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 EXPRESS, 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.
# Table of Contents

Chapter 1:  Introduction

Reference Material

Chapter 2:  ArubaOS or Amigopod for Visitor Management

Chapter 3:  Guest Networks with Captive Portal Authentication

Captive Portal

Captive Portal Authentication Process

Guest Provisioning

Licenses Required

Certificates

Chapter 4:  Captive Portal Configuration

Guest VLAN and Related DHCP Services

Guest User Roles

Network Destination Alias

Defining Guest Access Policies

Configuring the guest-logon Role

Configuring the auth-guest Role

Configuring the SSID Profile for Guest WLAN

Configuring the Internal Database for Guest Authentication

Configuring the Captive Portal Authentication Profile

Configuring the AAA Profile for Guest WLAN

Chapter 5:  Guest Provisioning

Configuring Guest Provisioning User

Configuring the Guest-Provisioning Page

Modifying Guest Fields on the GPP

Modifying Page Design of the GPP

Email Options for the GPP

Creating Guest User Accounts

Chapter 6:  Optional Configurations for Guest Network

Time Range

Bandwidth Contracts

Maximum User Sessions for Guest Role

Walled Garden

Prioritizing Employee Traffic Using Traffic Management Profile
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 given 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>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArubaOS™ (mobility controllers)</td>
<td>6.1</td>
</tr>
<tr>
<td>ArubaOS (mobility access switch)</td>
<td>7.0</td>
</tr>
<tr>
<td>Aruba Instant™</td>
<td>1.1</td>
</tr>
<tr>
<td>MeshOS</td>
<td>4.2</td>
</tr>
<tr>
<td>AirWave®</td>
<td>7.3</td>
</tr>
<tr>
<td>AmigopodOS</td>
<td>3.3</td>
</tr>
</tbody>
</table>

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:

- 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>ArubaOS</th>
<th>ArubaOS Plus Amigopod</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captive Portal Customization</td>
<td>![Not supported] = ✗</td>
<td>![Limited support] = ☑</td>
</tr>
<tr>
<td>Captive portal customization</td>
<td>☑</td>
<td>✓</td>
</tr>
<tr>
<td>Captive portal per-SSID customization</td>
<td>☑</td>
<td>✓</td>
</tr>
<tr>
<td>Anonymous logon</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>One time tokens/access codes</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Welcome page with session statistics and logout</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Mobile browser aware captive portal pages</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Skins: UI branding customization</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Guest Account Provisioning</td>
<td>![Not supported] = ✗</td>
<td>![Limited support] = ☑</td>
</tr>
<tr>
<td>Single point of management for guest account and captive portal in multiple master controller deployments</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Non-IT staff do not require IP access to master controller for provisioning guest accounts</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Guest-provisioning operator role</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Feature</td>
<td>ArubaOS</td>
<td>ArubaOS Plus</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>Customizable guest-provisioning operator role</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>External servers for operator logins</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Provisioning of nonguest user roles by operators</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Limit operators to view only the account they created</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Self-registration workflow with automated login</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Sponsor-approved self-registration</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Time zone support for guest access in distributed deployments</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Bulk provisioning of guest accounts (CSV import and automatic generation)</td>
<td>❔️</td>
<td></td>
</tr>
<tr>
<td>Export/import of user database</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Mandatory and nonmandatory fields</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Guest password complexity requirements</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Guest account information printing via templates</td>
<td>❔️</td>
<td></td>
</tr>
<tr>
<td>Guest credential delivery through email and SMS</td>
<td>❔️</td>
<td></td>
</tr>
<tr>
<td>Force password change on first login</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Delete and/or disable guest accounts on expiration</td>
<td>❔️</td>
<td></td>
</tr>
</tbody>
</table>

**Guest Session Management**

<table>
<thead>
<tr>
<th>Feature</th>
<th>ArubaOS</th>
<th>ArubaOS Plus</th>
<th>Amigopod</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time and day policy</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Guest access expiry timer starts on first login</td>
<td>X</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Limit access based on total session time across multiple logins</td>
<td>X</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Limit guest session data (total bytes)</td>
<td>X</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Limit guest session bandwidth (Mb/s)</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Limit guest session to single concurrent login</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Hotspot and Hospitality Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>ArubaOS</th>
<th>ArubaOS Plus</th>
<th>Amigopod</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walled garden</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Plug-and-play clients, any IP</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>VPN NAT (static NAT per client using public IP)</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Credit card billing</td>
<td>X</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Surveys and feedback forms</td>
<td>X</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Target ads and promotions</td>
<td>X</td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>
Table 2  Comparison of ArubaOS Guest Access and Amigopod (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>ArubaOS</th>
<th>ArubaOS Plus Amigopod</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor data mining</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>MAC or cookie-based reauthentication (portal bypass)</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Reporting and Notification**

<table>
<thead>
<tr>
<th>Feature</th>
<th>ArubaOS</th>
<th>ArubaOS Plus Amigopod</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak guest network usage</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Total guest sessions (per day, per week, etc.)</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Bandwidth usage on guest network</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Top x users (session time and bandwidth)</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Expiring passwords</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Enterprise Features and Scalability**

<table>
<thead>
<tr>
<th>Feature</th>
<th>ArubaOS</th>
<th>ArubaOS Plus Amigopod</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing 1000s of accounts</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>High availability/redundancy</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Expandability (plug-in architecture)</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>900</td>
<td>192.168.200.1</td>
</tr>
</tbody>
</table>

**Guest VLAN Configuration**

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

**Figure 1  Creating a VLAN**
### Figure 2 Configuring IP parameters for the guest VLAN

![Configuring IP parameters for the guest VLAN](image)

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>IP Address</th>
<th>IPv4 Net Mask</th>
<th>IPv6 Address</th>
<th>Associated Ports</th>
<th>AAA Profile</th>
<th>Admin State</th>
<th>Operation State</th>
<th>Mode</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.16.0.254</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
<td>N/A</td>
<td>Disabled</td>
<td>Down</td>
<td>Regular</td>
<td>Enable</td>
</tr>
<tr>
<td>145</td>
<td>10.169.145.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>150</td>
<td>10.169.150.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>151</td>
<td>10.169.151.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>152</td>
<td>10.169.152.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>153</td>
<td>10.169.153.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Down</td>
<td>Regular</td>
<td>Enable</td>
</tr>
<tr>
<td>154</td>
<td>10.169.154.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>155</td>
<td>10.169.155.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>156</td>
<td>10.169.156.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>157</td>
<td>10.169.157.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>158</td>
<td>10.169.158.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>159</td>
<td>10.169.159.4</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
<tr>
<td>900</td>
<td>192.168.200.1</td>
<td>255.255.255.0</td>
<td>fe80::b:b8601</td>
<td>GEO/0-0-1, GEO/0-0-1, GEO/0-0-1, GEO/0-0-1</td>
<td>N/A</td>
<td>Enabled</td>
<td>Up</td>
<td>Regular</td>
<td>Disable</td>
</tr>
</tbody>
</table>

### Figure 3 Guest VLAN

![Guest VLAN](image)
Source-NAT Configuration for the Guest VLAN

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

Figure 4 Source-NATing the guest VLAN

Table 4 DHCP Services for the Guest VLAN

<table>
<thead>
<tr>
<th>Pool Name</th>
<th>Default Router</th>
<th>DNS Server</th>
<th>Network</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>guestpool</td>
<td>192.168.200.1</td>
<td>208.67.222.222 (Public DNS server)</td>
<td>192.168.200.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>208.67.222.220 (Public DNS server)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

```plaintext
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
!
```

![Figure 5](image)$\text{Configuring the DHCP pool}$
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 polices 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**

<table>
<thead>
<tr>
<th>Alias Name</th>
<th>Purpose</th>
<th>IP Address/ Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public-DNS</td>
<td>Defines the public DNS servers</td>
<td>Host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>208.67.222.222</td>
</tr>
<tr>
<td></td>
<td></td>
<td>208.67.222.220</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These are OpenDNS servers. For more details on OpenDNS see <a href="http://www.opendns.com">www.opendns.com</a></td>
</tr>
<tr>
<td>Internal-Network</td>
<td>Defines the private IPv4 address range</td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.0.0.0/8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>172.16.0.0/12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.0.0/16</td>
</tr>
</tbody>
</table>

**Network Destination Alias Configuration**

```bash
! 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
!
```
Figure 7: Aliases
Defining Guest Access Policies

Guest roles are made up of a number of polices 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

<table>
<thead>
<tr>
<th>Rule Number</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User</td>
<td>Any</td>
<td>UDP</td>
<td>Drop</td>
<td>This rule drops responses from a personal DHCP server. This action prevents the clients from acting as DHCP servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>min port = 68</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>max port = 68</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Service svc-dhcp (udp 67 68)</td>
<td>Permit</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>User</td>
<td>Alias Public-DNS</td>
<td>Service svc-dns (udp 53)</td>
<td>permit</td>
<td>This rule allows DNS queries only to the DNS servers that are defined in the Public-DNS alias.</td>
</tr>
</tbody>
</table>

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
!```
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

<table>
<thead>
<tr>
<th>Rule Number</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>user</td>
<td>Alias</td>
<td>any</td>
<td>drop</td>
<td>This rule denies access to all the addresses that are in the Internal-Network alias.</td>
</tr>
</tbody>
</table>

block-internal-access Policy Configuration

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

<table>
<thead>
<tr>
<th>Rule Number</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User</td>
<td>Any</td>
<td>svc-http</td>
<td>permit</td>
<td>This rule allows HTTP traffic from the users to any destination.</td>
</tr>
<tr>
<td>2</td>
<td>User</td>
<td>Any</td>
<td>svc-https</td>
<td>permit</td>
<td>This rule allows HTTPS traffic from the users to any destination.</td>
</tr>
</tbody>
</table>
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
!
```

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.

NOTE

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

<table>
<thead>
<tr>
<th>Rule Number</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Log</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>Yes</td>
<td>This rule denies access to all services on the network and logs the network access attempt.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Policy Number</th>
<th>Policy Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>captiveportal (predefined policy)</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>guest-logon-access</td>
<td>This policy allows DHCP and DNS services. For details, see Configuring the guest-logon-access Policy on page 20.</td>
</tr>
</tbody>
</table>
**guest-logon Role Configuration**

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

![Dashboard interface](image)

**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.

### auth-guest Role

<table>
<thead>
<tr>
<th>Policy Number</th>
<th>Policy Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cplogout (predefined policy)</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>guest-logon-access</td>
<td>This policy denies personal DHCP servers and provides legitimate DHCP services and DNS.</td>
</tr>
<tr>
<td>3</td>
<td>block-internal-access</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>auth-guest-access</td>
<td>This policy allows HTTP and HTTPS services to any destination.</td>
</tr>
<tr>
<td>5</td>
<td>drop-and-log</td>
<td>Any traffic that does not match the previous policies encounters this policy. This policy denies all services and logs the network access attempt.</td>
</tr>
</tbody>
</table>

auth-guest Role Configuration

```plaintext
!  
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  
!```
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

<table>
<thead>
<tr>
<th>SSID Profile</th>
<th>Network Name (SSID)</th>
<th>Authentication</th>
<th>Encryption</th>
<th>WMM</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>guestnet</td>
<td>Guest</td>
<td>Open</td>
<td>none</td>
<td></td>
<td>Guest users. (Captive portal is used to provide Layer 3 authentication.)</td>
</tr>
</tbody>
</table>

**Guest SSID Profile Configuration**

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

**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

<table>
<thead>
<tr>
<th>Server Group</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest-internal</td>
<td>Internal (predefined)</td>
</tr>
</tbody>
</table>

Server Group Configuration

```plaintext
!  aaa server-group "Guest-internal"
    auth-server Internal
!```
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>
<thead>
<tr>
<th>Table 14</th>
<th>Captive portal profile</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Purpose</th>
<th>Sample Configuration (guestnet captive portal profile)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User login</td>
<td>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.</td>
<td>enabled</td>
</tr>
<tr>
<td>Default role</td>
<td>This role is assigned to users after successful authentication through user login.</td>
<td>auth-guest</td>
</tr>
<tr>
<td>Guest login</td>
<td>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.</td>
<td>disabled</td>
</tr>
<tr>
<td>Default Guest role</td>
<td>This role is assigned to users after successful authentication through guest login.</td>
<td>_</td>
</tr>
<tr>
<td>Logout popup window</td>
<td>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.</td>
<td>enabled</td>
</tr>
<tr>
<td>Login page</td>
<td>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.</td>
<td>/auth/index.html</td>
</tr>
<tr>
<td>Welcome page</td>
<td>This is the welcome page that is displayed after successful authentication.</td>
<td>/auth/welcome.html</td>
</tr>
<tr>
<td>Show Welcome Page</td>
<td>This enables the welcome page. If disabled, the authenticated user is redirected automatically to the page he was trying to browse initially.</td>
<td>enabled</td>
</tr>
<tr>
<td>Allow only one active user session</td>
<td>If enabled, only one active session is allowed per username/password.</td>
<td>enabled</td>
</tr>
<tr>
<td>White List</td>
<td>Lists the aliases to which the unauthenticated users are allowed access. For details, see Walled Garden on page 56.</td>
<td>--</td>
</tr>
</tbody>
</table>
Remember to add a server group, which defines internal database as the authentication server, to the captive portal profile.

### Table 14  Captive portal profile (Continued)

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

### Captive Portal Configuration

```bash
!  
  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  
  !
```
Figure 16  Captive portal profile (using the sample configuration in Table 14)
**Figure 17**  Captive portal page when user and guest login are enabled

**Figure 18**  Captive portal page for user 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
!
```
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

<table>
<thead>
<tr>
<th>AAA Profile Name</th>
<th>Initial Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>guestnet</td>
<td>guest-logon</td>
</tr>
</tbody>
</table>

Guest AAA Profile Configuration

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

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" ******
!
```

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.

*Figure 23  Editing guest-provisioning fields*
**Figure 24**  Guest-provisioning fields displayed on the GPP

**Figure 25**  Display In Listing fields shown on the GPP
**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.

![Management > Guest Provisioning](image)

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
```

![Figure 28](image)  
**Figure 28**  
**SMTP configuration for sending guest-provisioning emails**
Modifying Email Options

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.

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

**Figure 31**  Creating guest accounts using guest provisioning (step 2)
**Figure 32**  Manually sending emails for guests and sponsors from GPP

**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.

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 to 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>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Start Date</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working-hours</td>
<td>periodic</td>
<td>weekday</td>
<td>07:00</td>
<td>17:30</td>
</tr>
</tbody>
</table>

Time Range Configuration

```
! time-range "Working-hours" periodic Weekday 07:00 to 17:30
```
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 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
!```
Figure 36  guest-logon-access policy with time range

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Start Date</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny-access</td>
<td>periodic</td>
<td>weekday</td>
<td>17:30</td>
<td>23:59</td>
</tr>
<tr>
<td>deny-access</td>
<td>periodic</td>
<td>weekday</td>
<td>00:00</td>
<td>07:30</td>
</tr>
<tr>
<td>deny-access</td>
<td>periodic</td>
<td>weekend</td>
<td>00:00</td>
<td>23:59</td>
</tr>
</tbody>
</table>

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
```

Figure 38      Deny access time range
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.
Table 18 lists the parameters used in the configuration of separate per role bandwidth contracts for upstream and downstream traffic.

**Table 18   Bandwidth Contracts**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Rate</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest-upstream</td>
<td>per role</td>
<td>1 Mb/s</td>
<td>used as upstream bandwidth contract for authenticated guest role (auth-guest)</td>
</tr>
<tr>
<td>guest-downstream</td>
<td>per role</td>
<td>3 Mb/s</td>
<td>used as downstream bandwidth contract for authenticated guest role (auth-guest)</td>
</tr>
</tbody>
</table>

**Bandwidth Contracts Configuration for Authenticated Guest Role**

```plaintext
!
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
!
```
**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
!
```
**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.

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

Table 19       walled-garden-access Alias

<table>
<thead>
<tr>
<th>Alias Name</th>
<th>IP Address/ Range</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>walled-garden-access</td>
<td><a href="http://www.arubanetworks.com">www.arubanetworks.com</a></td>
<td>Define the websites to which unauthenticated guests are allowed access.</td>
</tr>
</tbody>
</table>

Walled Garden Configuration

```
! netdestination walled-garden-access
  name www.arubanetworks.com
! aaa authentication captive-portal "default"
  white-list walled-garden-access
!
```
**Figure 43**  
**walled-garden-access alias**

**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.
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.

![Figure 46](image-url) Deny inter user traffic on guest VAP
# Appendix A: Contacting Aruba Networks

## Contacting Aruba Networks

<table>
<thead>
<tr>
<th>Web Site Support</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Site</strong></td>
<td><a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a></td>
</tr>
<tr>
<td><strong>Support Site</strong></td>
<td><a href="https://support.arubanetworks.com">https://support.arubanetworks.com</a></td>
</tr>
<tr>
<td><strong>Software Licensing Site</strong></td>
<td><a href="https://licensing.arubanetworks.com/login.php">https://licensing.arubanetworks.com/login.php</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Support Emails</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Americas and APAC</strong></td>
<td><a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a></td>
</tr>
<tr>
<td><strong>EMEA</strong></td>
<td><a href="mailto:emea_support@arubanetworks.com">emea_support@arubanetworks.com</a></td>
</tr>
<tr>
<td><strong>WSIRT Email</strong></td>
<td><a href="mailto:wsirt@arubanetworks.com">wsirt@arubanetworks.com</a></td>
</tr>
</tbody>
</table>

**Validated Reference Design Contact and User Forum**

<table>
<thead>
<tr>
<th>Validated Reference Designs</th>
<th><a href="http://www.arubanetworks.com/vrd">http://www.arubanetworks.com/vrd</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VRD Contact Email</strong></td>
<td><a href="mailto:referencedesign@arubanetworks.com">referencedesign@arubanetworks.com</a></td>
</tr>
<tr>
<td><strong>AirHeads Online User Forum</strong></td>
<td><a href="http://community.arubanetworks.com">http://community.arubanetworks.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Telephone Support</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aruba Corporate</strong></td>
<td>+1 (408) 227-4500</td>
</tr>
<tr>
<td><strong>FAX</strong></td>
<td>+1 (408) 227-4550</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>United States</strong></td>
<td>+1-800-WI-FI-LAN (800-943-4526)</td>
</tr>
<tr>
<td><strong>Universal Free Phone Service Numbers (UIFN):</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Australia</strong></td>
<td>Reach: 1300 4 ARUBA (27822)</td>
</tr>
<tr>
<td><strong>United States</strong></td>
<td>1 800 9434526</td>
</tr>
<tr>
<td></td>
<td>1 650 3856589</td>
</tr>
<tr>
<td><strong>Canada</strong></td>
<td>1 800 9434526</td>
</tr>
<tr>
<td></td>
<td>1 650 3856589</td>
</tr>
<tr>
<td><strong>United Kingdom</strong></td>
<td>BT: 0 825 494 34526</td>
</tr>
<tr>
<td></td>
<td>MCL: 0 825 494 34526</td>
</tr>
</tbody>
</table>
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 Telkom: 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