using profiles such as SSID, VAP, and AAA profiles. The following prerequisite documentation is highly recommended before reading this document:

- Aruba 802.11n Networks Validated Reference Design, available at www.arubanetworks.com/vrd
- Aruba Campus Wireless Networks Validated Reference Design, available at www.arubanetworks.com/vrd.
- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations outside the scope of the VRD series. The Aruba support site is located at: <https://support.arubanetworks.com/>. This site requires a user login and is for current Aruba customers with support contracts.

Chapter 2: ArubaOS or Amigopod for Visitor Management

Businesses provide guest access for different reasons. Some organizations provide free guest access while others provide it as a paid service. Depending on the type of business, the guest access service has a varying degree of impact. Most large enterprises provide guest access as an amenity. Some businesses such as cafés and restaurant chains provide free guest access as a means to drive their core business, while others such as airports and hotels use it as a form of revenue. The Aruba guest access solution is designed to meet the guest access needs of all businesses. Aruba supports two methods of guest access, using just the mobility controller or using the mobility controller plus Amigopod. ArubaOS supports basic guest management and captive portal functionality, with guest access limited to a single master-local cluster. Aruba Amigopod extends the standard ArubaOS captive portal functionality by providing many advanced features, including:

- A fully branded user interface
- Short Message Service (SMS) integration for delivery of receipts
- Bulk upload of visitors for conference management
- Self-provisioning of users for public space environments

Choosing the right solution for your deployment depends on your guest access requirements.

[Table 2](#) summarizes the capabilities of the two Aruba guest access solutions.

Table 2 Comparison of ArubaOS Guest Access and Amigopod
























Feature	ArubaOS	ArubaOS Plus Amigopod
	Not supported = 	Limited support =  Supported = 
Captive Portal Customization		
Captive portal customization		
Captive portal per-SSID customization		
Anonymous logon		
One time tokens/access codes		
Welcome page with session statistics and logout		
Mobile browser aware captive portal pages		
Skins: UI branding customization		
Guest Account Provisioning		
Single point of management for guest account and captive portal in multiple master controller deployments		
Non-IT staff do not require IP access to master controller for provisioning guest accounts		
Guest-provisioning operator role		

Table 2 Comparison of ArubaOS Guest Access and Amigopod (Continued)

Feature	ArubaOS	ArubaOS Plus Amigopod
Customizable guest-provisioning operator role	✗	✓
External servers for operator logins	✓	✓
Provisioning of nonguest user roles by operators	✗	✓
Limit operators to view only the account they created	✓	✓
Self-registration workflow with automated login	✗	✓
Sponsor-approved self-registration	✗	✓
Time zone support for guest access in distributed deployments	✗	✓
Bulk provisioning of guest accounts (CSV import and automatic generation)	!	✓
Export/import of user database	✓	✓
Mandatory and nonmandatory fields	✗	✓
Guest password complexity requirements	✗	✓
Guest account information printing via templates	!	✓
Guest credential delivery through email and SMS	!	✓
Force password change on first login	✗	✓
Delete and/or disable guest accounts on expiration	!	✓
Guest Session Management		
Time and day policy	✓	✓
Guest access expiry timer starts on first login	✗	✓
Limit access based on total session time across multiple logins	✗	✓
Limit guest session data (total bytes)	✗	✓
Limit guest session bandwidth (Mb/s)	✓	✓
Limit guest session to single concurrent login	✓	✓
Hotspot and Hospitality Features		
Walled garden	✓	✓
Plug-and-play clients, any IP	✓	✓
VPN NAT (static NAT per client using public IP)	✓	✓
Credit card billing	✗	✓
Surveys and feedback forms	✗	✓
Target ads and promotions	✗	✓

Table 2 Comparison of ArubaOS Guest Access and Amigopod (Continued)

Feature	ArubaOS	ArubaOS Plus Amigopod
Visitor data mining	✗	✓
MAC or cookie-based reauthentication (portal bypass)	✗	✓
Reporting and Notification		
Peak guest network usage	✗	✓
Total guest sessions (per day, per week, etc.)	✗	✓
Bandwidth usage on guest network	✗	✓
Top x users (session time and bandwidth)	✗	✓
Expiring passwords	✗	✓
Enterprise Features and Scalability		
Managing 1000s of accounts	!	✓
High availability/redundancy	!	✓
Expandability (plug-in architecture)	✗	✓

Chapter 3: Guest Networks with Captive Portal Authentication

Guest networks are often defined by what the guest is not allowed to do and where they are not allowed to go. These are the most common guest usage requirements in enterprises deployments:

- Guest users must be separated from employee users.
- Guests must be limited by:
 - What resources they can access
 - What protocols they are allowed to use
 - What time of the day they can access the network
 - The amount of bandwidth or air time they can use
- Guests should be allowed to access only the local resources that are required for IP connectivity. These resources include DHCP and possibly DNS if an outside DNS server is not available. Aruba recommends the use of a public DNS server for guest networks.
- All other internal resources should be unavailable for the guest.
- Employee traffic should be prioritized on the wireless medium.

The native ArubaOS can be configured to address these requirements of an enterprise network.

Captive Portal

Wireless networks used by corporate employees should always be secured using Layer 2 methods such as WPA2. For guest access, providing Layer 2 authentication using pre-shared keys (PSK) or 802.1X is not a viable solution due to the technical complexity. Instead authentication is moved to Layer 3. Captive portal authentication is a Layer 3 authentication method that redirects users to a captive portal page when they start a web session. The captive portal page can be used for various purposes, such as authenticating the guest using a user name and password, providing an acceptable use policy, or self registration with an email address.

Captive portal on ArubaOS can be configured to authenticate guest users based on user/password or valid email ID information. The system can also be configured simply to present an acceptable use policy and an accept button through custom configuration of the HTML page. ArubaOS does not support the use of advanced features such as payment services, but it can redirect to other portals such as Amigopod for additional services.

Captive Portal Authentication Process

Captive portal is a Layer 3 authentication, which requires that the devices connect to the network and obtain an IP address and related DNS information before authenticating through the captive portal. The following steps explain the entire captive portal process when the native ArubaOS is used for captive portal authentication:

1. The device that is associating to the guest SSID is assigned an initial role (guest-logon role in the example configuration). This initial role allows DHCP, so the user gets an IP address.
2. The user opens a browser and makes an HTTP (or HTTPS) request to some destination (for example, www.bbc.com).

3. The resolver in the device sends a DNS request to resolve the `www.bbc.com`. The initial role (guest-logon role) permits DNS services, so the resolver can communicate with the DNS server.
4. The DNS server replies with the correct address to `www.bbc.com`.
5. The resolver tells the browser which IP address to use based on the DNS reply.
6. The browser initiates a TCP connection to port 80 of the `www.bbc.com` address.
7. The controller intercepts the connection and spoofs the initial TCP handshakes of the HTTP process. At this moment, the client browser thinks it is communicating with the `bbc.com` server.
8. When the browser sends the HTTP GET request for the web page, the controller replies saying that `bbc.com` has “temporarily moved” to `<https://securelogin.arubanetworks.com/[string that identifies client]>`.
9. The browser closes the connection.
10. The browser attempts to connect with `<https://securelogin.arubanetworks.com/[string that identifies client]>`, but it first needs to send a DNS request for the address.
11. The actual DNS server responds that it cannot resolve `<https://securelogin.arubanetworks.com>`, but the *controller* intercepts that reply and changes the packet to say that `securelogin.arubanetworks.com` is at the IP address of the controller itself. Remember that it is critical that the DNS server sends back a reply to the query. It is only then that the controller can spoof the reply back from the DNS server. Sending a DNS request without receiving a reply is not sufficient, since without a reply the controller will never help the client resolve `securelogin.arubanetworks.com`.
12. The browser initiates an HTTPS connection to address of controller, which responds with the captive portal login page, where the guest authenticates.
13. After successful authentication, the user is assigned the post authentication role (auth-guest role in the example configuration). This is the default role in the captive portal profile.
14. After authentication, the browser is redirected to `bbc.com` at the address originally resolved by the DNS. Alternatively, if a welcome page is configured, the browser is redirected to the welcome page.
15. To successfully redirect to the original web page the controller spoofs a reply from `bbc.com` to tell the client that `bbc.com` has “permanently moved” to `bbc.com`. This step corrects the “temporary relocation” that occurred as part of the captive portal login.
16. This causes the client to re-query DNS for the address of `www.bbc.com`.
17. The browser starts to communicate with the actual `bbc.com` server.

Guest Provisioning

Usually, guest users are required to provide a username and password for captive portal authentication. These guest accounts must be created on the authentication server against which the guest users are authenticated. Every time a guest user account has to be created, an IT staff must login to the authentication server and create it. Adding guest accounts to the authentication server quickly becomes a cumbersome task for the IT team. Aruba guest provisioning solves this problem by allowing non-IT professionals, such as receptionists, to create and delete guest accounts.

The Amigopod and base ArubaOS software have guest provisioning capabilities. Any authentication server type available on ArubaOS can be used as the authentication server for captive portal authentication. However, if the base ArubaOS software is used for guest provisioning, only the internal database of the controller can be used as the authentication server for captive portal authentication.

Licenses Required

Captive portal authentication is supported on the base ArubaOS software and it does not require any separate license. However, configuration of guest specific user roles requires the PEFNG license to be present on the mobility controller.

Certificates

The Aruba controller ships with a default server certificate. This certificate demonstrates the secure login process of the controller for captive portal, secure shell (SSH), and WebUI management access. This certificate is not recommended for use in a production network. Aruba strongly recommends that you replace this certificate with a unique certificate that is issued to the organization or its domain by a trusted certificate authority (CA).

Chapter 4: Captive Portal Configuration

A number of tasks are necessary to configure a fully functional guest WLAN. Some of this work is simplified through the use of the configuration wizards, and Aruba highly recommends that you use the wizard where possible. The following list outlines the tasks necessary to configure captive portal authentication:

1. Configure the guest VLAN and related DHCP services (required)
2. Configure guest user roles (required)
3. Configure captive portal profile (required)
4. Configure an SSID profile (required)
5. Configure a AAA profile (required)
6. Configure a VAP profile (required)
7. Configure guest provisioning and create guest user accounts (required)
8. Configure time restrictions (optional)
9. Configure bandwidth contracts (optional)
10. Configure maximum session count (optional)
11. Configure walled garden (optional)
12. Configure traffic management profile (optional)

Guest VLAN and Related DHCP Services

The guest users must be isolated to a subnet that is hidden from the corporate network. Defining a VLAN (subnet) that is local to the controller restricts the guests to a subnet that is not routable in the core network. This VLAN adds an additional layer of security to the design by hiding the IP addressing scheme used in the core network from guests and users who accidentally associate with the guest WLAN.

The guest VLAN is local to the controller, so it is essential to source-NAT this VLAN and define the required DHCP and DNS services. The controller should be the DHCP server for the guest VLAN and this VLAN should be source-NATed by the IP address of the controller to which the VLAN belongs. Source-NATing allows the guest users to reach the allowed destinations while they are still isolated from the core network.



The VLAN and DHCP services required for the guest network should be configured on the controller that terminates the APs. In a master/local deployment, this is usually the local controller.

Table 3 and Table 4 and Figure 1 through Figure 5 show the configuration of a guest VLAN and the related DHCP services.

Table 3 Guest VLAN

VLAN ID	IP
900	192.168.200.1

Guest VLAN Configuration

```
!
interface vlan 900
interface vlan 900 ip address 192.168.200.1 255.255.255.0
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

WIZARDS
AP Wizard
Controller Wizard
WLAN/LAN Wizard
License Wizard
WIP Wizard

NETWORK
Controller
VLANs
Ports
Cellular Profile
IP

SECURITY
Authentication
Access Control

WIRELESS
AP Configuration
AP Installation

MANAGEMENT

Network > VLAN > Add New VLAN « Back

Configuration

VLAN ID 900

Associate with ☒ Port ☐ Port-Channel

Wired AAA Profile N/A

Port Selection

0 1 2 3

Apply

Commands View Commands

Figure 1 Creating a VLAN

Dashboard Monitoring **Configuration** Diagnostics Maintenance Master Switch [Save Configuration](#) [Logout admin](#)

WIZARDS
AP Wizard
Controller Wizard
License Wizard

NETWORK
Controller
VLANs
Ports
Cellular Profile
> IP

SECURITY
Authentication
Access Control

WIRELESS
AP Configuration
AP Installation

MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning

Network > IP > IP Interface > Edit VLAN (900) [« Back](#)

IP version: IPv4
VLAN ID: 900

Details

☐ Obtain an IP address from DHCP

☐ Client ID

☐ Obtain an IP address with PPPoE

Service name:
Username:
Password:
Confirm Password:

☒ Use the following IP address

IP Address: 192.168.200.1
Net Mask: 255.255.255.0
Uplink Priority: 0

DHCP Helper Addresses

No Helper Addresses

Add

Option-82: None

IGMP

Enable IGMP: ☐
Snooping: ☐
Proxy: ☐

☒ Interface: GigabitEthernet 0/0
☐ Port-Channel ID: 0

NAT

Enable source NAT for this VLAN: ☒

Inter-VLAN Routing

Enable Inter-VLAN Routing: ☒

MLD

Enable MLD Snooping: ☐

Figure 2 Configuring IP parameters for the guest VLAN

Configuration Diagnostics Maintenance Master Switch [Save Configuration](#) [Logout admin](#)

Network > IP > IP Interface

IP Interfaces IP Routes IPv6 Neighbors GRE Tunnels NAT Pools DHCP Server OSPF Multicast Routing

VLAN ID	IPv4 Address	IPv4 Net Mask	IPv6 Address	Associated Ports	AAA Profile	Admin State	Operation State	Mode	Actions
1	172.16.0.254	255.255.255.0		GE0/0-1,GE0/7-9,XG0/10-11,Pc0-7	N/A	Disabled	Down	Regular	Enable Edit
145	10.169.145.4	255.255.255.0	fe80::b:8600::	GE0/0-6,Pc1	N/A	Enabled	Up	Regular	Disable Edit
150	10.169.150.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
151	10.169.151.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
152	10.169.152.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
153	10.169.153.4	255.255.255.0		GE0/0-1,Pc1	N/A	Disabled	Down	Regular	Enable Edit
154	10.169.154.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
155	10.169.155.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
156	10.169.156.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
157	10.169.157.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
158	10.169.158.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
159	10.169.159.4	255.255.255.0	fe80::b:8600::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit
900	192.168.200.1	255.255.255.0	fe80::b:8603::	GE0/0-1,Pc1	N/A	Enabled	Up	Regular	Disable Edit

Figure 3 Guest VLAN

Source-NAT Configuration for the Guest VLAN

```
!
interface vlan 900
ip nat inside
!
```

The screenshot shows the 'Edit VLAN (900)' configuration page. The 'NAT' section is circled in red, indicating the configuration for Source-NAT. The 'Enable source NAT for this VLAN' checkbox is checked. Other sections include 'DHCP Helper Addresses', 'IGMP', 'Inter-VLAN Routing', 'MLD', 'BCMC (Broadcast-Multicast) Optimization', and 'OSPF'.

Figure 4 Source-NATing the guest VLAN

Table 4 DHCP Services for the Guest VLAN

Pool Name	Default Router	DNS Server	Network	Netmask
guestpool	192.168.200.1	208.67.222.222 (Public DNS server) 208.67.222.220 (Public DNS server)	192.168.200.0	255.255.255.0



Test that the DNS services are working properly from the guest subnet. A functional DNS service is an integral part of captive portal authentication process.

DHCP Server Configuration for the Guest VLAN

```

!
ip dhcp pool "guestpool"
  default-router 192.168.200.1
  dns-server 208.67.222.222 208.67.222.220
  network 192.168.200.0 255.255.255.0
!
service dhcp
!

```

Dashboard
Monitoring
Configuration
Diagnostics
Maintenance
Master Switch
Save Configuration
Logout admin

WIZARDS
AP Wizard
Controller Wizard
License Wizard
NETWORK
Controller
VLANs
Ports
Cellular Profile
> IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation

Network > IP > DHCP > Edit DHCP Pool (guestpool)
« Back

Default Router	<input type="text" value="192.168.200.1"/>		
DNS Servers	<input type="text" value="208.67.222.222"/> <input type="text" value="208.67.222.220"/> <input type="checkbox"/> Import from DHCP/PPPoE (Multiple DNS Servers should be separated by spaces)		
Domain Name	<input type="text"/>		
WINS Servers	<input type="text"/> <input type="checkbox"/> Import from DHCP/PPPoE (Multiple WINS Servers should be separated by spaces)		
Lease	<input type="text"/>	Days	<input type="text"/> Hrs <input type="text"/> Mins
Network	IP Address	<input type="text" value="192.168.200.0"/>	Net Mask <input type="text" value="255.255.255.0"/>

Apply

Figure 5 Configuring the DHCP pool

Dashboard Monitoring **Configuration** Diagnostics Maintenance Master Switch Save Configuration Logout admin

WIZARDS
AP Wizard
Controller Wizard
License Wizard

NETWORK
Controller
VLANs
Ports
Cellular Profile
IP

SECURITY
Authentication
Access Control

WIRELESS
AP Configuration
AP Installation

MANAGEMENT
General

Network > IP > DHCP Server

IP Interfaces IP Routes IPv6 Neighbors GRE Tunnels NAT Pools **DHCP Server**

OSPF Multicast Routing

Enable DHCP Server ☒

Pool Configuration

Name	Default Router	Network	Range	Action
guestpool	192.168.200.1	192.168.200.0	192.168.200.2-192.168.200.254	Edit Delete

Add

Excluded Address Range

Excluded Address Add Delete

Apply

Commands View Commands

Figure 6 Enabling the DHCP server



NOTE

Use the public DNS server in your location. If a public DNS server is not available in your region, the guest users should be allowed access to the internal DNS server.

Guest User Roles

In the Aruba user-centric network, every client is associated with a user role. The user roles that are enforced through the firewall policies determine the network privileges of a user. A policy is a set of rules that applies to the traffic that passes through the Aruba devices. The rules and policies are processed in a top-down fashion, so the position of a rule within a policy and the position of a policy within a role determine the functionality of the user role. When you construct a role, you must put the rules and policies in the proper order.

Usually, guests are assigned two different roles. The first role is assigned when they associate to the guest SSID, and the other is assigned when they authenticate successfully through the captive portal. Only the guests who successfully authenticate are allowed to use the services needed to connect to the Internet.

Consider the guest-logon role as the initial role and the auth-guest role for authenticated guests. Before these two roles are configured, the policies that are associated with them must be configured.

The guest-logon role uses these policies:

- captiveportal (predefined policy)
- guest-logon-access

The auth-guest role uses these policies:

- cplogout (predefined)
- guest-logon-access
- block-internal-access
- auth-guest-access
- drop-and-log

A policy might have one or more rules that apply to several networks or hosts. Creating a separate rule for each host or network might be laborious and will increase the number of rules in the policy. The network destination alias feature in the ArubaOS can be used to simplify firewall policies that have a set of rules that are common to a group of hosts, domains, or networks.

Network Destination Alias

The network destination alias feature in the ArubaOS can be used to group several hosts or networks. Aliases can be used when several rules have protocols and actions common to multiple hosts or networks. Alias allows the addition of domain/host names and IP addresses. The IP addresses can be added by host, network, or range. When the invert parameter of an alias is enabled, the rules that use that alias are applied to all the IP addresses, domains and hostnames except those specified in the alias.

Table 5 lists the aliases that will be useful in configuration of user roles.

Table 5 Aliases

Alias Name	Purpose	IP Address/ Range
Public-DNS	Defines the public DNS servers	Host 208.67.222.222 208.67.222.220 These are OpenDNS servers. For more details on OpenDNS see www.opendns.com
Internal-Network	Defines the private IPv4 address range	Network 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16

Network Destination Alias Configuration

```
!
netdestination Internal-Network
  network 10.0.0.0 255.0.0.0
  network 172.16.0.0 255.240.0.0
  network 192.168.0.0 255.255.255.0
!
netdestination Public-DNS
  host 208.67.222.222
  host 208.67.222.220
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Master Switch [Save Configuration](#) [Logout](#)

WIZARDS
 AP Wizard
 Controller Wizard
 License Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

ADVANCED SERVICES
 Redundancy
 IP Mobility
 > **Stateful Firewall**
 External Services
 VPN Services
 Wired Access
 Wireless

Advanced Services > Stateful Firewall > Destinations

Global Setting White List BW Contracts Network Services **Destination** BW Contracts

BW Contracts Exception List

Name	Rule Count	Invert	Action	
controller	1	No	Edit	Delete
vrrp_ip	2	No	Edit	Delete
walled-garden-white	1	No	Edit	Delete
Internal-Network	3	No	Edit	Delete
Public-DNS	2	No	Edit	Delete
tftp-server	1	No	Edit	Delete
mcast-subnet	1	No	Edit	Delete
user	1	No	Edit	Delete
dns-servers	1	No	Edit	Delete
controller6	1	No	Edit	Delete
sip-server	2	No	Edit	Delete
localip	1	No	Edit	Delete
mswitch	1	No	Edit	Delete
Amigopod	1	No	Edit	Delete
any	1	No	Edit	Delete
ocs-lync	1	No	Edit	Delete
Add				

Figure 7 Aliases

Defining Guest Access Policies

Guest roles are made up of a number of policies that can be predefined and reused in the system. The following sections describe the policies that will be used to define the rights of the guest in their various roles.

Configuring the guest-logon-access Policy

The guest-logon-access policy is similar to predefined logon-control policy, but it is much more restrictive. The guest-logon-access policy is a part of the guest-logon and auth-guest roles. The rules defined in this policy allow these exchanges:

- Allow DHCP exchanges between the user and the DHCP server, but block other users from responding to DHCP requests.
- Allow DNS exchanges between the user and the public DNS server.

Remember that the guests should be allowed to access only the local resources that are required for IP connectivity. These resources include DHCP and possibly DNS if an outside DNS server is not available.

Table 6 summarizes the rules used by the guest-logon-access policy.

Table 6 guest-logon-access Policy

Rule Number	Source	Destination	Service	Action	Purpose
1	User	Any	UDP min port = 68 max port = 68	Drop	This rule drops responses from a personal DHCP server. This action prevents the clients from acting as DHCP servers.
2	Any	Any	Service svc-dhcp (udp 67 68)	Permit	This rule allows clients to request and discover DHCP IP addresses over the network. The DHCP server on the network does not fall under the user category. Therefore, its response on port 68 is not dropped by the first rule. The first two rules guarantee that DHCP is processed only by legitimate DHCP servers on the network.
3	User	Alias Public-DNS	Service svc-dns (udp 53)	permit	This rule allows DNS queries only to the DNS servers that are defined in the Public-DNS alias.

guest-logon-access Policy Configuration

```
!
ip access-list session guest-logon-access
  user any udp 68 deny position 1
  any any svc-dhcp permit position 2
  user alias Public-DNS svc-dns permit position 3
!
```

The screenshot shows the ArubaOS configuration interface. The top navigation bar includes Dashboard, Monitoring, Configuration (highlighted), Diagnostics, Maintenance, and Plan. A 'Save Configuration' button is on the right. The left sidebar lists various configuration sections: WIZARDS (AP Wizard, Controller Wizard, WLAN/LAN Wizard, License Wizard, WIP Wizard), NETWORK (Controller, VLANs, Ports, Cellular Profile, IP), SECURITY (Authentication, Access Control (highlighted)), and WIRELESS (AP Configuration). The main content area is titled 'Security > Firewall Policies > Edit Session (guest-logon-access)'. It features tabs for User Roles, System Roles, Policies (selected), Time Ranges, and Guest Access. Below the tabs is a 'Rules' table with columns: IP Version, Source, Destination, Service, Action, Log, Mirror, Queue, and Tim. The table contains three rules: 1. IPv4, user, any, udp 68, deny, Low. 2. IPv4, any, any, svc-dhcp, permit, Low. 3. IPv4, user, Public-DNS, svc-dns, permit, Low. An 'Add' button is below the table. A 'Commands' section is at the bottom.

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Tim
IPv4	user	any	udp 68	deny			Low	
IPv4	any	any	svc-dhcp	permit			Low	
IPv4	user	Public-DNS	svc-dns	permit			Low	

Figure 8 *guest-logon-access policy*

Configuring the block-internal-access Policy

The internal resources of an organization should be available only to employees or to trusted groups. Guest users are not part of the trusted entity, so they must be denied access to all internal resources. As the name implies, the block-internal-access policy denies access to all internal resources. This policy is a part of the guest-logon and auth-guest roles.

Table 7 summarizes the rules used by the block-internal-access policy.

Table 7 **block-internal-access Policy**

Rule Number	Source	Destination	Service	Action	Purpose
1	user	Alias Internal-Network	any	drop	This rule denies access to all the addresses that are in the Internal-Network alias.

block-internal-access Policy Configuration

```
!
ip access-list session block-internal-access
  user alias Internal-Network any deny position 1
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

WIZARDS
AP Wizard
Controller Wizard
WLAN/LAN Wizard
License Wizard
WIP Wizard

NETWORK
Controller
VLANs
Ports
Cellular Profile
IP

SECURITY
Authentication
Access Control

Security > Firewall Policies > Edit Session (block-internal-access)

User Roles System Roles Policies Time Ranges Guest Access

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
IPv4	user	Internal-Network	any	deny			Low	

Add

Commands

Figure 9 *block-internal-access policy*

Configuring the auth-guest-access Policy

The most important purpose of the auth-guest-access policy is to define the protocols and ports that the users are allowed to access. This policy is an integral part of the auth-guest role. The auth-guest-access policy allows HTTP and HTTPS traffic to go to any destination from the user. When this policy is combined with the block-internal-access policy in the auth-guest role, the users will be allowed HTTP and HTTPS access to the public websites only.



If you want your guest users to use their IPsec clients, create rules in this policy that allows the use of ports 4500 (for IPsec NAT-T) and 500 (for IKE).

Table 8 summarizes the rules used by the auth-guest-access policy.

Table 8 *auth-guest-access Policy*

Rule Number	Source	Destination	Service	Action	Purpose
1	User	Any	Service svc-http	permit	This rule allows HTTP traffic from the users to any destination.
2	User	Any	Service svc-https	permit	This rule allows HTTPS traffic from the users to any destination.

auth-guest-access Policy Configuration

```
!
ip access-list session auth-guest-access
  user any svc-http permit position 1
  user any svc-https permit position 2
!
```

The screenshot shows the ArubaOS configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (highlighted), 'Diagnostics', 'Maintenance', and 'Plan'. A 'Save Configuration' button and a 'Logout admin' link are on the right. The left sidebar lists various configuration categories: WIZARDS (AP Wizard, Controller Wizard, WLAN/LAN Wizard, License Wizard, WIP Wizard), NETWORK (Controller, VLANs, Ports, Cellular Profile, IP), SECURITY (Authentication, Access Control), and WIRELESS (AP Configuration). The main content area is titled 'Security > Firewall Policies > Edit Session (auth-guest-access)'. It features tabs for 'User Roles', 'System Roles', 'Policies' (selected), 'Time Ranges', and 'Guest Access'. Under the 'Policies' tab, there is a 'Rules' section with a table showing two rules:

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
IPv4	user	any	svc-http	permit			Low	
IPv4	user	any	svc-https	permit			Low	

Below the table is an 'Add' button. At the bottom of the configuration area is a 'Commands' section.

Figure 10 auth-guest-access policy

Configuring the drop-and-log Policy

The drop-and-log policy denies all traffic and records the network access attempt.



The logging function in this policy increases your syslog repository. If you do not require logging, remove the log action from the firewall rule of this policy.

Table 9 summarizes the rule used by the drop-and-log policy.

Table 9 drop-and-log Policy

Rule Number	Source	Destination	Service	Action	Log	Purpose
1	User	Any	Any	Deny	Yes	This rule denies access to all services on the network and logs the network access attempt.

drop-and-log Policy Configuration

```
!
ip access-list session drop-and-log
  user any any deny log position 1
!
```

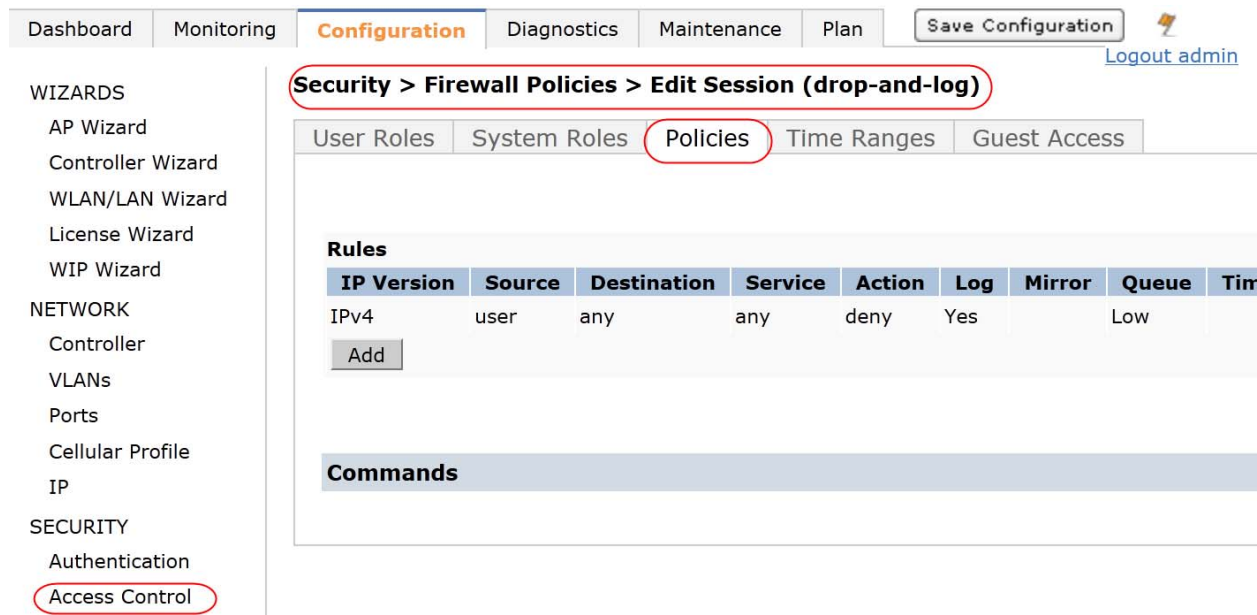


Figure 11 drop-and-log policy

Configuring the guest-logon Role

The guest-logon role is the first role that is assigned to the users when they associate with the guest SSID. Users in this role have access only to the DHCP/DNS services and are redirected to the captive portal page whenever they try to access a web page. The captive portal page requires login credentials. The captive portal authentication profile that is appended to this role specifies the captive portal login page and other configurable parameters such as the default role and the type of login. To create and add the captive portal authentication profile to this guest role, see [Configuring the Captive Portal Authentication Profile](#) on page 30. [Table 10](#) describes the policies in the guest-logon role.

Table 10 guest-logon Role

Policy Number	Policy Name	Purpose
1	captiveportal (predefined policy)	This predefined policy initiates captive portal authentication. This policy redirects any HTTP or HTTPS traffic to port 8080, 8081, or 8088 of the controller. When the controller sees traffic on these ports, it checks the captive portal authentication profile associated with the current role of the user and processes the values specified on this profile.
2	guest-logon-access	This policy allows DHCP and DNS services. For details, see Configuring the guest-logon-access Policy on page 20.

guest-logon Role Configuration

```
!
user-role guest-logon
  access-list session captiveportal position 1
  access-list session guest-logon-access position 2
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Security > User Roles > Edit Role(guest-logon)

User Roles System Roles Policies Time Ranges Guest Access

« Back

Firewall Policies

Name	Rule Count	Location	Action
captiveportal	6		Edit Delete ▲ ▼
guest-logon-access	3		Edit Delete ▲ ▼

Add

Re-authentication Interval

Disabled Change (0 disables re-authentication. A positive value enables authentication 0 - 4096)

Role VLAN ID

Not Assigned Not Assigned ▼ Change

Figure 12 *guest-logon role*

Configuring the auth-guest Role

The auth-guest role is assigned to users after they authenticate successfully through the captive portal. This role is the default role in the captive portal authentication profile. This role allows only HTTP and HTTPS services to Internet.

Sometimes an organization wants its guest users to use the printers in the internal network. In such cases, create a separate policy that allows user traffic to an alias called printers. This alias must include only the IP address of the printers that the guests are allowed to use. Place this policy in the auth-guest user role just above the block-internal-access policy.

Table 11 describes the policies in the auth-guest role.

Table 11 auth-guest Role

Policy Number	Policy Name	Purpose
1	cplogout (predefined policy)	This policy makes the controller present the captive portal logout window. If the user attempts to connect to the controller on the standard HTTPS port (443), the client is NATed to port 8081, where the captive portal server will answer. If this rule is not present, a wireless client may be able to access the administrative interface of the controller.
2	guest-logon-access	This policy denies personal DHCP servers and provides legitimate DHCP services and DNS.
3	block-internal-access	This policy blocks access to internal network. This policy should be placed before the next policy that allows HTTP and HTTPS service, otherwise guest users will have access to the internal websites.
4	auth-guest-access	This policy allows HTTP and HTTPS services to any destination.
5	drop-and-log	Any traffic that does not match the previous policies encounters this policy. This policy denies all services and logs the network access attempt.

auth-guest Role Configuration

```

!
user-role auth-guest
  access-list session cplogout position 1
  access-list session guest-logon-access position 2
  access-list session block-internal-access position 3
  access-list session auth-guest-access position 4
  access-list session drop-and-log position 5
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 > **Access Control**

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General

Security > User Roles > Edit Role(auth-guest)

User Roles System Roles Policies Time Ranges Guest Access

[« Back](#)

Firewall Policies

Name	Rule Count	Location	Action			
cplogout	1		Edit	Delete	▲	▼
guest-logon-access	3		Edit	Delete	▲	▼
block-internal-access	1		Edit	Delete	▲	▼
auth-guest-access	2		Edit	Delete	▲	▼
drop-and-log	1		Edit	Delete	▲	▼

[Add](#)

Re-authentication Interval

Disabled [Change](#) (0 disables re-authentication. A positive value enables authentication 0 - 4096)

Figure 13 *auth-guest*

Configuring the SSID Profile for Guest WLAN

As previously mentioned, guest SSIDs typically do not provide any Layer 2 authentication and encryption. The Layer 2 authentication type used is open. In open authentication, hello messages are exchanged with the client before it is allowed to associate and obtain necessary IP information. All the user traffic is unencrypted. The users that associate to this SSID are placed in the guest VLAN. This WLAN uses captive portal to authenticate the users. Captive portal with open Layer 2 authentication should never be used for employee networks, because captive portal does not provide encryption. The wireless traffic is visible to anyone doing a passive packet capture unless the data is encrypted by higher-layer protocols such as HTTPS and IPsec.



If you require encryption of data for guest users, other Layer 2 authentication types such as WPA2-PSK can be used before the users are redirected to the captive portal. However, this approach requires that credentials such as the pre-shared key are distributed to all guest users.

Table 12 summarizes the parameter in the sample guest SSID profile.

Table 12 Guest SSID Profile

SSID Profile	Network Name (SSID)	Authentication	Encryption	WMM	Purpose
guestnet	Guest	Open	none	—	Guest users. (Captive portal is used to provide Layer 3 authentication.)

Guest SSID Profile Configuration

```
!
wlan ssid-profile "guestnet"
  essid "Guest"
  opmode opensystem
!
```

The screenshot displays the ArubaOS configuration interface for the 'guestnet' SSID profile. The interface is divided into a sidebar and a main configuration area. The sidebar on the left contains navigation links for WIZARDS, NETWORK, SECURITY, and WIRELESS. The main area is titled 'Advanced Services > All Profile Management' and features a list of profiles on the left and configuration details on the right. The 'guestnet' profile is selected, and the 'Basic' tab is active. The 'Network' section shows 'Network Name (SSID)' set to 'Guest'. The '802.11 Security' section shows 'Network Authentication' set to 'None' and 'Encryption' set to 'Open'.

Figure 14 Guest SSID profile configuration

Configuring the Internal Database for Guest Authentication

The user credentials provided by the captive portal users must be authenticated against an authentication server. Any server type available in ArubaOS can be used as an authentication server, including the internal database. If the guest provisioning feature of ArubaOS is required, the internal database must be used as the authentication server.

Create a server group that defines the internal database of the controller as the authentication server. By default, the credentials entered on the captive portal page by the guests are validated against the user credentials in the database of the master controller. So, in a master/local operation all the guest user accounts are created in the internal database of the master controller. For details about using the internal database of the local controllers for guest accounts in master/local deployments, see [Chapter 5: Guest Provisioning](#).

Table 13 lists the parameter in the Guest-internal server group.

Table 13

Server Group	Server
Guest-internal	Internal (predefined)

Server Group Configuration

```
!
aaa server-group "Guest-internal"
    auth-server Internal
!
```

The screenshot shows the ArubaOS configuration interface. The top navigation bar includes Dashboard, Monitoring, Configuration (selected), Diagnostics, Maintenance, and Plan. There are buttons for 'Save Configuration' and 'Logout admin'. The left sidebar lists various configuration sections: WIZARDS, NETWORK, SECURITY, and WIRELESS. Under SECURITY, 'Authentication' is selected. The main content area is titled 'Security > Authentication > Servers'. The 'Servers' tab is selected, and the 'Guest-internal' server group is highlighted. The 'Internal' server is listed under the 'Guest-internal' group. The 'Internal DB' option is selected under the 'Internal' server.

Figure 15 Server group

Configuring the Captive Portal Authentication Profile

As discussed earlier, to authenticate the users who are associated with the guest SSID via captive portal, you must define and attach a captive portal profile to the initial role that is assigned to the guest users. Configurable parameters such as the default role, type of login (user or guest), welcome page, and others are available in a captive portal profile. The default captive portal page in the ArubaOS is customizable.

Table 14 summarizes the most important parameters of the captive portal profile and the configuration used in the example.

Table 14 Captive portal profile

Parameter	Purpose	Sample Configuration (guestnet captive portal profile)
User login	A username and password is necessary to pass captive portal authentication when user login is enabled. Users authenticating through user login are assigned the role specified in the default role field of the captive portal profile.	enabled
Default role	This role is assigned to users after successful authentication through user login.	auth-guest
Guest login	The captive portal does not request any credentials and the users can login by providing a valid email address. Users authenticating through guest login are assigned the role specified in the default guest role field of the captive portal profile. When user login and guest login is enabled, users can login using either credentials or valid email address.	disabled
Default Guest role	This role is assigned to users after successful authentication through guest login.	—
Logout popup window	Presents a logout window after the user is authenticated. If this is disabled, the user will be logged in until the user age-out is reached or until the client device is rebooted. Pop-up blockers in the browsers may block this pop-up.	enabled
Login page	This is the captive portal page that is displayed to the users. This can be the default page, the new customized page, or any external captive portal page such as the one hosted on Amigopod.	/auth/index.html
Welcome page	This is the welcome page that is displayed after successful authentication.	/auth/welcome.html
Show Welcome Page	This enables the welcome page. If disabled, the authenticated user is redirected automatically to the page he was trying to browse initially.	enabled
Allow only one active user session	If enabled, only one active session is allowed per username/password.	enabled
White List	Lists the aliases to which the unauthenticated users are allowed access. For details, see Walled Garden on page 56 .	--

Table 14 Captive portal profile (Continued)

Parameter	Purpose	Sample Configuration (guestnet captive portal profile)
Black List	Lists the aliases to which the unauthenticated users are denied access. For details, see Walled Garden on page 56 .	--
Show the acceptable use policy page	If enabled, it displays the acceptable use policy during captive portal authentication. For detail, see Walled Garden on page 56 .	enabled

Remember to add a server group, which defines internal database as the authentication server, to the captive portal profile.

Captive Portal Configuration

```

!
aaa authentication captive-portal "guestnet"
    default-role "auth-guest"
no guest-logon
server-group "Guest-internal"
logout-popup-window
login-page "/auth/index.html"
welcome-page "/auth/welcome.html"
show-acceptable-use-policy
!

```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 > **Authentication**
 Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

ADVANCED SERVICES
 Redundancy
 IP Mobility
 Stateful Firewall
 External Services

Security > Authentication > L3 Authentication

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Captive Portal Authentication Profile

default
 guestnet
 Server Guest-Group internal

WISPr Authentication Profile
 VPN Authentication Profile
 Stateful NTLM Authentication Profile

Captive Portal Authentication Profile > guestnet Show Reference Save As

Default Role	auth-guest	Default Guest Role	guest
Redirect Pause	3 sec	User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>	Logout popup window	<input checked="" type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	<input type="checkbox"/>
Use CHAP (non-standard)	<input type="checkbox"/>	Login page	/auth/index.html
Welcome page	/auth/welcome.html	Show Welcome Page	<input checked="" type="checkbox"/>
Add switch IP address in the redirection URL	<input checked="" type="checkbox"/>	Allow only one active user session	<input type="checkbox"/>
White List	<input type="text"/> Delete Add	Black List	<input type="text"/> Delete Add
Show the acceptable use policy page	<input type="checkbox"/>		

Figure 16 Captive portal profile (using the sample configuration in Table 14)

The image shows the Aruba Captive Portal page. The background is a blue sky with a grid pattern and a bright sunburst effect. The Aruba logo is prominently displayed in the center. On the left side, there are two login sections. The top section is titled 'REGISTERED USER' and contains fields for 'USERNAME' and 'PASSWORD', followed by a 'Log In' button. The bottom section is titled 'GUEST USER' and contains an 'EMAIL' field, followed by a 'Log In' button. Below the 'GUEST USER' login button, there is a message: 'Logging in as a guest user indicates you have read and accepted the [Acceptable Use Policy](#).'

Figure 17 Captive portal page when user and guest login are enabled

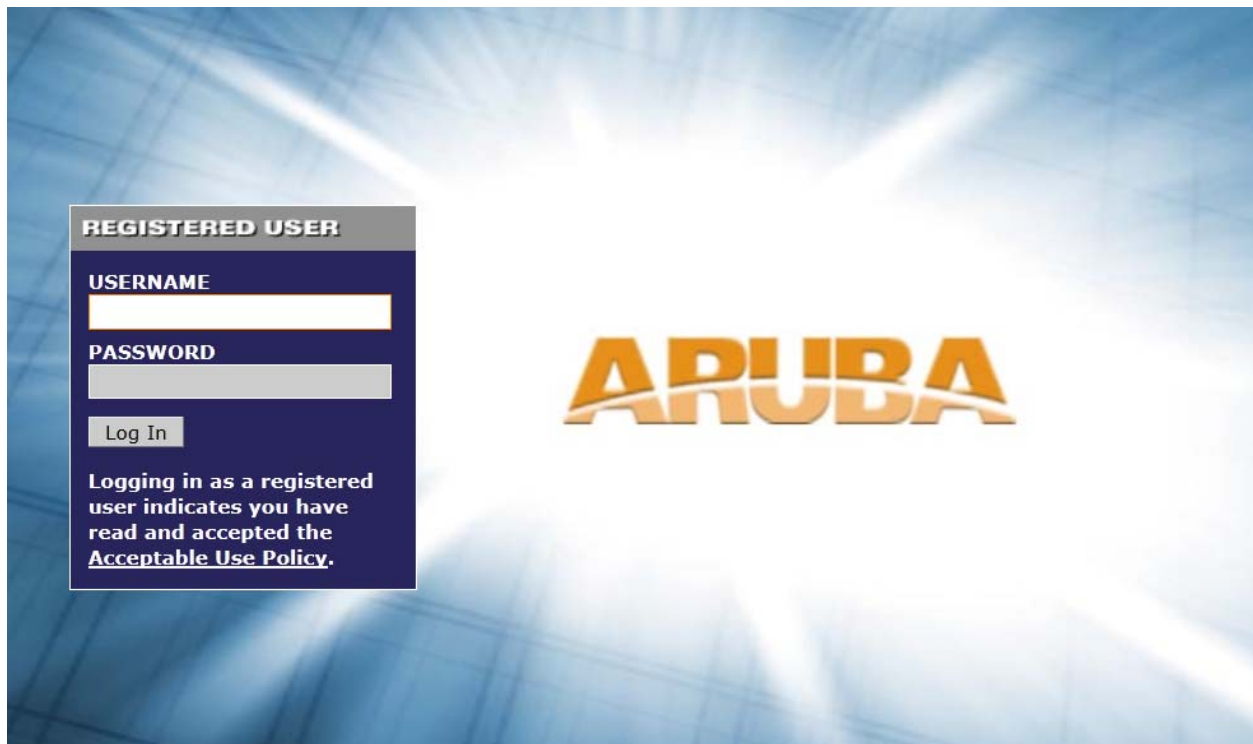
The image shows the Aruba Captive Portal page, similar to Figure 17, but with a different layout. The background is the same blue sky with a grid pattern and a bright sunburst effect. The Aruba logo is prominently displayed in the center. On the left side, there is a single login section titled 'REGISTERED USER'. It contains fields for 'USERNAME' and 'PASSWORD', followed by a 'Log In' button. Below the 'Log In' button, there is a message: 'Logging in as a registered user indicates you have read and accepted the [Acceptable Use Policy](#).'

Figure 18 Captive portal page for user login



Figure 19 *Captive portal page for guest login*

After you configure the captive portal profile, append it to the initial role, which is the guest-logon role in the example configuration.

Appending Captive Portal Profile to Initial Guest Role

```
!  
user-role guest-logon  
  captive-portal guestnet  
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Lc](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 > **Access Control**

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

ADVANCED SERVICES
 Redundancy
 IP Mobility
 Stateful Firewall
 External Services
 VPN Services
 Wired Access
 Wireless
 All Profiles

Security > User Roles > Edit Role(guest-logon)

User Roles System Roles Policies Time Ranges Guest Access

Firewall Policies

Name	Rule Count	Location	Action			
Amigopod	2		Edit	Delete	▲	▼
captiveportal	3		Edit	Delete	▲	▼
guest-logon-access	3		Edit	Delete	▲	▼

[Add](#)

Re-authentication Interval

Disabled [Change](#) (0 disables re-authentication. A positive value enables authentication 0 - 4096)

Role VLAN ID

Not Assigned Not Assigned [Change](#)

Bandwidth Contract

Upstream: Not Enforced [Change](#) Per Role

Downstream: Not Enforced [Change](#) Per Role

VPN Dialer

Not Assigned Not Assigned [Change](#)

PPTP Pool

default-pptp-pool Not Assigned [Change](#)

Captive Portal Profile

guestnet Not Assigned [Change](#)

VIA Connection Profile

Not Assigned Not Assigned [Change](#)

Max Sessions

128 [Change](#) (0 - 65535)

Stateful NTLM Profile

Not Assigned Not Assigned [Change](#)

Figure 20 Appending the captive portal profile to the initial guest role

Configuring the AAA Profile for Guest WLAN

The AAA profile defines the user role assigned to authenticated and unauthenticated users. Since the guest SSID is open, any user associating is given the user role specified as the initial role in the AAA profile. The initial guest role should be the initial role in the AAA profile. In the example configuration this is the guest-logon role.

Table 15 lists the initial role of the guest AAA profile.

Table 15 Guest AAA Profile

AAA Profile Name	Initial Role
guestnet	guest-logon

Guest AAA Profile Configuration

```
!
aaa profile "guestnet"
  initial-role "guest-logon"
!
```

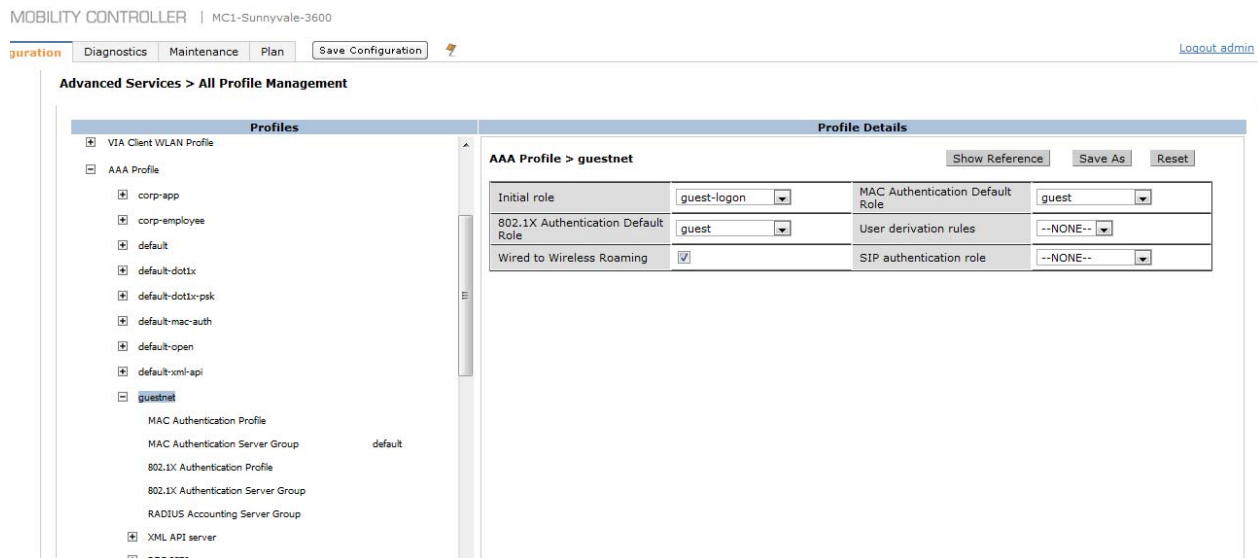


Figure 21 Guest AAA profile configuration

After completing all the above configurations, create the required VAP profile and attach it to an AP group. For details about configuring the VAP profiles and AP groups, see the [Aruba Campus Wireless Networks Validated Reference Design](#).

Chapter 5: Guest Provisioning

Guest provisioning allows authenticated non-IT members to create and delete visitor accounts. Guest provisioning eliminates the need for an IT staff to be involved every time a user account has to be created. A guest-provisioning user is usually a front-desk person, such as a receptionist, but it can be anyone in the organization. As mentioned before, to use the guest-provisioning capabilities of the base ArubaOS software, the internal database on the controller must be used as the authentication server for captive portal authentication. The user accounts can be created in the internal database of the controller by the members of the IT team who have root access to the controller and by authenticated guest-provisioning users. An authenticated guest-provisioning user can only create guest accounts. A guest-provisioning user does not see the same interface seen by a root user, but instead he is presented with a guest provisioning page. The guest provisioning user can create, delete, or modify the guest accounts that they create.



A guest user account that is created by a guest provisioning user can only be viewed, modified, or deleted by the guest-provisioning user who created the account or by the network administrator. A guest user account that is created by the network administrator can only be viewed, modified, or deleted by the network administrator.

Configuring Guest Provisioning User

You can configure and authenticate a guest-provisioning user in one of three ways:

- Local authentication on the controller using user name and password
- Smart cards
- Other External authentication servers supported on ArubaOS

A guest-provisioning users should always authenticate to the mobility controller that holds the account database, usually the master. The guest accounts created by a guest-provisioning user are always added to the internal database of the controller to which the guest-provisioning user authenticated.

In master/local deployments, the guest credentials are authenticated against the internal database of the master controller by default. However, certain deployments may require that the guest accounts in a region reside on the local controller for that region. The requirements for using the internal database of the local controller for guest authentication in a master/local deployment are these:

1. The local controller must be configured to use the internal database of the local controllers and not the master to authenticate the users terminating on that local controller. To configure this, issue the “aaa authentication-server internal use-local-switch” command in the command line interface (CLI) of the local controller that has to use its internal database to authenticate users.
2. Guest-provisioning accounts must be created on the local controller that will be using its internal database for guest authentication. These guest-provisioning users authenticate to the local controller and the guest accounts created by them are added to the internal database on the local controller.

A network administrator with root access to the controller can create a guest-provisioning user on the controller for local authentication. To create guest-provisioning user, add a management user account with the role set to guest-provisioning. The predefined guest-provisioning role available on the ArubaOS software cannot be edited.

Creating a Guest-Provisioning User Account on the Controller

```
!
mgmt-user "receptionist" "guest-provisioning" *****
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

WIZARDS
AP Wizard
Controller Wizard
WLAN/LAN Wizard
License Wizard
WIP Wizard

NETWORK
Controller
VLANs
Ports
Cellular Profile
IP

SECURITY
Authentication
Access Control

WIRELESS
AP Configuration
AP Installation

MANAGEMENT
General
Administration
Certificates
SNMP

Management > Administration > Add User Back

Add User

☒ Conventional User Accounts

User Name receptionist

Password

Confirm Password

Role guest-provisioning

☐ Certificate Management

☐ WebUI Certificate ☐ Use external authentication server to authenticate

Username

Role root

Client

Certificate Serial No.

Trusted CA

Certificate Name Default

☐ SSH Public Key ☐ Copy The WebUI Certificate Management Information (username and role)

Username

Role root

Client

Certificate name

Apply

Figure 22 Creating a guest-provisioning user on the Aruba controller

Configuring the Guest-Provisioning Page

The guest-provisioning page (GPP) is the web page that is displayed to the authenticated guest-provisioning users. GPP is used by the guest-provisioning users to create, delete, and modify accounts. The GPP that is displayed to an authenticated guest-provisioning user can be modified. The network administrator can modify the fields displayed in the GPP, the design of the GPP, and the email options for the created accounts.

Modifying Guest Fields on the GPP

When a guest-provisioning user creates a guest user account, he is required to enter certain information about the guest such as the guest username, password, company name, email ID, and phone number. The guest fields on the GPP define the information that a guest-provisioning user has to supply when he creates a guest account. These guest fields can be modified.

The Guest Fields tab has these columns:

- **Internal Name:** The unique identifier that is mapped to the label in the UI. This field cannot be edited.
- **Label in UI:** Name of the field display on the main GPP and while creating guest accounts.
- **Display in Details:** The fields of the guest account that are selected as “display in details” are hidden from the main GPP. These fields are shown only when the show details parameter in the GPP is enabled and a user account is selected.
- **Display in Listing:** These fields of the guest account are displayed on the main GPP by default.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration

WIZARDS
AP Wizard
Controller Wizard
WLAN/LAN Wizard
License Wizard
WIP Wizard

NETWORK
Controller
VLANs
Ports
Cellular Profile
IP

SECURITY
Authentication
Access Control

WIRELESS
AP Configuration
AP Installation

MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock

Management > Guest Provisioning

Guest Fields Page Design Email

Specify the fields you wish to appear on the Guest Provisioning Page. [Help](#)

Field	Internal Name	Label in UI	Display In	
			Details	Listing
guest_category		Guest	<input checked="" type="checkbox"/>	<input type="checkbox"/>
guest_username		Username	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
guest_password		Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>
guest_fullname		Full name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
guest_company		Company	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
guest_email		Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
guest_phone		Phone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
comments		Comments	<input checked="" type="checkbox"/>	<input type="checkbox"/>
account_category		Account	<input checked="" type="checkbox"/>	<input type="checkbox"/>
creation_date		Created	<input checked="" type="checkbox"/>	<input type="checkbox"/>
start_date		Start	<input checked="" type="checkbox"/>	<input type="checkbox"/>

> Guest Provisioning

Figure 23 Editing guest-provisioning fields

Guests

Guest		
Username	Full name	Com
guest100	guest10	xxxx
guest101	guest101	yyyy

New Guest

Guest

Username:*

Generate

Password:*

Generate

Retype:*

Full name:

Company:

Email:

Phone:

Comments:

Account

Start:

Sep 08, 2011 06:07 PM

End:

Sep 09, 2011 02:07 AM

Sponsor

Username:

Full name:

Department:

Email:

CreateCreate & PrintCancel

Figure 24 Guest-provisioning fields displayed on the GPP

Logout Username

Guests

Show detailsNewImportDeletePrintEdit

Guest				
Username	Full name	Company	Email	Phone
guest100	guest10	xxxx	xxxx@xxx.com	000-000-0000
guest101	guest101	yyyyy	yyyy@yyy.com	111-111-1111



Figure 25 Display In Listing fields shown on the GPP

Logout Username

Guests

☒ Show details

NewImportDeletePrintEdit

Guest	Username	Full name	Company	Email	Phon
	guest100	guest10	xxxx	xxxx@xxx.com	000-
	guest101	guest101	yyyyy	yyyy@yyy.com	111-

guest100

Guest

Username:*
Full name:
Company:
Email:
Phone:
Comments:

guest100
guest10
xxxx
xxxx@xxx.com
000-000-0000
--

Send Email Now

Account

Created:
Start:
End:
Grantor:
Grantor Role:

Sep 08, 2011 06:04 PM
Sep 08, 2011 06:04 PM
Sep 09, 2011 02:04 AM
provision
guest-provisioning

Sponsor

Username:
Full name:
Department:
Email:

jim
jim smith
front desk
jim@aaa.com

Send Email Now

Figure 26 *Display In Details fields shown only when the Show details field is enabled on the GPP*

Modifying Page Design of the GPP

The page design of the GPP can be modified to add or change the company banner, heading and text, and background colors that appear on the GPP.

The screenshot shows the ArubaOS configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (highlighted), 'Diagnostics', 'Maintenance', 'Plan', and 'Save Configuration'. The left sidebar lists various configuration categories: WIZARDS (AP Wizard, Controller Wizard, WLAN/LAN Wizard, License Wizard, WIP Wizard), NETWORK (Controller, VLANs, Ports, Cellular Profile, IP), SECURITY (Authentication, Access Control), WIRELESS (AP Configuration, AP Installation), and MANAGEMENT (General, Administration, Certificates, SNMP, Logging, Clock). The 'Guest Provisioning' link under MANAGEMENT is highlighted with a red circle. The main content area shows the 'Management > Guest Provisioning' breadcrumb, with 'Page Design' selected. Below this, there are tabs for 'Guest Fields', 'Page Design', and 'Email'. The 'Page Design' tab is active, showing options to specify the logo and colors for the Guest Provisioning Page. A 'Banner' field with a 'Browse...' button is present. A 'Text' field contains the word 'Guests'. The 'Text Color' is set to '000000' (black) with a color swatch. The 'Background color' is set to 'b0d2eb' (light blue) with a color swatch. A 'Help' link is also visible.

Figure 27 GPP Page Design

Email Options for the GPP

The email options of guest provisioning allows you to edit the subject, from address field and the body of the email send, to the guests and sponsors. Emails can be chosen to be sent automatically when an account is created or manually from the GPP at any time.

To send emails to the guests and sponsors from the controller, the simple mail transfer protocol (SMTP) parameters on the controller must be configured. To configure SMTP on the controller, this information is required:

- IP address of the SMTP server
- SMTP port number (port 25)

Aruba controller does not support the use of secure simple mail transfer protocol (SMTPS).

SMTP Configuration

```
!  
guest-access-email  
  smtp-server "10.10.10.100"  
  smtp-port 25  
!
```

The screenshot displays the ArubaOS web interface. At the top, a navigation bar includes tabs for Dashboard, Monitoring, Configuration (highlighted in orange), Diagnostics, Maintenance, and Plan. On the left, a sidebar menu lists various configuration categories: WIZARDS, NETWORK, SECURITY, WIRELESS, and MANAGEMENT. Under MANAGEMENT, the 'SMTP' option is circled in red. The main content area shows the 'Management > SMTP' configuration page. It features two input fields: 'IP Address of SMTP server:' with the value '10.10.10.100' and 'Port:' with the value '25'. Below these fields is a 'Commands' section, which is currently empty.

Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Plan
Management > SMTP					
IP Address of SMTP server: <input type="text" value="10.10.10.100"/>					
Port: <input type="text" value="25"/>					
Commands					

Figure 28 SMTP configuration for sending guest-provisioning emails

Modifying Email Options

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
Guest Provisioning

Management > Guest Provisioning

Guest Fields Page Design Email

Specify optional message to be sent to the guest and sponsor. [Help](#)

Guest Message

Subject: Guest account information

From: a@a.com

Body: A guest account has been created for your use. The username, password and valid dates for the account are given below.

☐ Send automatically at account creation time

Sponsor Message

Subject: Guest account information

From: a@a.com

Body: You are listed as the Sponsor for the following guest account.

☐ Send automatically at account creation time

Figure 29 Guest-provisioning email options

Creating Guest User Accounts

The users with root access to the controller can create the guest accounts directly in the internal database or they can navigate to the < https://<controller IP or FQDN>/switch/gpp.html> and login using their root access credential to view the GPP and create guest accounts on it.

For guest-provisioning users, the guest accounts created in the GPP are added automatically to the internal database of the controller to which the guest-provisioning users authenticated. ArubaOS provides the option of importing a list of guest user accounts in CSV file format. Remember that a guest-provisioning user can create only guest accounts.

To create a guest account on the GPP, the guest-provisioning user must perform these tasks:

1. Click the **New** tab on the GPP.
2. Fill the guest fields.
3. If required, send emails manually.



Guest user accounts are automatically removed from the internal database when they expire.

[Logout Username](#)

Guests					<input type="checkbox"/> Show details	New	Import	Delete	Print	Edit
Guest			Account							
Username	Full name	Company	Start				End			
 guest11	a	a	Aug 23, 2011 08:12 AM				Aug 23, 2011 04:12 PM			

Figure 30 Creating guest accounts using guest provisioning (step 1)

New Guest

Guest

Username:*

Password:*

Retype:*

Full name:

Company:

Email:

Phone:

Comments:

Account

Start:

End:

Sponsor

Username:

Full name:

Department:

Email:

Figure 31 Creating guest accounts using guest provisioning (step 2)

[Logout Username](#)

Guests ☒ Show details [New](#) [Import](#) [Delete](#) [Print](#) [Edit](#)

Guest	Username	Full name	Company	Email	Phone
guest101	guest101	guest101	xxxxxx	guest101@xxx.com	000-000-0000

guest101

Guest

Username: * guest101
 Full name: guest101
 Company: xxxxxx
 Email: guest101@xxx.com
 Phone: 000-000-0000
 Comments: --

[Send Email Now](#)

Account

Created: Sep 09, 2011 02:24 PM
 Start: Sep 09, 2011 02:20 PM
 End: Sep 09, 2011 10:20 PM
 Grantor: receptionist-1
 Grantor Role: guest-provisioning

Sponsor

Username: aaaa
 Full name: aaaa
 Department: Marketing
 Email: aaa@bbb.com

[Send Email Now](#)

Figure 32 Manually sending emails for guests and sponsors from GPP

Configuration [Diagnostics](#) [Maintenance](#) [Plan](#) [Save Configuration](#) [Logout admin](#)

Monitoring **Security > Authentication > Servers**

Servers [AAA Profiles](#) [L2 Authentication](#) [L3 Authentication](#) [User Rules](#) [Advanced](#)

- Server Group
- RADIUS Server
- LDAP Server
- Internal DB**
- Tacacs Accounting Server
- TACACS Server
- XML API Server
- RFC 3576 Server
- Windows Server

Internal DB Maintenance

Maximum Expiration min

[Guest User Page](#) [Export](#) [Import](#) [Delete All Users](#) [Repair Database](#)

Users

User Name	Password	Role	E-mail	Enabled	Expiry	IP-Address	Action
guest3	*****	guest	Yes			0.0.0.0	Disable Delete Modify
guest4	*****	guest	Yes			0.0.0.0	Disable Delete Modify
guest1	*****	guest	Yes			0.0.0.0	Disable Delete Modify

[Add User](#)

1 | 1-3 of 3

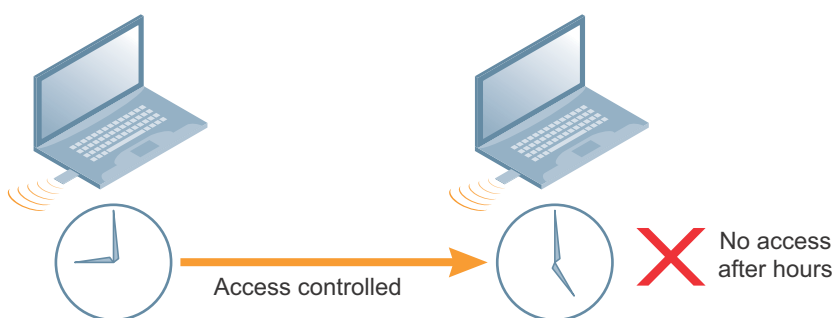
Figure 33 Creating guest accounts directly on the internal database using root access

Chapter 6: Optional Configurations for Guest Network

All the configurations explained in [Chapter 4: Captive Portal Configuration](#) and [Chapter 5: Guest Provisioning](#) are necessary to build a functional guest network with guest provisioning. In addition, ArubaOS provides features such as bandwidth contracts, walled garden, and time range that are optional and are not critical for the operation for a guest WLAN. This chapter explains these optional features in detail.

Time Range

A time-of-day restriction policy can be used to allow guests to access the network only during normal working hours, because they should be using the network only while conducting official business. A time-of-day restriction policy prevents guest users from using the network after normal working hours. You can define a time range in ArubaOS that can be used in firewall policies to allow users to associate to the guest network only during certain hours of the day.



arun_060

Figure 34 Guest access with a time limit

The types of time ranges available are these:

1. Absolute: This time range starts and ends on a specific date and at a specific time.
2. Periodic: This recurring time-range starts and ends at a specific time. The recurring interval can be set to be daily, weekdays, weekends, or any particular day of the week.

[Table 16](#) lists the parameters used in the configuration of a time range named Working-hours.

Table 16 Time Range

Name	Type	Start Date	Start Time	End Time
Working-hours	periodic	weekday	07:00	17:30

Time Range Configuration

```
!
time-range "Working-hours" periodic Weekday 07:00 to 17:30
!
```

The screenshot shows the ArubaOS configuration interface. The breadcrumb path is **Security > Access Control > TimeRange > Edit Time Range(Working-hours)**. The left sidebar shows the navigation menu with **Access Control** selected. The main content area has tabs for **User Roles**, **System Roles**, **Policies**, **Time Ranges** (selected), and **Guest Access**. The **Time Ranges** tab shows a configuration for **Working-hours** with the following details:

- Name:** Working-hours
- Type:** ☒ Absolute ☒ Periodic
- Start Day:** weekday
- Start Time:** 7:30
- End Day:**
- End Time:** 17:30
- Actions:**

There is an **Add** button below the table and an **Apply** button at the bottom right. A **Commands** section at the bottom has a **View Commands** link.

Figure 35 Time range

Time range can be used as a part of the rules in a firewall policy to impose an action during a particular time. For example, if the guest access is to be allowed only during 7:30 am to 5:30 pm on weekdays, then a time range should be attached to certain rules of some guest firewall policies. To impose a time range for guest access, add a time range to rules 2 and 3 in the guest-logon-access policy and to the both the rules in the auth-guest-access policy.

Time Range Configuration for guest-logon-access and auth-guest-access Policies

```
!
ip access-list session guest-logon-access
  user any udp 68 deny position 1
  any any svc-dhcp permit time-range Working-hours position 2
  user alias Public-DNS svc-dns permit time-range Working-hours position 3
!
!
ip access-list session auth-guest-access
  user any svc-http permit time-range Working-hours position 1
  user any svc-https permit time-range Working-hours position 2
!
```


Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
> Access Control

WIRELESS
 AP Configuration

Security > User Roles > Edit Role(guest-logon) > Edit Session (guest-logon-access)

User Roles System Roles Policies Time Ranges Guest Access

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
IPv4	user	any	udp 68	deny			Low	
IPv4	any	any	svc-dhcp	permit			Low	Working-hours
IPv4	user	Public-DNS	svc-dns	permit			Low	Working-hours
Add								

Figure 36 *guest-logon-access policy with time range*

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT

Security > Firewall Policies > Edit Session (auth-guest-access)

User Roles System Roles Policies Time Ranges Guest Access

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
IPv4	user	any	svc-http	permit			Low	Working-hours
IPv4	user	any	svc-https	permit			Low	Working-hours
Add								

Commands

Figure 37 *auth-guest-access policy with time range*

An alternative method of using time range to restrict guest access to business hours or a particular time is by using the deny time range parameter of the VAP profile. If configured, the deny time range parameter of the VAP profile will deny access to the associated SSID during the defined time range. If guest access is to be restricted to business hours then define a time range that includes the non-business hours and add it to the deny time range parameter of the VAP profile.

Table 17 shows the parameters used in the configuration of deny-access time range.

Table 17 deny-access time range

Name	Type	Start Date	Start Time	End Time
deny-access	periodic	weekday	17:30	23:59
deny-access	periodic	weekday	00:00	07:30
deny-access	periodic	weekend	00:00	23:59

Deny Time Range Parameter Configuration

```

!
time-range "deny-access" periodic Weekday 17:30 to 23:59
time-range "deny-access" periodic Weekday 00:00 to 07:30
time-range "deny-access" periodic Weekend 00:00 to 23:59
!
wlan virtual-ap "guestnet"
deny-time-range deny-access

```

Configuration | Diagnostics | Maintenance | Plan | [Save Configuration](#) | [Logout admin](#)

Security > Access Control > TimeRange > Edit Time Range(deny-access) | [« Back](#)

User Roles | System Roles | Policies | **Time Ranges** | Guest Access

Name: deny-access

Type: ☐ Absolute ☒ Periodic

Start Day	Start Time	End Day	End Time	Actions
weekday	17:30		23:59	Delete
weekday	00:00		07:30	Delete
weekend	00:00		23:59	Delete

[Add](#) [Apply](#)

Commands [View Commands](#)

Figure 38 Deny access time range

Configuration | Diagnostics | Maintenance | Plan | Save Configuration | Logout admin

Advanced Services > All Profile Management

Profiles	Profile Details																																								
<ul style="list-style-type: none"> AP RF Management Wireless LAN <ul style="list-style-type: none"> 802.11K Profile SSID Profile High-throughput SSID profile Virtual AP profile <ul style="list-style-type: none"> Corp-App-LC1-Sunnyvale-6000 Corp-App-LC2-Sunnyvale-6000 Corp-Employee-LC1-Sunnyvale-6000 Corp-Employee-LC2-Sunnyvale-6000 Corp-Employee-TLS-LC1-Sunnyvale-6000 default guestnet AAA Profile 	<p>Virtual AP profile > guestnet Show Reference Save As Reset</p> <table border="1"> <tr> <td>Virtual AP enable</td> <td><input checked="" type="checkbox"/></td> <td>Allowed band</td> <td>all</td> </tr> <tr> <td>VLAN</td> <td>900</td> <td>Forward mode</td> <td>tunnel</td> </tr> <tr> <td>Deny time range</td> <td>deny-access</td> <td>Mobile IP</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>HA Discovery on-association</td> <td><input type="checkbox"/></td> <td>DoS Prevention</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Station Blacklisting</td> <td><input checked="" type="checkbox"/></td> <td>Blacklist Time</td> <td>3600 sec</td> </tr> <tr> <td>Dynamic Multicast Optimization (DMO)</td> <td><input type="checkbox"/></td> <td>Dynamic Multicast Optimization (DMO) Threshold</td> <td>6</td> </tr> <tr> <td>Authentication Failure Blacklist Time</td> <td>3600 sec</td> <td>Multi Association</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Strict Compliance</td> <td><input type="checkbox"/></td> <td>VLAN Mobility</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Preserve Client VLAN</td> <td><input type="checkbox"/></td> <td>Remote-AP Operation</td> <td>standard</td> </tr> <tr> <td>Drop Broadcast and Multicast</td> <td><input type="checkbox"/></td> <td>Convert Broadcast ARP requests to unicast</td> <td><input type="checkbox"/></td> </tr> </table>	Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all	VLAN	900	Forward mode	tunnel	Deny time range	deny-access	Mobile IP	<input checked="" type="checkbox"/>	HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>	Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 sec	Dynamic Multicast Optimization (DMO)	<input type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	6	Authentication Failure Blacklist Time	3600 sec	Multi Association	<input type="checkbox"/>	Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>	Preserve Client VLAN	<input type="checkbox"/>	Remote-AP Operation	standard	Drop Broadcast and Multicast	<input type="checkbox"/>	Convert Broadcast ARP requests to unicast	<input type="checkbox"/>
Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all																																						
VLAN	900	Forward mode	tunnel																																						
Deny time range	deny-access	Mobile IP	<input checked="" type="checkbox"/>																																						
HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>																																						
Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 sec																																						
Dynamic Multicast Optimization (DMO)	<input type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	6																																						
Authentication Failure Blacklist Time	3600 sec	Multi Association	<input type="checkbox"/>																																						
Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>																																						
Preserve Client VLAN	<input type="checkbox"/>	Remote-AP Operation	standard																																						
Drop Broadcast and Multicast	<input type="checkbox"/>	Convert Broadcast ARP requests to unicast	<input type="checkbox"/>																																						

Figure 39 Deny time range parameter of the VAP profile

Bandwidth Contracts

The amount of upstream and downstream bandwidth used by guests can be limited using bandwidth contracts. A bandwidth contract policy rate limits the traffic to the configured value as it flows through the controller. Bandwidth contracts can be assigned on per role or per user basis. When a bandwidth contract is created on per user basis, each user can pass traffic equivalent or less than the configured rate. If the bandwidth contract is created on per role basis, then the bandwidth pool is shared by all the users that belong to that role. The bandwidth is configurable in Kb/s or Mb/s and separate bandwidth contracts can be assigned for upstream and downstream traffic.

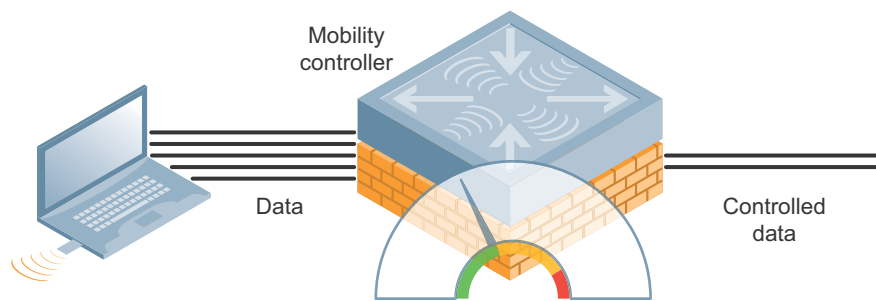


Figure 40 Guest access with bandwidth limit

Table 18 lists the parameters used in the configuration of separate per role bandwidth contracts for upstream and downstream traffic.

Table 18 Bandwidth Contracts

Name	Type	Rate	Purpose
guest-upstream	per role	1 Mb/s	used as upstream bandwidth contract for authenticated guest role (auth-guest)
guest-downstream	per role	3 Mb/s	used as downstream bandwidth contract for authenticated guest role (auth-guest)

Bandwidth Contracts Configuration for Authenticated Guest Role

```

!
aaa bandwidth-contract "guest-upstream" mbits 1
!
aaa bandwidth-contract "guest-downstream" mbits 3
!
user-role "auth-guest"
bw-contract "guest-upstream" upstream
bw-contract "guest-downstream" downstream
!

```

Configuration Diagnostics Maintenance Plan Save Configuration [Logout admin](#)

Security > User Roles > Edit Role(auth-guest)

User Roles System Roles Policies Time Ranges Guest Access

« Back

Firewall Policies

Name	Rule Count	Location	Action
cplogout	1		Edit Delete ▲ ▼
guest-logon-access	3		Edit Delete ▲ ▼
block-internal-access	1		Edit Delete ▲ ▼
auth-guest-access	2		Edit Delete ▲ ▼
drop-and-log	1		Edit Delete ▲ ▼
Add			

Re-authentication Interval

Disabled Change (0 disables re-authentication. A positive value enables authentication 0 - 4096)

Role VLAN ID

Not Assigned Not Assigned Change

Bandwidth Contract

Upstream: Not Enforced Add New... Change ☐ Per User

Downstream: Not Enforced Change ☐ Per User

New Bandwidth Contract

Name guest-upstream

Bandwidth 1 mbps

Done Cancel

Figure 41 Bandwidth contracts for authenticated guest role

Maximum User Sessions for Guest Role

Though it is a very small possibility, a malicious user can connect to the guest network and initiate a denial of service (DoS) attack by using up all of the 65535 sessions available. To defend against such an attack, restrict the maximum number of sessions per user in a role. Aruba recommends that you restrict the maximum sessions per user in the guest role to 128. This limitation should be placed on all the roles used in the guest network.

Maximum User Sessions Configuration

```
!  
user-role guest-logon  
    max-sessions 128  
!  
user-role auth-guest  
    max-sessions 128  
!
```

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
> Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

ADVANCED SERVICES
 Redundancy
 IP Mobility
 Stateful Firewall
 External Services
 VPN Services
 Wired Access
 Wireless
 All Profiles

Security > User Roles > Edit Role(guest-logon)

User Roles System Roles Policies Time Ranges Guest Access

Firewall Policies

Name	Rule Count	Location	Action			
Amigopod	2		Edit	Delete	▲	▼
captiveportal	3		Edit	Delete	▲	▼
guest-logon-access	3		Edit	Delete	▲	▼

[Add](#)

Re-authentication Interval

Disabled [Change](#) (0 disables re-authentication. A positive value enables authentication 0 - 4096)

Role VLAN ID

Not Assigned [Change](#)

Bandwidth Contract

Upstream: Not Enforced [Change](#) Per Role

Downstream: Not Enforced [Change](#) Per Role

VPN Dialer

Not Assigned [Change](#)

PPTP Pool

default-pptp-pool [Change](#)

Captive Portal Profile

guestnet [Change](#)

VIA Connection Profile

Not Assigned [Change](#)

Max Sessions

128 [Change](#) (0 - 65535)

Stateful NTLM Profile

Not Assigned [Change](#)

Figure 42 Maximum user sessions for guest role

Walled Garden

The walled garden feature of the ArubaOS, which is a part of captive portal authentication, allows access by unauthenticated guest to certain websites. The whitelist feature of walled garden (available in the captive portal profile) allows you to define a list of websites to which unauthenticated users are allowed access. The blacklist feature of walled garden can be configured to explicitly block navigation to certain websites from unauthenticated guests. This feature is very useful for businesses such as hotels, which want guests to access their websites for free, but require them to pay for Internet services.

Configuring walled garden includes the following two steps:

1. Create an alias for the allowed or disallowed websites.
2. To allow unauthenticated guests to access the websites defined in the alias, add the alias to the whitelist of the captive portal profile used for guest access. If you want to deny access, add the alias to the blacklist of the captive portal profile.



If you want to allow or deny access using walled garden to just a website, include the entire hostname in the alias such as www.arubanetworks.com (include all prefixes, such as WWW). If you just use the domain name such as arubanetworks.com in the alias, then all of the domain and subdomain hostnames that can be resolved are accessible by the unauthenticated guest users. In deployments that use internal DNS servers for guest networks, whitelisting the entire domain allows unauthenticated guests access to all the internal hostnames that can be resolved by the internal DNS server.

Table 19 summarizes the configuration of the walled-garden-access alias, which defines the hostname www.arubanetworks.com.

Table 19 walled-garden-access Alias

Alias Name	IP Address/ Range	Purpose
walled-garden-access	www.arubanetworks.com	Define the websites to which unauthenticated guests are allowed access.

Walled Garden Configuration

```
!
netdestination walled-garden-access
name www.arubanetworks.com
!
aaa authentication captive-portal "default"
white-list walled-garden-access
!
```


Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT

Advanced Services > Stateful Firewall > Destinations > Add Destination [« Back](#)

Global Setting White List BW Contracts Network Services **Destination**

BW Contracts BW Contracts Exception List

IP Version IPv4 ▾

Destination Name walled-garden-access

Invert ☐

Type	IP Address	NetMask/Range	Actions
Add			

Add Rule

Rule Type name ▾

Domain Name www.arubanetworks.com

Add Cancel

Apply

Commands [View Commands](#)

Figure 43 *walled-garden-access alias*

Configuration Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Security > Authentication > L3 Authentication

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Captive Portal Authentication Profile

- default
- guestnet**

Server Group Guest-internal

WISPr Authentication Profile

VPN Authentication Profile

Stateful NTLM Authentication Profile

VIA Authentication Profile

VIA Connection Profile

VIA Web Authentication

Captive Portal Authentication Profile > guestnet [Show Reference](#) [Save As](#) [Reset](#)

Default Role	auth-guest ▾	Default Guest Role	guest ▾
Redirect Pause	10 sec	User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>	Logout popup window	<input checked="" type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	<input type="checkbox"/>
Use CHAP (non-standard)	<input type="checkbox"/>	Login page	https://10.169.130.50/A
Welcome page	http://www.arubanetwc	Show Welcome Page	<input checked="" type="checkbox"/>
Add switch IP address in the redirection URL	<input type="checkbox"/>	Allow only one active user session	<input type="checkbox"/>
White List	walled-garden-access Delete	Black List	Delete
	Add		Add
Show the acceptable use policy page	<input checked="" type="checkbox"/>		

Figure 44 *walled-garden (captive portal whitelist)*

Prioritizing Employee Traffic Using Traffic Management Profile

While a rate limit can be put on each guest user, you may also want to limit access to the wireless medium to keep the guest from using up the limited wireless airtime. Rate limiting on wireless medium can be implemented using the traffic management profile. The traffic management profile is used to provide a service level agreement (SLA). The SLA guarantees a minimum percentage of available bandwidth to be allocated to a VAP when the wireless network is congested. During congestion the traffic is shaped depending on the configured percentage. Remember to leave enough bandwidth to keep the system usable by guests. Aruba recommends a minimum of 10% of total bandwidth be made available to guests. Guests can always burst when the medium is idle.

For more information on traffic management profile and its configuration, see the [Aruba Campus Wireless Networks Validated Reference Design](#).

Optional SSID and VAP Profile Parameters for Guest Network

In addition to the standard SSID and VAP profile configurations used for guest WLANs, certain parameters in these profiles can be tweaked depending on the guest network requirements of an organization.

Disabling lower Data Rates

In the SSID profile, network administrators might choose to disable lower transmit rates of 1 and 2 to prevent clients in the parking lot being associated to the network and consuming DHCP leases. This behavior is quite common with devices such as smartphones. Disabling the lower rates forces the clients to get closer to the building in order to get associated and eliminates the possibility of the parking lot clients consuming the DHCP leases of your guest network. To disable lower transmit rates, make these changes to the SSID profile

1. Disable the 802.11g transmit rates of 1 and 2
2. Change the 802.11g basic rates from 1 and 2 to 5 and 11.

Remember that disabling the lower rates causes connectivity issues with some handheld devices and most games consoles such as PS3, Nintendo Wii and Xbox. Most guest networks are not built to support such devices, so disabling the lower data rates might be an acceptable option in guest networks. However, turning off lower data rates in student dormitories will result in huge volume of support calls due to the behavior of most gaming consoles. Aruba strongly recommends that you test the devices that are expected to connect to a WLAN for connectivity issues before turning off the lower data rates in that WLAN.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

WIZARDS
 AP Wizard
 Controller Wizard
 WLAN/LAN Wizard
 License Wizard
 WIP Wizard

NETWORK
 Controller
 VLANs
 Ports
 Cellular Profile
 IP

SECURITY
 Authentication
 Access Control

WIRELESS
 AP Configuration
 AP Installation

MANAGEMENT
 General
 Administration
 Certificates
 SNMP
 Logging
 Clock
 Guest Provisioning
 Captive Portal
 SMTP
 Bandwidth Calculator

ADVANCED SERVICES

Advanced Services > All Profile Management

Profiles

- AP
- RF Management
- Wireless LAN
 - 802.11K Profile
 - SSID Profile
 - Corp-App
 - Corp-Employee
 - default
 - Employee-TLS
 - guestnet
 - EDCA Parameters Station profile
 - EDCA Parameters AP profile
 - High-throughput SSID Profile default
 - test-rde-tunnel
 - High-throughput SSID profile
 - Virtual AP profile
 - VIA Client WLAN Profile
 - AAA Profile
 - XML API Server
 - RFC 3576 Server

Profile Details

SSID Profile > guestnet [Show Reference](#) [Save As](#) [Reset](#)

Basic **Advanced**

SSID enable	<input checked="" type="checkbox"/>	ESSID	Guest
Encryption	<input checked="" type="checkbox"/> opensystem	<input type="checkbox"/> static-wep	
	<input type="checkbox"/> dynamic-wep	<input type="checkbox"/> wpa-tkip	
	<input type="checkbox"/> wpa-aes	<input type="checkbox"/> wpa-psk-tkip	
	<input type="checkbox"/> wpa-psk-aes	<input type="checkbox"/> wpa2-aes	
	<input type="checkbox"/> wpa2-psk-aes		
	<input type="checkbox"/> wpa2-psk-tkip		
	<input type="checkbox"/> wpa2-tkip		
	DTIM Interval	1 beacon periods	Station Ageout Time
802.11g Transmit Rates	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 24 <input checked="" type="checkbox"/> 36 <input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 54		
802.11g Basic Rates	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 9 <input checked="" type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 18 <input type="checkbox"/> 24 <input type="checkbox"/> 36 <input type="checkbox"/> 48 <input type="checkbox"/> 54		
802.11a Transmit Rates	<input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 24 <input checked="" type="checkbox"/> 36 <input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 54		
802.11a Basic	<input checked="" type="checkbox"/> 6 <input type="checkbox"/> 9 <input checked="" type="checkbox"/> 12 <input type="checkbox"/> 18 <input checked="" type="checkbox"/> 24		

Figure 45 Disabling lower data rates

Denying Inter User Traffic

Usually, there is no need for guests to share anything with other guests. Organizations which want to deny inter user communication between the guests can use the deny inter user traffic parameter of the VAP profile. If the deny inter user traffic parameter is enabled on a VAP, traffic between users connected to that VAP is denied.

19 **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

Advanced Services > All Profile Management

Profiles	Profile Details																																																
<ul style="list-style-type: none"> + AP + RF Management - Wireless LAN <ul style="list-style-type: none"> + 802.11K Profile + SSID Profile + High-throughput SSID profile - Virtual AP profile <ul style="list-style-type: none"> + Corp-App-LC1-Sunnyvale-6000 + Corp-App-LC2-Sunnyvale-6000 + Corp-Employee-LC1-Sunnyvale-6000 + Corp-Employee-LC2-Sunnyvale-6000 + Corp-Employee-TLS-LC1-Sunnyvale-6000 + default - guestnet + AAA Profile guestnet 802.11K Profile default 	<p>Virtual AP profile > guestnet Show Reference Save As Reset</p> <table border="1"> <tbody> <tr> <td>Virtual AP enable</td> <td><input checked="" type="checkbox"/></td> <td>Allowed band</td> <td>all</td> </tr> <tr> <td>VLAN</td> <td>900 <-- --NONE--</td> <td>Forward mode</td> <td>tunnel</td> </tr> <tr> <td>Deny time range</td> <td>--NONE--</td> <td>Mobile IP</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>HA Discovery on-association</td> <td><input type="checkbox"/></td> <td>DoS Prevention</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Station Blacklisting</td> <td><input checked="" type="checkbox"/></td> <td>Blacklist Time</td> <td>3600 sec</td> </tr> <tr> <td>Dynamic Multicast Optimization (DMO)</td> <td><input type="checkbox"/></td> <td>Dynamic Multicast Optimization (DMO) Threshold</td> <td>6</td> </tr> <tr> <td>Authentication Failure Blacklist Time</td> <td>3600 sec</td> <td>Multi Association</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Strict Compliance</td> <td><input type="checkbox"/></td> <td>VLAN Mobility</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Preserve Client VLAN</td> <td><input type="checkbox"/></td> <td>Remote-AP Operation</td> <td>standard</td> </tr> <tr> <td>Drop Broadcast and Multicast</td> <td><input type="checkbox"/></td> <td>Convert Broadcast ARP requests to unicast</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Disable conversion multicast RA packets to unicast</td> <td><input type="checkbox"/></td> <td>Deny inter user traffic</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Band Steering</td> <td><input checked="" type="checkbox"/></td> <td>Steering Mode</td> <td>prefer-5ghz</td> </tr> </tbody> </table>	Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all	VLAN	900 <-- --NONE--	Forward mode	tunnel	Deny time range	--NONE--	Mobile IP	<input checked="" type="checkbox"/>	HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>	Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 sec	Dynamic Multicast Optimization (DMO)	<input type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	6	Authentication Failure Blacklist Time	3600 sec	Multi Association	<input type="checkbox"/>	Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>	Preserve Client VLAN	<input type="checkbox"/>	Remote-AP Operation	standard	Drop Broadcast and Multicast	<input type="checkbox"/>	Convert Broadcast ARP requests to unicast	<input type="checkbox"/>	Disable conversion multicast RA packets to unicast	<input type="checkbox"/>	Deny inter user traffic	<input checked="" type="checkbox"/>	Band Steering	<input checked="" type="checkbox"/>	Steering Mode	prefer-5ghz
Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all																																														
VLAN	900 <-- --NONE--	Forward mode	tunnel																																														
Deny time range	--NONE--	Mobile IP	<input checked="" type="checkbox"/>																																														
HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>																																														
Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 sec																																														
Dynamic Multicast Optimization (DMO)	<input type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	6																																														
Authentication Failure Blacklist Time	3600 sec	Multi Association	<input type="checkbox"/>																																														
Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>																																														
Preserve Client VLAN	<input type="checkbox"/>	Remote-AP Operation	standard																																														
Drop Broadcast and Multicast	<input type="checkbox"/>	Convert Broadcast ARP requests to unicast	<input type="checkbox"/>																																														
Disable conversion multicast RA packets to unicast	<input type="checkbox"/>	Deny inter user traffic	<input checked="" type="checkbox"/>																																														
Band Steering	<input checked="" type="checkbox"/>	Steering Mode	prefer-5ghz																																														

Figure 46 Deny inter user traffic on guest VAP

Appendix A: Contacting Aruba Networks

Contacting Aruba Networks

Web Site Support	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Software Licensing Site	https://licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Validated Reference Design Contact and User Forum	
Validated Reference Designs	http://www.arubanetworks.com/vrd
VRD Contact Email	referencedesign@arubanetworks.com
AirHeads Online User Forum	http://community.arubanetworks.com

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
● United States	+1-800-WI-FI-LAN (800-943-4526)
● Universal Free Phone Service Numbers (UIFN):	
■ Australia	Reach: 1300 4 ARUBA (27822)
■ United States	1 800 9434526 1 650 3856589
■ Canada	1 800 9434526 1 650 3856589
■ United Kingdom	BT: 0 825 494 34526 MCL: 0 825 494 34526

Telephone Support

● Universal Free Phone Service Numbers (UIFN):

■ Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
■ Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
■ Singapore	Singapore Telecom: 1 822 494 34526
■ Taiwan (U)	CHT-I: 0 824 494 34526
■ Belgium	Belgacom: 0 827 494 34526
■ Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
■ Ireland	EIRCOM: 0 806 494 34526
■ Hong Kong	HKTI: 1 805 494 34526
■ Germany	Deutsche Telekom: 0 804 494 34526
■ France	France Telecom: 0 803 494 34526
■ China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
■ Saudi Arabia	800 8445708
■ UAE	800 04416077
■ Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
■ India	91 044 66768150