Copyright Information

© Copyright 2018 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA
Contents

About This Document ......................................................... 10
  Intended Audience .......................................................... 10
  Related Documents .......................................................... 10
  Conventions ................................................................. 10
  Contacting Support .......................................................... 11

SD Branch Solution ............................................................ 12
  Why SD-WAN? ............................................................... 12
  How It Works ............................................................... 13
  What are the Solution Requirements? ................................. 15
  How Do I Get Started? ...................................................... 15

Getting Started ................................................................. 16
  Onboarding Devices to Central ........................................... 16
    Manually Adding Devices to Inventory ............................... 17
  Assigning Subscriptions to SD-WAN Gateways ..................... 17
  Assigning Groups .......................................................... 18
    Important Points to Note ............................................... 18
    Assigning SD-WAN Gateways to Groups ............................ 18
  Assigning SD-WAN Gateways to Sites ............................... 19
  Assigning Labels ........................................................... 19
  Assigning a Group Role or Persona ................................... 19
  Connecting SD-WAN Gateways to Central ............................ 20
  Allowing Device Communication over Network Firewall .......... 20
  Uploading Certificates .................................................... 22
    Uploading Certificates .................................................. 22
Managing Certificates on Instant APs Configured Using Templates ........................................ 23

SD Branch Redundancy ........................................................................................................... 24
  Data Center Redundancy .................................................................................................... 24
  VRRP Redundancy ............................................................................................................. 24
  Configuring SD-WAN Gateway Redundancy .................................................................... 24

Building an SD-WAN Network .............................................................................................. 28
  SD-WAN Configuration Checklist .................................................................................... 29
  Configuring Address Pools for SD-WAN Gateways ......................................................... 29
    Configuring Gateway Pools for SD-WAN Gateways ...................................................... 29
    Configuring DHCP Address Pools .................................................................................. 30
    Configuring NAT Pools ................................................................................................. 32
    Configuring Tunnel Pools for SD-WAN Gateways ....................................................... 33
  Uploading Bulk Configuration Template .......................................................................... 33
  Configuring System Information for SD-WAN Gateways ............................................... 34
    Configuring Hostname for SD-WAN Gateways ............................................................ 34
    Configuring System IP Address for SD-WAN Gateways ............................................ 34
    Setting System Clock and Time Zone on SD-WAN Gateways .................................... 35
    Configuring Domain Name System .............................................................................. 36
    Configuring Redirect DNS Servers .............................................................................. 36
    Configuring Dynamic Domain Name System ............................................................... 37
    Setting Capacity Threshold ........................................................................................... 38
    Configuring Device Administrator Credentials for SD-WAN Gateways .................. 38
    Configuring Switching Parameters .............................................................................. 41
  Configuring AMON Receivers for SD-WAN Gateways .................................................. 42
  Configuring VLANs ........................................................................................................... 43
    Adding VLANs for SD-WAN Gateways ...................................................................... 43
    Configuring VLANs for WAN Interfaces .................................................................... 43
    Configuring VLANs for LAN Interfaces ...................................................................... 44
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Other Parameters for VLAN</td>
<td>44</td>
</tr>
<tr>
<td>Configuring Ports</td>
<td>46</td>
</tr>
<tr>
<td>Adding Ports</td>
<td>47</td>
</tr>
<tr>
<td>Configuring Ports for WAN Interfaces</td>
<td>47</td>
</tr>
<tr>
<td>Configuring Ports for LAN Interfaces</td>
<td>48</td>
</tr>
<tr>
<td>Configuring Other Parameters for Port</td>
<td>48</td>
</tr>
<tr>
<td>Configuring Uplinks</td>
<td>50</td>
</tr>
<tr>
<td>Uplink Load Balancing</td>
<td>50</td>
</tr>
<tr>
<td>WAN Bandwidth Optimization</td>
<td>51</td>
</tr>
<tr>
<td>Bandwidth Estimation</td>
<td>51</td>
</tr>
<tr>
<td>Configuring Uplink Interfaces</td>
<td>51</td>
</tr>
<tr>
<td>Enabling WAN Health Check Probes</td>
<td>52</td>
</tr>
<tr>
<td>Configuring WAN Interface Bandwidth Priorities</td>
<td>53</td>
</tr>
<tr>
<td>Enabling WLAN Interface Bandwidth Priorities</td>
<td>53</td>
</tr>
<tr>
<td>Configuring Hub and Spoke VPN</td>
<td>54</td>
</tr>
<tr>
<td>Whitelisting Branch Gateways on VPN Concentrator</td>
<td>55</td>
</tr>
<tr>
<td>Configuring VPN Tunnels on Branch Gateways</td>
<td>56</td>
</tr>
<tr>
<td>Configuring IKE Policies</td>
<td>57</td>
</tr>
<tr>
<td>Configuring IKEv1 Policies and Dynamic Maps</td>
<td>57</td>
</tr>
<tr>
<td>Configuring IKEv2 Policies and Dynamic Maps</td>
<td>59</td>
</tr>
<tr>
<td>Configuring Site-to-Site VPN</td>
<td>61</td>
</tr>
<tr>
<td>Configuring IPsec Map for Site-to-Site VPNs</td>
<td>62</td>
</tr>
<tr>
<td>Enabling Dead Peer Detection</td>
<td>65</td>
</tr>
<tr>
<td>Configuring Dead Peer Detection Parameters</td>
<td>65</td>
</tr>
<tr>
<td>Configuring Site-to-Site VPN with GRE Tunnel</td>
<td>65</td>
</tr>
<tr>
<td>Configuring GRE Tunnels</td>
<td>66</td>
</tr>
<tr>
<td>Directing Traffic into the GRE Tunnel</td>
<td>70</td>
</tr>
<tr>
<td>Configuring Static Routes</td>
<td>70</td>
</tr>
<tr>
<td>Configuring a Firewall Policy Rule</td>
<td>70</td>
</tr>
</tbody>
</table>
Configuring Routes ............................................................................................................. 70
  Underlay Routes .................................................................................................................. 70
  Overlay Routes .................................................................................................................... 71
Configuring Static IP Routes ............................................................................................... 71
  Creating a Static IP Route .................................................................................................... 71
Configuring Default Gateways for Routing ........................................................................ 71
Configuring OSPF ................................................................................................................ 72
  Prerequisites ....................................................................................................................... 72
  Enabling and Configuring OSPF Parameters ....................................................................... 72
Configuring Policies for PBR ............................................................................................... 73
  PBR Policies for WAN Networks ......................................................................................... 73
Configuring Policies for Dynamic Path Steering ................................................................. 75
  How Dynamic Path Selection Works ................................................................................ 76
  Configuring a Dynamic Path Steering Policy ...................................................................... 76
Enforcing a Common Security Policy for Wired and Wireless Users ............................... 78
Configuring Policies for Website Content Classification ................................................... 79
  Enabling WebCC Visibility ............................................................................................... 79
  Configuring WebCC Services ............................................................................................ 79
Configuring Firewall Policies and ACLs ............................................................................. 81
  Firewall Policies for SD Branch ......................................................................................... 82
    Types of ACLs .................................................................................................................. 82
  Configuring Aliases for Firewall Policies .......................................................................... 82
  Creating a Firewall Policy for Network Services ............................................................... 83
    Configuring Access Rules ............................................................................................... 84
  Configuring ACLs for Deep Packet Inspection ................................................................ 85
    Creating ACLs for Application Usage ........................................................................... 85
  Configuring ACLs for Web Content Classification ............................................................ 86
  Configuring Global Firewall Parameters .......................................................................... 87
  Configuring User Roles ..................................................................................................... 91
Creating a Role .................................................................................................................. 92
Assigning a Policy to a Role .............................................................................................. 92
Assigning User Roles in AAA Profiles .................................................................................. 92
Configuring a Default Role Based on Authentication Methods ........................................... 93
Configuring Bandwidth Contracts ....................................................................................... 93
Configuring Authentication Profiles ..................................................................................... 94
Configuring RADIUS Authentication Server ...................................................................... 94
  Configuring an RFC 3576 Server ...................................................................................... 96
Configuring Other External Authentication Servers ........................................................... 96
  Configuring an LDAP Server ............................................................................................ 96
  Configuring a TACACS+ Server ....................................................................................... 97
  Configuring a Windows Server ......................................................................................... 98
  Configuring XML Server .................................................................................................. 99
Configuring Server Groups .................................................................................................. 99
Creating a AAA Profile ......................................................................................................... 99
Applying Policies on SD-WAN Gateway Interfaces ............................................................. 101
  Applying Policies for VLANs on Access Ports ................................................................. 101
  Applying Policies for VLANs on Trunk Ports .................................................................... 101
  Applying Route ACLs for VLAN Interfaces ..................................................................... 102
  Assigning AAA profile to VLAN Interfaces for Role Assignment ..................................... 102
Configuring SD-WAN Gateways for Certificate-Based Authentication ............................. 102
  Adding Certificates to Certificate Store in Central ............................................................ 102
  Installing Certificates .................................................................................................... 103
  Configuring Revocation Checkpoint .............................................................................. 103
Integrating Zscaler Security Service ................................................................................. 105
  Integrating with ZIA ..................................................................................................... 105
  Configuring the Branch Gateway for Zscaler Integration ............................................... 105
Integrating GlobalProtect Cloud Service ........................................................................... 106
Deploying Palo Alto Networks - GlobalProtect Cloud Service Dashboard ........................... 107
## Contents

- Configuring GlobalProtect Cloud Service for Aruba SD-WAN .................................................. 107
- Configure IPsec Maps for GlobalProtect Cloud Service ............................................................. 107

**Viewing Configuration Status** ........................................................................................................ 108

- Configuration Synchronization Errors ............................................................................................. 108
- Local Overrides .................................................................................................................................. 109
- Viewing Configuration Status for a UI Group .................................................................................... 109
- Viewing Configuration Status for Devices .......................................................................................... 109
- Configuring SD-WAN Gateways for SNMP-Based Reporting ............................................................ 110
  - Community String for SNMPv1 and SNMPv2 ................................................................................ 110
  - SNMP Trap Receivers ...................................................................................................................... 110

**Configuring a Micro Branch with Instant APs** .............................................................................. 111

- Configuring Instant APs for Micro Branch Solution ......................................................................... 111
- Configuring VPN Concentrators for Micro Branch Solution ............................................................ 111
- Configuring Instant AP VPN Pool for SD-WAN Gateways ............................................................... 111
- Configuring Authentication Server .................................................................................................... 112
- Redistributing Branch Subnets ........................................................................................................ 113

**Aruba VIA Solution** ...................................................................................................................... 114

- Configuring VIA .............................................................................................................................. 114

**Monitoring SD Branch** .................................................................................................................. 123

- Gateway Details ............................................................................................................................... 123
- Gateway Details ............................................................................................................................... 124
- Analyzing Application Usage ......................................................................................................... 131

**Network Health** ............................................................................................................................. 132

- Data Source ...................................................................................................................................... 133
- Page Views ....................................................................................................................................... 133
- Site Health ........................................................................................................................................ 134

**Topology** ........................................................................................................................................ 135

- Before You Begin .............................................................................................................................. 135
This user guide describes the Aruba Software-Defined WAN (SD-WAN) Solution and provides detailed instructions for setting up, configuring, and managing SD-WAN Gateways from Aruba Central.

**Intended Audience**
This guide is intended for network administrators who manage and monitor branch networks.

**Related Documents**
In addition to this document, see the following documents for more details on the SD Branch devices and Aruba Central:
- *Aruba Central Help Center*
- *ArubaOS User Guide*
- *HPE-ArubaOS Switch Management and Configuration Guide*
- *Aruba ClearPass Policy Manager User Guide*

**Conventions**
Table 1 lists the typographical conventions used throughout this guide to emphasize important concepts:

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italics</em></td>
<td>This style is used to emphasize important terms and to mark the titles of books.</td>
</tr>
</tbody>
</table>
| **System items** | This fixed-width font depicts the following:  
  - Sample screen output  
  - System prompts |
| **Bold**   |  
  - Keys that are pressed  
  - Text typed into a GUI element  
  - GUI elements that are clicked or selected |

The following informational icons are used throughout this guide:

**NOTE**
Indicates helpful suggestions, pertinent information, and important things to remember.

**CAUTION**
Indicates a risk of damage to your hardware or loss of data.

**WARNING**
Indicates a risk of personal injury or death.
# Contacting Support

**Table 2: Contact Information**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Site</strong></td>
<td><strong><a href="http://arubanetworks.com">arubanetworks.com</a></strong></td>
</tr>
<tr>
<td><strong>Support Site</strong></td>
<td><strong><a href="http://support.arubanetworks.com">support.arubanetworks.com</a></strong></td>
</tr>
<tr>
<td><strong>Airheads Social Forums and Knowledge Base</strong></td>
<td><strong><a href="http://community.arubanetworks.com">community.arubanetworks.com</a></strong></td>
</tr>
<tr>
<td><strong>North American Telephone</strong></td>
<td>1-800-943-4526 (Toll Free) 1-408-754-1200</td>
</tr>
<tr>
<td><strong>International Telephone</strong></td>
<td><strong><a href="http://arubanetworks.com/support-services/contact-support/">arubanetworks.com/support-services/contact-support/</a></strong></td>
</tr>
<tr>
<td><strong>Software Licensing Site</strong></td>
<td><strong><a href="http://hpe.com/networking/support">hpe.com/networking/support</a></strong></td>
</tr>
<tr>
<td><strong>End-of-life Information</strong></td>
<td><strong><a href="http://arubanetworks.com/support-services/end-of-life/">arubanetworks.com/support-services/end-of-life/</a></strong></td>
</tr>
<tr>
<td><strong>Security Incident Response Team</strong></td>
<td><strong>Site: <a href="http://arubanetworks.com/support-services/security-bulletins/">arubanetworks.com/support-services/security-bulletins/</a> Email: <a href="mailto:sirt@arubanetworks.com">sirt@arubanetworks.com</a></strong></td>
</tr>
</tbody>
</table>
The Aruba SD Branch solution offers the best-in-class wireless and wired infrastructure and management orchestration features with the SD-WAN capabilities. The SD Branch solution extends the SD-WAN concept to all elements in the branch to deliver a full stack solution that addresses the business challenges of distributed enterprises. Coupled with Central, the solution provides a cloud-hosted environment with simplified operations and improved agility.

Why SD-WAN?

A traditional branch setup supports client connectivity requirements across different geographical locations for various types of business operations. The sites in remote geographical locations serve as branch offices, while the headquarters or main office serves as a data center that hosts network resources to store, manage, and distribute data. The main office also hosts a centralized Virtual Private Network (VPN) management system to aggregate traffic from the remote branch sites. A Wide Area Network (WAN) — with Multiprotocol Label Switching (MPLS), T1, T3, Broadband, or Cellular links—is used for connecting multiple local area networks to a central corporate network or data centers separated by distance.

Due to an increase in the number of client devices at the remote sites and the new bandwidth requirements, branch office networks are expected rapidly scale to provide uninterrupted user experience. A traditional branch infrastructure with multiple appliances, different operating systems, and management tools only adds to the cost, involves a maintenance overhead, and demands skilled IT personnel.

The Aruba SD-WAN solution simplifies your branch deployments with a single management interface for administering, managing, and monitoring your branch networks. It also provides a unified policy enforcement framework with operational ease.

Key Features and Benefits

The SD-WAN solution comes with the following key capabilities:

- Zero Touch Provisioning of devices—Ability to self-provision without operator’s intervention.
- Centralized overlay management and control—A single cloud-based network management interface for managing and monitoring SD Branch devices. Aruba Central, the cloud-based network management system, supports unified management of SD branch devices with ZTP and hierarchical configuration.
- IPsec based Automatic VPN Tunnels—Support for high-performance and automatic IPsec VPN for secure overlay networking.
- Unified security policy for wired, wireless, and WAN—Support for a common security policy framework based on user roles for WAN, WLAN, and LAN users.
- Dynamic path selection—Support for dynamically steering traffic or a service request to the best available path. For example, you can configure a policy to dynamically route the real-time voice and video traffic on the link with the lowest latency and jitter, and the bulk file traffic on the link with the maximum bandwidth.
- Deep Packet Inspection and Web Content Classification—Support for monitoring and analyzing application usage by clients.
- Visibility, analytics, and troubleshooting—Dashboards for monitoring branch health, device performance, and client connectivity metrics. Alerts, reports, and audit trails for monitoring and troubleshooting network performance issues.
Policy-based Routing—In addition to the traditional destination-based routing, the SD Branch devices support routing client traffic based on user role or type of application. For example, traffic generated from the guest devices can be routed directly to the internet, while traffic from the employees can be routed to the MPLS network.

How It Works

The SD-WAN solution includes a new set of devices called SD-WAN Gateways that inter-operate Aruba Switches and Instant APs to provide a full-fledged WAN architecture.

Based on the size of your branch setup, you can choose device combination that best suits your requirement:

- **Medium to large branches**—For branches that require more than 24 ports, you can use a combination of Branch Gateways and one or more Aruba switches at the branch site, with Aruba 7200 Series Mobility Controller as VPN Concentrator at the data center.

- **Small to medium branches**—For branches that require less than 24 ports (including all WAN and LAN ports), you can deploy Branch Gateways at the branch sites, with Aruba 7200 Series Mobility Controller as VPN Concentrator at the data center.

- **Micro branches**—For micro branches, you can deploy an Instant AP cluster at the branch site, with Aruba 7200 Series Mobility Controller as the VPN Concentrator at the data center.

*Figure 1* shows a typical deployment topology of an SD Branch with Branch Gateways and a micro branch with Instant APs:

*Figure 1  SD Branch Topology*
Figure 2 illustrates the communication flow between Aruba Central, branch sites, and data center.

**Figure 2** *Aruba Central and Cloud Communication*

![Aruba Central and Cloud Communication Diagram](image)

Figure 3 shows all elements in an SD Branch and the SD-WAN data flow.

**Figure 3** *Aruba SD-WAN Data Flow*

![Aruba SD-WAN Data Flow Diagram](image)
What are the Solution Requirements?

The following sections list the supported hardware platforms and minimum software versions required for setting up an SD Branch.

At the Branch Site

Table 3 shows the list of hardware and software requirements for a branch site:

**Table 3: SD Branch Site Devices**

<table>
<thead>
<tr>
<th>SD Branch Component</th>
<th>Hardware Platforms</th>
<th>Minimum Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch Gateways</td>
<td>Aruba 7000 Series Mobility Controller</td>
<td>ArubaOS_70xx_8.1.0.0-1.0.0.0</td>
</tr>
<tr>
<td>Aruba Switches function with Branch Gateways to detect and isolate rogue APs, and blacklist rogue devices.</td>
<td>Aruba 3810 Switch Series</td>
<td>KB.16.05.0007 or later</td>
</tr>
<tr>
<td></td>
<td>Aruba 5400R Switch Series</td>
<td>KB.16.05.0007 or later</td>
</tr>
<tr>
<td></td>
<td>Aruba 2920 Switch Series</td>
<td>WB.16.05.0007 or later</td>
</tr>
<tr>
<td></td>
<td>Aruba 2930F Switch Series</td>
<td>WC.16.05.0007 or later</td>
</tr>
<tr>
<td>Instant APs function as VPN clients at branch sites. The client data traffic from these APs are aggregated by the VPN Concentrator located at the data center</td>
<td>Aruba 310 Series and 300 Series Instant APs</td>
<td>Aruba Instant 6.5.3.x Aruba Instant 8.3.0.0 or later</td>
</tr>
</tbody>
</table>

At the Data Center

At the data center, you can deploy Aruba 7200 Series Mobility Controller as VPN Concentrator. For data center redundancy, you can deploy two VPN concentrators in the active-standby or active-active mode.

**Table 4: Data Center**

<table>
<thead>
<tr>
<th>SD Branch Component</th>
<th>Hardware Platform</th>
<th>Minimum Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>A VPN Concentrator functions as a VPN management system that aggregates data traffic from the branches and terminates IPsec VPN tunnels.</td>
<td>Aruba 7200 Series Mobility Controllers</td>
<td>ArubaOS_72xx_8.1.0.0-1.0.0.0</td>
</tr>
</tbody>
</table>

In the Cloud

A valid Central subscription is required to avail cloud-based administration, management, configuration and monitoring of SD branch components such as Branch Gateways, VPN Concentrators, Instant APs, and Aruba Switches.

How Do I Get Started?

To start using the SD-WAN solution, complete the steps described in the [Getting Started](#) section.
To start using the SD-WAN solution, ensure that you have a valid Aruba Central subscription and licenses for the SD branch devices.

- If you are an existing Aruba Central customer with a valid subscription and device licenses, access the Central UI and complete the provisioning tasks.
- If you are an existing Aruba customer with valid device licenses, but are not an Aruba Central customer, sign up for Aruba Central. After a successful registration, Aruba sends a verification email with a link to Central portal. For more information, see Aruba Central Help Center.

Central offers a 90-day evaluation subscription for customers who want to try the Aruba cloud solution for managing their networks. When you sign up for Central, an evaluation subscription is automatically assigned, unless you purchased a subscription. To purchase subscriptions, contact the Aruba support team.

Gateway Provisioning Tasks
Complete the following provisioning tasks to bring up your devices in the Central management interface:

- Onboard Devices
- Assign Subscriptions
- Assign Devices to Sites
- Assign Labels
- Assign Groups
- Assigning a Group Role or Persona
- Provision Gateways
- Open Firewall Ports for Device Communication

Onboarding Devices to Central
If you are a registered Central portal user, Central automatically retrieves the devices associated with your account and adds it to the device inventory. To verify if the devices are added to Central's device inventory, go to Global Settings > Device Inventory in the Central UI.

The users with the evaluation subscription may have to add the devices manually using their Aruba Activate credentials.

- If the devices are listed in the inventory, proceed to assign devices to groups, labels, and sites.
- If the devices do not show up in the inventory, click Sync Now to synchronize the inventory with the Activate database.
- If the devices do not show up in the inventory even after the sync operation, manually add these devices.
Manually Adding Devices to Inventory

To manually add the devices, on the **Device Inventory** page, click one of the device addition options described in the following table:

**Table 5: Adding Devices**

<table>
<thead>
<tr>
<th>Device Addition Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add by MAC/SN</td>
<td>Allows you to add devices based on MAC address and serial numbers. You can add up to 32 devices.</td>
</tr>
</tbody>
</table>
| Add with Cloud Activation Key   | Allows you add multiple devices from a single purchase order by using the cloud activation key. To add devices:  
1. Enter the **Cloud Activation Key** and MAC address of the device. 
2. Click **Add**. Central retrieves all devices that belong to the same purchase order and displays the list. |
| Add Using Activate              | Allows you to retrieve the devices associated with an Activate user account. To add devices:  
1. Enter the username and password of the Activate user account.  
2. Click **Add**. The devices associated with the Activate account are retrieved and added to the list of devices displayed on the **Device Inventory** page.  
**NOTE:** You can use this option only once. After the devices are added, Central does not allow you to modify or re-import the devices using your Aruba Activate credentials. |

Assigning Subscriptions to SD-WAN Gateways

After adding gateways to the Central device inventory, you must ensure that the gateway devices are assigned a valid subscription. The gateway subscription allows Aruba Mobility Controllers to function as SD branch devices.

Central supports the following types of subscriptions for gateways:

- **Foundation**—This subscription can be assigned to all Mobility Controllers irrespective of the hardware model.
- **Foundation-Base capacity**—This subscription can be assigned only to Aruba 7005 Mobility Controllers. Gateway devices with the Foundation-Base capacity subscription can support up to 75 client devices per branch.

To assign gateway subscription to a device, complete the following steps:

1. Go to **Global Settings** > Click **Subscription Assignment**. The **Subscription Assignment** page opens.
2. Under **Gateway Subscriptions**, select the device to which you want to assign a subscription.
3. Expand the drop-down in Assignment column for the selected device.
4. Select the subscription; for example, **Foundation**.
5. To assign subscription to multiple devices:
   a. Select the devices in the table.
   b. Click **Batch Assignment**.
   c. Select the subscription that you to assign.

When a gateway subscription assigned to a device expires, Central automatically assigns a valid subscription from the same subscription category.
Assigning Groups

A group in Central is a primary configuration element that acts like a container. In other words, groups are a subset of one or several devices that share common configuration settings. Central supports assigning devices to groups for the ease of configuration and maintenance. For example, you can create a common group for Branch Gateways that have similar configuration requirements.

The device groups in Central allow you to:

- Combine Branch Gateways of identical characteristics and configuration requirements under a single group.
- Create groups according to your branch requirements.
  - You can create separate groups for the small, medium, and large sized branches.
  - You can also create separate groups for the branch sites in different geographical locations; for example, East Coast and West Coast branch sites. If these groups have similar characteristics with minor differences, you can create the first group and then clone it.
  - You can use either a single group for all the devices or deploy devices in multiple groups. For example, you can deploy 7008 controllers and Aruba 2930F Switch Series with 24 ports in a single group for every branch.
  - You can also deploy 7005 controller and Aruba 2930F Switch Series with 24 ports in one group and provision 7008 controller with Aruba 2930F Switch Series with 48 ports in another group.
- Provision Branch Gateways and VPN Concentrators in separate groups. Because the configuration requirements for Branch Gateways and VPN Concentrators are different, the Branch Gateways and VPN Concentrators must be assigned to different groups.
- Combine different types of devices under a group. For example, a group can have Instant APs, switches, and SD-WAN Gateways. Central allows you to manage configuration of these devices in separate containers (Wired Management for Switches, Wireless Management for Instant APs, and Gateway Management for SD-WAN Gateways within the same group).

Important Points to Note

Note the following points about groups in Central:

- The groups in Central are not device-specific, so you can provision Branch Gateways, Switches, and Instant AP in a single group. However, VPN Concentrators and Branch Gateways must be assigned to different groups.
- A device can be part of only one group at any given time.
- After assigning the SD-WAN Gateways to groups, you must set the group persona or role as Branch Gateway or VPN Concentrator.

Assigning SD-WAN Gateways to Groups

To assign devices to groups:

2. If the group is already available in the list of groups, select the device, and drag and drop the device to the group.
3. If the group is not available in the list, click New Group and create a new group. Drag and drop the device to the group you just created.
Assigning SD-WAN Gateways to Sites

A site in Central refers to a physical location where a set of devices are installed; for example, campus, branch, or a venue. You can create a branch site, for example BranchA, for a specific geographical location and assign SD Branch devices to it. You can use these sites as filters when monitoring network and branch health or generating reports.

To manage your SD Branch devices, you can create a site for data center (for example, MainSite) and separate sets of sites for branch offices.

To assign SD-WAN Gateways to a site:

1. On the **Global Settings > Labels and Sites > Sites** page, locate the site to which you want to assign a device. You can also add a new site by clicking **New Site** and providing details, such as site name and address.
2. To view devices that are not assigned to any site, click **Unassigned**.
3. Select one or several devices from the list of devices.
4. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
5. To confirm the assignment, click **Yes**.

Assigning Labels

In Central, labels refer to the tags attached to a device provisioned in the network. You can use labels for tagging devices to a specific area in a physical location, to an owner or a specific branch, or a business unit. You can use these labels as filters for monitoring branch and device health, and generating reports.

To assign a label to a device, complete the following steps:

1. On the **Global Settings > Labels and Sites > Labels** page, locate the label to which you want to assign a device. You can also create a new label by clicking **Add Label** and providing a label name.
2. In the table that lists the labels, you can perform one of the following actions:
   - Click **All Devices** to view all devices.
   - Click **Unassigned** to view all the devices that are not assigned to any labels.
3. Select **Unassigned**. A list of devices that are not assigned to any label is displayed.
4. Select one or several devices from the list of devices.
5. Drag and drop the selected devices to a specific label. A pop-up window opens and prompts you to confirm the label assignment.
6. To confirm the assignment, click **Yes**.

Assigning a Group Role or Persona

A persona in Central refers to a device role that you can set for the SD Branch device groups. To deploy the SD Branch solution, you must assign different roles to the devices that function as Branch Gateways and VPN Concentrators.

When you add a Gateway to a group, Central does not assign a persona or group role to the group by default. However, when you try to access device for the first time, Central prompts you to set the group role to either Branch Gateway or VPNC (VPN Concentrator). Ensure that you explicitly set the group persona.

---

**NOTE**

After you mark a group as a VPNC or Branch Gateway, Central does not allow you to edit or modify the device
Connecting SD-WAN Gateways to Central

The SD-WAN Gateways have the ability to automatically provision themselves and connect to Central once they are powered on. The SD-WAN Gateways also support multiple active uplinks for ZTP (also referred to as automatic provisioning). By default, ZTP is enabled on all ports except for 0/0/1. All these ZTP ports are assigned to VLAN 4094.

To automatically provision the SD-WAN Gateways:

1. Connect your SD-WAN Gateway to the provisioning network.
2. Wait for the device to obtain an IP address through DHCP. SD-WAN Gateways support multiple uplink ports. The first port to receive the DHCP IP connects to the Activate server and completes the provisioning procedure:
   - If the device has factory default configuration, it receives an IP address through DHCP, connects to Aruba Activate, and downloads the provisioning parameters. When a device identifies Central as its management entity, it automatically connects to Central.
   - If the device is running a software version that does not have the SD-WAN image, the devices are automatically upgraded to a supported SD-WAN software version.
3. Observe the LED indicators. Table 6 describes the LED behavior.

<table>
<thead>
<tr>
<th>LED Indicator</th>
<th>LCD Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid Amber</td>
<td>Getting DHCP IP</td>
<td>Indicates that the uplink connection is UP, but DHCP IP is yet to be retrieved.</td>
</tr>
<tr>
<td>Blinking Amber</td>
<td>Activate Wait</td>
<td>Indicates that the device was able to reach the DHCP server and the connection to the Activate server is yet to be established.</td>
</tr>
<tr>
<td>Solid Green</td>
<td>Activate OK</td>
<td>Indicates that the device was able to retrieve provisioning parameters from the Activate server.</td>
</tr>
<tr>
<td>Alternating Solid Green and Amber</td>
<td>Activate Error</td>
<td>Indicates that the device was not able to retrieve provisioning parameters.</td>
</tr>
</tbody>
</table>

After successfully connecting to Central, the SD-WAN Gateways download the configuration from Central and reload.

The SD-WAN Gateways also include service ports that the technicians can use for manually provisioning devices in the event of ZTP failure. For more information on ports available for Aruba 7000 Series Mobility Controllers and Aruba 7200 Series Mobility Controllers, see ArubaOS User Guide.

Allowing Device Communication over Network Firewall

The SD Branch appliances use HTTPS and IPsec tunnels for secure communication:

- The HTTPS WebSockets is used for the management traffic; that is, for communication between Central and VPN Concentrators, and Central and Branch Gateways.
- The IPsec tunnel is used for communication between Branch Gateways and VPN Concentrators.
Although most of the communication between devices on the remote site and the Central server is carried out through HTTPS (TCP 443), you may want to open the ports listed in Table 7 to allow communication over a network firewall.

**Table 7: Domain Names and Ports**

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Protocol and port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool.ntp.org</td>
<td>UDP port 123</td>
<td>To update internal clock on and configure time zone when a factory default device comes up. By default, devices contact pool.ntp.org and use NTP to synchronize their system clocks.</td>
</tr>
<tr>
<td>device.arubanetworks.com</td>
<td>TCP port 443</td>
<td>To get provisioning parameters from Aruba Activate. NOTE: Devices must be able to resolve device.arubanetworks.com with a valid DNS server.</td>
</tr>
<tr>
<td>activate.arubanetworks.com</td>
<td>TCP port 443</td>
<td>To configure provisioning rules in Activate.</td>
</tr>
<tr>
<td>portal.central.arubanetworks.com</td>
<td>TCP port 443</td>
<td>To access Central login portal. After a successful authentication, the users are redirected to their respective accounts from which they can manage, configure, and monitor devices.</td>
</tr>
<tr>
<td>app1.central.arubanetworks.com</td>
<td>TCP port 443</td>
<td>To allow devices to communicate with Central.</td>
</tr>
<tr>
<td>internal.central.arubanetworks.com</td>
<td>TCP port 443</td>
<td>To allow users to access Central portal.</td>
</tr>
<tr>
<td>images.arubanetworks.com</td>
<td>TCP port 80</td>
<td>To access the first server for firmware images to upgrade the devices managed by Central.</td>
</tr>
<tr>
<td><a href="http://h30537.www3.hpe.com">http://h30537.www3.hpe.com</a></td>
<td>TCP port 80</td>
<td>To access firmware images for switches hosted on HPE My Network Portal (MNP).</td>
</tr>
<tr>
<td>d2vxf1jrhr3p0.cloudfront.net</td>
<td>TCP port 80</td>
<td>To access the second server for Instant AP firmware upgrade.</td>
</tr>
<tr>
<td>rcs-m.central.arubanetworks.com</td>
<td>TCP port 443</td>
<td>To access an AP console through SSH.</td>
</tr>
<tr>
<td>cloud.arubanetworks.com</td>
<td>TCP port 80</td>
<td>To open the Central evaluation sign-up page.</td>
</tr>
<tr>
<td>aruba.brightcloud.com</td>
<td>TCP port 443</td>
<td>To access the Brightcloud server for application, application categories, and website content classification.</td>
</tr>
<tr>
<td>pqm.arubathena.com</td>
<td>ICMP</td>
<td>To allow Central to probe PQM nodes for the source IP address of the SD-WAN Gateways. To enable PQM nodes to communicate with Central and whitelist IP addresses of the SD-WAN Gateways using the PQM service.</td>
</tr>
</tbody>
</table>
Uploading Certificates

By default, Central includes a self-signed certificate that is available on the **Global Settings > Certificates** page. The default certificate is not signed by a root CA. For devices to validate and authorize Central, administrators must upload a valid certificate signed by the root CAs.

Aruba devices use digital certificates for authenticating a client’s access to user-centric network services. Most devices such as controllers and Instant APs include a server certificate by default for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Central-managed devices such as Instant AP and switches support the following root CA certificates:

<table>
<thead>
<tr>
<th>Instant APs</th>
<th>Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>● AddTrust</td>
<td>● Comodo</td>
</tr>
<tr>
<td>● GeoTrust</td>
<td>● GeoTrust</td>
</tr>
<tr>
<td>● VeriSign</td>
<td></td>
</tr>
<tr>
<td>● Go Daddy</td>
<td></td>
</tr>
</tbody>
</table>

Uploading Certificates

To upload certificates, complete the following steps:

1. Go to **Global Settings > Certificates**. The **Certificates** page opens.
2. Click the plus icon to add the certificate to the certificate store.
3. In the **Add Certificate** dialog box, do the following:
   a. In the **Name** text box, specify the certificate name.
   b. Select the type of certificate. You can select any one of the following certificates:
      i. **CA** — Digital certificates issued by the CA.
      ii. **Server** — Server certificates required for communication between devices and authentication servers.
      iii. **CRL** — Certificate Revocation List that contains the serial numbers of certificates that have been revoked. This certificate is required for performing a certificate revocation check.
      iv. **OCSP Responder Cert** — OCSP responder certificates.
      v. **OCSP Signer Cert** — OCSP Response Signing Certificate.
   c. The OCSP certificates are required for OCSP server authentication.
   d. From the **Format** drop-down list, select a certificate format; for example, PEM, DER, and PKCS12.
   e. In the **Passphrase** text box, select a passphrase.
   f. In the **Retype Passphrase** text box, retype the passphrase for confirmation.
The Passphrase and Retype Passphrase text boxes are displayed only when you select Server Certificate from the Type drop-down list.

f. In the Certificate File field, click Choose File and browse to the location where the certificates are stored and select the certificate files.

g. Click Add. The certificate is added to the Certificate Store.

Managing Certificates on Instant APs Configured Using Templates

Central supports uploading multiple certificates to Instant APs configured using templates. You can manage certificates either from the Central UI or through the API Gateway. For more information about APIs, see API Documentation.

To push certificates to Instant APs configured using templates:

1. Upload certificate(s).
   a. From the app selector, go to Global Settings > Certificates and click the plus icon to upload the certificate to the certificate store. For more information, see Uploading Certificates on page 22.
   b. API—Use the [POST] /configuration/v1/certificates API to upload certificates.

2. Make a note of the certificate name and MD5 checksum.
   a. In the UI, go to Global Settings > Certificates > Certificate Store table to get these details.
   b. Use the [GET] /configuration/v1/certificates API to get these details.

3. In the template, anywhere before the per-ap settings block, depending on your requirement, add one or more of the following commands:

   ca-cert-checksum <ca_cert_checksum/ca_cert_name>
   cp-cert-checksum <captive_portal_cert_checksum/captive_portal_cert_name>
   radsec-ca-cert-checksum <radsec_ca_checksum/radsec_ca_name>
   radsec-cert-checksum <radsec_cert_checksum/radsec_cert_name>
   server-cert-checksum <server_cert_checksum/server_cert_name>

You can either use the certificate name or the checksum value in the command. Or, you can set it as a variable and enter the variable value for the Instant AP. Aruba recommends using the certificate name.

Example 1

ca-cert-checksum my_default_cert

Example 2

ca-cert-checksum %ca_cert_name%

variable:
{
    "ca_cert_name": "my_default_cert"
}
Administrators can set up a redundancy scheme in the SD branches and data centers to provide a highly available and an always-on network. The data center, VPN Concentrator, and Branch Gateway failover redundancy features allow network administrators to significantly reduce the downtime and client traffic disruptions.

**Data Center Redundancy**

The SD-WAN solution supports active-standby or active-active VPN Concentrator configuration at the data center. Any of the Aruba 7200 Series controllers can be set to function as a VPN Concentrator at the data center or headquarters, to aggregate data traffic from branches.

Administrators can configure primary and redundant VPN Concentrators in active-active mode to allow some Branch Gateways to terminate on one VPN Concentrator and the remaining on the second VPN Concentrator.

For example, if you have data centers on the East and West Coasts, half of the branch sites could connect to the data center on the West Coast as primary and that on the East Coast as backup. The remaining sites could connect to the East Coast data center as primary and that on the West Coast as backup. This architecture reduces downtime during VPN Concentrator failures as only half of the sites need to switch to the backup VPN Concentrator.

**VRRP Redundancy**

The Virtual Router Redundancy Protocol (VRRP) is used to create various redundancy solutions, such as pairs of SD-WAN Gateways acting in active-backup mode or in primary-standby mode by using a virtual IP address. When the primary device becomes unavailable, a backup SD-WAN Gateway comes up as the primary device with the virtual IP address. All network elements (APs and other devices) can be configured to access the virtual IP address, thereby providing a transparent redundant solution to your network.

VRRP eliminates a single point of failure by providing a mechanism to elect a VRRP master device. If VRRP preemption is disabled and all SD-WAN Gateways share the same priority, the first device that comes up is elected as the VRRP master. However, if VRRP preemption is enabled and all devices share the same priority, the device with the highest IP address becomes the VRRP master.

To avoid routing loops during overlay negotiation with the hubs, Branch Gateways automatically suppress route advertisements for subnets that do not have VRRP state as Master.

**Configuring SD-WAN Gateway Redundancy**

To configure redundancy on the primary and backup SD-WAN Gateways, complete the following steps:

- Configure DHCP State Synchronization on page 25
- Configure Peer SD-WAN Gateways and Transport VLAN for WAN Redundancy on page 25
- Configure VRRP for LAN Redundancy on page 25
Configure DHCP State Synchronization
To configure DHCP state synchronization, configure a corporate NTP server at the group level. For more information, see Configuring NTP Server on page 35.

Ensure that you create the same DHCP scope on both SD-WAN Gateways.

Configure Peer SD-WAN Gateways and Transport VLAN for WAN Redundancy
Aruba SD-Branch solution is capable of establishing a virtual link between redundant SD-WAN Gateways to share the WAN interfaces. This virtual link is a GRE tunnel that is automatically established between Branch Gateways when peer SD-WAN Gateways and transport VLAN are configured.

When the virtual link is established, Branch Gateways share uplink interfaces with their peers. Peer SD-WAN Gateways use uplink interfaces from the other SD-WAN Gateways only if WAN ports are configured with different uplink VLANs.

It is recommended not to configure the same SD-WAN Gateway as the Master for some VLANs and as Backup for some other VLANs.

To set up the communication between SD-WAN Gateways, complete the following tasks:
1. From the app selector, click Gateway Management.
2. Select the SD-WAN Gateway for which you want to configure redundancy.
3. Click High Availability. The Redundancy configuration page opens.
4. Enter the peer SD-WAN Gateway IP address in the Peer gateway IP address field to enable Branch Gateway redundancy with uplink sharing.
5. Select the VLAN ID from the VLAN ID connecting to peer gateway field to configure the transport VLAN for communication between the redundant SD-WAN Gateways.
6. Save the changes.
7. Repeat steps 1-6 on the configured peer SD-WAN Gateway to enable uplink load sharing.

Peer SD-WAN Gateways use uplink interfaces from the other SD-WAN Gateways only if WAN ports are configured with different uplink VLANs.

Configure VRRP for LAN Redundancy
Before you begin configuring VRRP redundancy, obtain the following network information:

- VLAN ID for the two SD-WAN Gateways on the same layer 2 network.
- Virtual IP address to be used for the VRRP instance.

To configure VRRP redundancy, complete the following tasks:
1. From the app selector, click Gateway Management.
2. Select the group in which the SD-WAN Gateways are assigned.
3. Click High Availability. The Redundancy configuration page opens.
4. Click + to add a new virtual router in the Virtual Router Table. The New Virtual Router section appears.
5. Select the IP version from the IP Version drop-down list.
6. Select the VLAN on which you want to configure VRRP from the VLAN drop-down list.
7. Set Admin State to UP.
8. Specify the priority value in the Priority field. For a backup SD-WAN Gateway, use the default priority value of 100. For the primary SD-WAN Gateway, use a priority value higher than the default value, such as 110.
9. Configure other VRRP parameters as described in Table 8.
10. Save the changes.
11. Repeat steps 1-10 to configure VRRP on the other device in the primary and backup redundant pair.

Table 8: VRRP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The ID uniquely identifies a VRRP instance. For ease of administration, specify VLAN ID as the ID.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the VRRP instance.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Password to authenticate VRRP peers in their advertisements.</td>
</tr>
<tr>
<td>Retype authentication password</td>
<td>Reconfirm the password, if configured.</td>
</tr>
<tr>
<td>IP address</td>
<td>This is the virtual IP address that will be owned by the elected VRRP master. Ensure that the same IP address and VRRP ID is configured on each member of the redundant pair.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority level of the VRRP instance for the device. This value is used in the election mechanism for the master. When configuring VRRP on a standby device, use the default priority value of 100. For a master device, use a higher priority value such as 110.</td>
</tr>
<tr>
<td>Advertisement interval (secs)</td>
<td>This is the interval, in seconds, between successive VRRP advertisements sent by the current master. The default interval time is recommended. Default: 1 second</td>
</tr>
<tr>
<td>Enable router Pre-emption</td>
<td>Selecting this option means that a device can take over the role of master if it detects a lower priority device that is currently acting as master.</td>
</tr>
<tr>
<td>Pre-emption delay (secs)</td>
<td>Specifying a value enables the delay timer. The timer is triggered when the VRRP state moves out of backup or init state to become a master. This is applicable only if you enable router pre-emption. When the timer is triggered, it forces VRRP to wait for a specified period of time, so that all the applications are ready before coming up. This prevents the APs from connecting to the SD-WAN Gateway before the SD-WAN Gateway can accept the connection. In the meantime, if there is an advertisement from another VRRP, the VRRP stops the timer and does not transition to master.</td>
</tr>
<tr>
<td>Admin state</td>
<td>Administrative state of the VRRP instance. To start the VRRP instance, change the admin state to UP.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN on which the VRRP protocol runs.</td>
</tr>
</tbody>
</table>
### Table 8: VRRP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking master uptime</td>
<td>(Optional) Perform VRRP priority tracking based on how long the device has been the master. This feature is designed to ensure that a master will only be allowed to take and maintain control of the VRRP if it has been up for a certain amount of time in minutes (0-1440). This prevents a common issue where a device that is periodically going up and down assumes the role of primary master.</td>
</tr>
<tr>
<td>Tracking master uptime priority</td>
<td>(Optional) The additional priority given to the master once it has been up for the time interval defined by the Tracking Master Up-time parameter.</td>
</tr>
<tr>
<td>Tracking VRRP master state ID</td>
<td>(Optional) Perform tracking based on the UP or DOWN state of another VRRP master by specifying the VRRP ID of the master to be tracked.</td>
</tr>
<tr>
<td>Tracking VRRP master state priority</td>
<td>(Optional) The priority taken away from a VRRP master if it is in a DOWN state. The priority levels are returned to their previous state when the VRRP master comes back up.</td>
</tr>
<tr>
<td>Tracking VLAN</td>
<td>(Optional) Perform VRRP priority tracking based on the UP or DOWN state of a VLAN. Click + below the Tracking VLAN table and specify the following values:</td>
</tr>
<tr>
<td>- VLAN Id: ID of the VLAN to be tracked.</td>
<td></td>
</tr>
<tr>
<td>- Subtract: Priority level to be subtracted from the device's VRRP priority if the tracked VLAN goes down.</td>
<td></td>
</tr>
<tr>
<td>Tracking interface</td>
<td>(Optional) Perform VRRP priority tracking based on the UP or DOWN state of a specific interface. Click + below the Tracking Interface table and specify the following values:</td>
</tr>
<tr>
<td>- Interface: Interface Port to be tracked.</td>
<td></td>
</tr>
<tr>
<td>- Subtract: Priority level to be subtracted from the device's VRRP priority if the tracked interface goes down.</td>
<td></td>
</tr>
</tbody>
</table>
This section guides you through the steps required to set up your SD-WAN network.

Central offers the following options for configuring your branch devices for building an SD-WAN network:

- **Groups**—You can create a logical subset of devices as groups. If you have devices that must share common configuration settings, ensure that you assign these devices to the same group. Any new device joining a group inherits the configuration that is already applied on the devices in a group. Similarly, you can also maintain separate groups for Branch Gateways and VPN Concentrators by assigning a group role for the devices. For more information, see Assigning Groups on page 18.

- **Device-specific configuration**—If you have fewer devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration on one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level. Central marks the discrepancies in the group and device configuration as overrides on the Configuration Audit page.

- **Bulk Configuration**—Central supports several bulk configuration options for SD-WAN Gateways:

  - **Bulk Configuration Upload**—Allows you to download a list of SD-WAN Gateways from Central in the CSV file format. You can add the configuration parameters for host name, system IP address, VLAN, and Ports, and then upload the CSV file to Central. For more information, see Uploading Bulk Configuration Template on page 33.

  - **Gateway Pools**—Allows you to create a common pool of IP addresses and enable automatic assignment of IP addresses to SD-WAN Gateways. For more information, see Configuring Gateway Pools for SD-WAN Gateways on page 29.

  - **DHCP Pools**—Allows you to configure a DHCP pool, using which Central automatically assigns a subnet to each SD-WAN Gateway for a given VLAN. For more information, see Configuring DHCP Address Pools on page 30.

  - **APIs**—Allows you to configure and monitor devices using NB APIs.
**SD-WAN Configuration Checklist**

*Table 9* describes the configuration workflow for the SD Branch devices:

<table>
<thead>
<tr>
<th><strong>VPN Concentrators</strong></th>
<th><strong>Branch Gateways</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Address Pools</td>
<td>Configure Address Pools</td>
</tr>
<tr>
<td>Configure Hostname and IP address</td>
<td>Configure Hostname and IP address</td>
</tr>
<tr>
<td>Configure VLAN Interfaces</td>
<td>Configure VLAN Interfaces</td>
</tr>
<tr>
<td>Assign VLANs to Switchports</td>
<td>Configure Ports</td>
</tr>
<tr>
<td>Whitelist Branch Gateways</td>
<td>Assign VLANs to Switchports</td>
</tr>
<tr>
<td>Configure Static Routes</td>
<td>Configure WAN Uplinks</td>
</tr>
<tr>
<td>Configure OSPF</td>
<td>Configure Hub and Spoke VPN</td>
</tr>
<tr>
<td></td>
<td>Configure Site to Site VPN</td>
</tr>
<tr>
<td></td>
<td>Configure Dynamic Path Steering Policies</td>
</tr>
<tr>
<td></td>
<td>Configure Policies for PBR</td>
</tr>
<tr>
<td></td>
<td>Configure Firewall Policies</td>
</tr>
<tr>
<td></td>
<td>Configure User Roles</td>
</tr>
<tr>
<td></td>
<td>Configure Authentication Profiles</td>
</tr>
<tr>
<td></td>
<td>Install CA and Server Certificates</td>
</tr>
</tbody>
</table>

**Configuring Address Pools for SD-WAN Gateways**

The SD Branch requires a pool of IP addresses to be configured for a branch site to allow dynamic assignment of IP addresses to SD Branch and client devices.

The SD Branch deployment requires the following types of address pools:

- **Gateway Pool**—A gateway pool is used to assign a range of IP addresses for a device group, from which IP addresses are assigned to each SD-WAN Gateway that joins this device group.

- **DHCP pools**—A DHCP pool for a configuration group defines a set of IP addresses that can be assigned to client devices associated to Branch Gateways.

- **NAT Pools**—A NAT pool is used for translating the source IP address when forwarding port traffic or allowing traffic from the outside network to the designated hosts in the branch network.

- **Tunnel Pools**—A tunnel pool defines a range of IP addresses that can be used by the Branch Gateway to create a GRE tunnel to the headend gateway. When you add a Branch Gateway, an IP address is removed from the tunnel pool on that hierarchy node and is leased to that device. Addresses no longer in use are automatically returned to the pool for reallocation.

*Note:* Tunnel pools and gateway pools can be configured only at the group level as they are not applicable to the device level configuration.

**Configuring Gateway Pools for SD-WAN Gateways**

A gateway pool refers to a pool of IP addresses configured for a device group. The system IP addresses for the SD-WAN Gateways are assigned from the gateway pool as and when a device joins the group.
Creating Gateway Pools for SD-WAN Gateways
To create a gateway pool for a device group, complete the following steps:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the device group to configure.
3. Click Interfaces > Pool Management.
4. Expand Gateway Pool.
5. To create a new gateway pool, click +.
6. In the Pool name field, enter a name for the new pool.
7. In the Start IP address field, enter the first IP address of the IP address range.
8. In the End IP address field, enter the last IP address of the IP address range.
9. Click Save Settings. The gateway pool must be assigned to a VLAN to allow Central to dynamically assign IP addresses from the pool.

Assigning a VLAN to a Gateway Pool
To assign a VLAN to a gateway pool:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the device group to configure.
3. Click Interfaces > VLANs.
4. Select a VLAN from the VLANs table.
5. Select the VLAN ID from the VLAN IDs table. The VLAN details are displayed.
6. From the IP assignment drop-down list, select Gateway pool.
7. Select the required gateway pool from the VLAN Pool drop-down list.
8. Save the changes. To enable IP address assignment to SD-WAN Gateways from the gateway pool, see Configuring System IP Address for SD-WAN Gateways on page 34.

Configuring DHCP Address Pools
A DHCP pool is a set of IP addresses that can be assigned to the client devices associated to the Branch Gateways of a specific branch. DHCP pools allow dynamic and automatic assignment of IP addresses for VLAN interfaces when the SD-WAN Gateway acts as the DHCP server.

Creating a DHCP Pool
To create a DHCP address pool on a Branch Gateway:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click Interfaces > DHCP.
4. Select the IPv4 DHCP server checkbox to enable the SD-WAN Gateway to act as a DHCP server.
5. To add a new pool, click + below the Pool Configuration table.
6. Configure the following parameters:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP version</td>
<td>The IP version of the pool.</td>
</tr>
<tr>
<td>Pool Name</td>
<td>Name of the new address pool.</td>
</tr>
<tr>
<td>Network IP address type</td>
<td>Network address type. Select <strong>Static</strong> to add a static IP address and netmask to the pool, or select <strong>Dynamic</strong> to define a range of addresses that the DHCP server may assign to clients.</td>
</tr>
<tr>
<td></td>
<td>- If you selected <strong>Static</strong>, you must enter the IP address and IP mask of the network in the <strong>Network IP address</strong> and <strong>Network IP mask</strong> fields. You must also specify the IP address of the default router for the DHCP client in the <strong>Default routers</strong> field. The client should be on the same subnet as the default router. You can specify up to eight IP addresses.</td>
</tr>
<tr>
<td></td>
<td>- If you selected <strong>Dynamic</strong>, you must enter the starting and ending IP addresses for the address range, as well as the maximum number of hosts to be supported by the pool.</td>
</tr>
<tr>
<td>Import DNS address from DHCP/PPPoE</td>
<td>Enable this option to import DNS server address obtained through PPPoE or DHCP.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Domain name to which the client belongs.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Configure the DNS server IP address by selecting one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Specify Servers</strong>—Select this option and specify the IP addresses of the DNS servers in the <strong>DNS servers IP addresses</strong> field. You can specify up to eight IP addresses. Multiple IP addresses must be separated by spaces.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Import DNS address from DHCP/PPPoE</strong>—Select this option to import DNS server address obtained through PPPoE or DHCP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Use address of MM/MD</strong>—Select this option to use the SD-WAN Gateway as the DNS server.</td>
</tr>
<tr>
<td>Import WINS server from DHCP/PPPoE</td>
<td>Enable this to import the NetBIOS name server address that is obtained through PPPoE or DHCP.</td>
</tr>
<tr>
<td>WINS</td>
<td>IP address of a NetBIOS Windows Internet Naming Service (WINS) server if you are not importing the WINS address from DHCP or PPPoE. You can specify up to eight IP addresses. Multiple IP addresses must be separated by spaces. <strong>NOTE:</strong> This field is not applicable if you enabled the <strong>Import DNS address from DHCP/PPPoE</strong> option.</td>
</tr>
<tr>
<td>Lease time</td>
<td>The number of days, hours, or minutes for which the assigned IP address is valid for the client.</td>
</tr>
<tr>
<td>Pool type</td>
<td>Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>public</strong>—To assign addresses from a public pool.</td>
</tr>
<tr>
<td></td>
<td>- <strong>private</strong>—To assign addresses from a private pool.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ipupsell</strong>—To assign either private or public address from a designated DHCP pool.</td>
</tr>
<tr>
<td>Option</td>
<td>Click <strong>Option</strong> to add a client-specific option code and IP address or text string.</td>
</tr>
</tbody>
</table>
Excluding IP Address Range

To exclude an IP address or a range of IP addresses from the DHCP pool, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Interfaces > DHCP**.
4. Click + from the **IPv4 Excluded Address Range** table.
5. Specify the IP address range in the **IPv4 excluded range** field.
6. Save the changes.

Assigning a VLAN to a DHCP Address Pool

To assign a DHCP address pool to a VLAN:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Interfaces > VLAN**.
4. In the **VLANs** table, select the name of the VLAN to which you want to assign the DHCP pool.
5. Select the VLAN ID of the VLAN. The VLAN details are displayed.
6. In the **IPv4** tab, click the **IP assignment** field.
   a. To add static DHCP pool, select DHCP.
   b. To add dynamic DHCP pool, select **Dynamic DHCP Pool** and select a DHCP pool to associate to the VLAN from the **Dynamic DHCP Pool** drop-down list.
7. Save the changes.

Configuring NAT Pools

A NAT pool provides a set of IP addresses that can be used for translating network addresses for the outgoing traffic from the branch network.

Creating a NAT Pool

To create a NAT pool, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Interfaces > Pool Management**.
4. Expand **NAT Pool**.
5. To add a new pool, click + below the **NAT Pools** table.
6. In the **Pool name** field, enter a name for the new pool.
7. In the **Start IP address** field, enter the first IP address of IP address range.
8. In the **End IP address** field, enter the last IP address of the IP address range.
9. In the **Destination NAT IP address** field, enter the IP address to configure the destination NAT.
10. Select the **Used by VPN** if this NAT pool is used by the VPN.
11. Click **Save Settings**.
Creating a Static 1:1 NAT Pool

To create a static 1:1 NAT pool on a Branch Gateway, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Interfaces > Pool Management**.
4. Expand **Static 1:1 NAT**.
5. In the **INTERNAL ADDRESS** field, enter the internal IP address of the device.
6. In the **EXTERNAL ADDRESS** field, enter the IP address to be mapped to the device; this IP address is exposed outside of the network.
7. Click **Save Settings**.

Based on your branch requirements, you can enable NAT on VLAN interfaces for the traffic that is routed through the tunnel. For more information on enabling NAT for egress traffic, see Configuring VLANs for WAN Interfaces on page 43.

A tunnel pool defines a range of IP addresses that can be used by the Branch Gateways in a group to create a GRE tunnel to the headend gateway. When you add a Branch Gateway to the group, an IP address is removed from the tunnel pool on that hierarchy node and is leased to that device. Addresses no longer in use are automatically returned to the pool for reallocation.

---

**NOTE**

Tunnel pools can be configured only at the group level and is not applicable for the device level configuration.

---

Configuring Tunnel Pools for SD-WAN Gateways

To create a tunnel pool on a Branch Gateway group, perform the following tasks:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device group to configure.
3. Click **Interfaces > Pool Management**.
4. Expand **Tunnel Pools**.
5. To add a new pool, click + below the **Add New Tunnel Pool** table.
6. Configure the following parameters and click **Save Settings**.

### Table 11: DHCP Pool Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool Name</td>
<td>Name of the new tunnel pool.</td>
</tr>
<tr>
<td>Start IP address</td>
<td>Enter the IP address to define the start of the range of addresses.</td>
</tr>
<tr>
<td>End IP address</td>
<td>Enter the IP address to define the end of the range of addresses.</td>
</tr>
</tbody>
</table>

---

Uploading Bulk Configuration Template

Central allows you to configure VLANs, ports, DHCP Pools, PPPoE credentials or IP addresses for SD-WAN Gateways in bulk.

To upload a template for bulk configuration:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select a device group.
3. Click **Interfaces > Bulk Configuration Uploads**.
4. Click **Download Device Template**. A CSV file with a list of SD-WAN Gateways is downloaded to your local directory.
5. Update the CSV file with configuration parameters for VLANs, DHCP pools, and IP address assignment.
6. Upload the template and click **Submit**. The configuration changes are applied to the SD-WAN Gateways in the group.

### Configuring System Information for SD-WAN Gateways

This section describes the procedures for configuring system parameters for SD-WAN Gateways.

- [Configuring Hostname for SD-WAN Gateways on page 34](#)
- [Setting System Clock and Time Zone on SD-WAN Gateways on page 35](#)
- [Configuring System IP Address for SD-WAN Gateways on page 34](#)
- [Configuring Domain Name System on page 36](#)
- [Configuring Redirect DNS Servers on page 36](#)
- [Configuring Dynamic Domain Name System on page 37](#)
- [Setting Capacity Threshold on page 38](#)

#### Configuring Hostname for SD-WAN Gateways

To assign a hostname to SD-WAN Gateways:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway to configure.
3. Click **System > General**.
4. Click **Basic Info**.
5. Enter a hostname.
6. If required, configure admin credentials.
7. Click **Save Settings**.

#### Configuring System IP Address for SD-WAN Gateways

To configure system IP address for SD-WAN Gateways, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or the device group.
3. Click **System > General**.
4. Click **System IP Address**.

- To dynamically assign system IP addresses to all devices in a group, ensure that a gateway address pool is configured and assigned to a VLAN interface. Central dynamically assigns system IP addresses from the gateway address pool to the devices when they join the group. For more information on gateway pools, see [Assigning a VLAN to a Gateway Pool on page 30](#).

- To assign a system IP address at the device level, ensure that a VLAN interface is configured for the device with one of the following IP assignment methods:
  - **Static IP**—Assigns a static IP address to the SD-WAN Gateway.
• **DHCP**—Allows you to configure a DHCP server for dynamic assignment of a system IP address to the SD-WAN Gateway.
• **PPPoE**—Allows you to configure a PPPoE server for assigning a system IP address to the SD-WAN Gateway.

For more information on IP assignment methods, see [IP assignment on page 45](#).

5. From IPv4 drop-down, select the required VLAN interface.
6. Click **Save Settings**.

### Setting System Clock and Time Zone on SD-WAN Gateways

You can set the clock on a Branch Gateway manually or by configuring the SD-WAN Gateways to use an NTP server to synchronize its system clock with a central time source. The system automatically updates the time zone including the relevant daylight savings time (DST) across time zones. This is done in view with keeping the time up-to-date and precise with daylight savings time adjustments effected automatically.

### Configuring NTP Server

The **Burst Mode** is a configurable option and not the default behavior for the Branch Gateway, as this option is considered recommended by some public NTP servers. If an NTP server is unresponsive, the **Burst Mode** continues to send frequent queries until the server responds and time synchronization starts.

To add an NTP server:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > General**.
4. Click **Clock**.
5. Select **Get time from NTP server** and click the + icon.
7. Enter the IPv4 or IPv6 address of the NTP server based on your selection in the previous step.
8. Select the **Burst mode** check box, if required. It is disabled by default.
9. Enter the authentication key to be used by NTP server in the **Authentication key** text box. The range of allowed values is 1–65534.

### Enabling NTP Authentication

NTP authentication allows NTP clients to authenticate before synchronizing clocks. NTP authentication works by using a symmetric key that is configured by the user. The secret key is shared both by the SD-WAN Gateway and an external NTP server.

NTP authentication is disabled by default.

1. Enable **Use NTP authentication**.
2. Under NTP Authentication, click +. The **Add NTP Authentication** section is displayed.
3. Enter the authentication key in the **Authentication key** text box. The allowed range of numeric values is 1–65534.
4. Enter value for the MD5 secret. The valid key value must be an ASCII string from 0 to 255 characters.
5. Select the **Trusted key** check box to specify that the authentication key is trusted. By default, the check box is cleared.

6. Click **Save Settings**.

### Setting Time Zone

To set a time zone:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > General**.
4. Click **Clock**.
5. In the **Timezone** section, select the appropriate time zone from the drop-down list.
6. Click **Save Settings**.

### Setting the Clock to Summer Time

If your time zone supports Daylight Saving Time (DST) or summer time, you can enable DST to adjust the clocks. DST refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > General**.
4. Click **Clock**.
5. Under **Summer Time**, using the toggle switch activate **Adjust clock in summer**.
6. Configured the desired time settings and click **Save Settings**.

### Configuring Domain Name System

Network devices on the Internet use an IP address to route your request to the site you are trying to reach. Once you connect through a DNS server, it manages a database that maps domain names to IP addresses and routes your query to the next appropriate server.

To enable SD-WAN Gateways to connect to a DNS server:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device group.
3. Click **System > General**.
4. Click **Domain Name System**.
5. Enter a domain name.
6. Enable DNS name resolution.
7. To add a DNS Server, click + in the **DNS Servers** table and enter the IP address of the DNS server.
8. Click **Save Settings**.

### Configuring Redirect DNS Servers

SD-WAN Gateways can now redirect DNS queries to dedicated DNS servers configured for the corporate and public domains. This feature allows you to optimize the load on the corporate DNS servers by splitting and
redirecting non-corporate traffic to a separate DNS server configured on the Branch Gateway.

To enable Redirect DNS feature and to configure name servers for specific domains, complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device group.
3. Click **System > General**.
4. Click **Domain Name System**.
5. Enable DNS name resolution.
6. Enable the Redirect DNS option.
7. To add domains, click + in the **Domains to Redirect** table.
8. Enter the following information in the **New Redirect DNS Server** pop-up:
   - **Domain**—Enter the domain name.
   - **IP Version**—Select the IP version.
   - **IP address**—Enter the IP address of the DNS server to be redirected for the specified domain name.

   You can configure up to three IPv4 and three IPv6 redirect DNS servers on a Branch Gateway.

9. Click **Save Settings**.

**Configuring Dynamic Domain Name System**

Dynamic DNS, also known as DDNS, solves the problem of ever changing IP addresses by associating your address with a consistent domain name without the need for a static IP.

The dynamic IP addresses assigned through a DHCP server frequently change, as the ISPs manage their own online systems. This makes it difficult to access the Branch Gateway if the DHCP issued address continues to change without notice.

The dynamic DNS feature assigns a custom domain name to your home IP address that updates automatically whenever your home IP changes. A device on your network periodically communicates your IP to the dynamic DNS service. The domain name resolution changes as your IP changes. Thus, even if your IP changes, you can still connect to your device to the network using the same hostname.

To configure SD-WAN Gateways to connect to a dynamic DNS server:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device group.
3. Click **System > General**.
4. Click **Dynamic Domain Name System**.
5. Specify the **Server interval** and **Server IP** values.
6. Select one of the following values for **Authentication type**:
   - **hmac-md5**
   - **hmac-sha1**
   - **hmac-sha256**
7. Enter appropriate values in **Authentication name** and **Authentication key** for the specified authentication type.
8. Add the required DHCP pools from the available list.
9. Save the changes.

**Setting Capacity Threshold**

You can set capacity thresholds for SD-WAN Gateways to trigger alerts when they exceed the set percentage of the total capacity configured for its resources.

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > General**.
4. Click **Capacity Threshold**. Configure the threshold parameters listed in Table 12 as per your requirement.

**Table 12: Capacity Alert Thresholds**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Datapath CPU</strong></td>
<td>Sets an alert threshold for datapath CPU capacity. When the total datapath CPU capacity exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 30%.</td>
</tr>
<tr>
<td><strong>Controlpath CPU</strong></td>
<td>Set an alert threshold for controlpath CPU capacity. When the total controlpath CPU capacity exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 45%.</td>
</tr>
<tr>
<td><strong>Controlpath memory</strong></td>
<td>Set an alert threshold for controlpath memory consumption. When total memory capacity exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 85%.</td>
</tr>
<tr>
<td><strong>Total tunnels</strong></td>
<td>Set an alert threshold for the tunnel capacity. When the total tunnel capacity of the device exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 80%.</td>
</tr>
<tr>
<td><strong>Total users</strong></td>
<td>Set an alert threshold for the user capacity. When the total resource capacity of the device exceeds the configured threshold percentage, an alert is triggered. The default threshold for this parameter is 80%.</td>
</tr>
</tbody>
</table>

**Configuring Device Administrator Credentials for SD-WAN Gateways**

An SD-WAN Gateway administrator or a management user referred in this topic denotes a user who can access the SD-WAN Gateway device user interface for troubleshooting purposes. We need to configure credentials for these administrators to access the SD-WAN Gateway user interface for troubleshooting device specific issues. The Central system administrators or other Central system users need not be the management users of the SD-WAN Gateways.

The management users configured on SD-WAN Gateways are restricted to access and troubleshoot only the device related issues through the device user interface. Any other tasks such as configuration, management, or device upgrade for an SD-WAN Gateway are performed only from the Aruba Central UI.

**Configuring Management User Accounts for SD-WAN Gateways**

To create a management user account complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > Admin**.
4. Under **Management User** enable the **Enable local authentication** toggle switch.
5. Click + from the **Management User** table.
6. Enter values for **Username** and **Password**.
7. Select a role from the drop-down list.
8. Click **Save Settings**.

**Creating a New User with Certificate Authentication**

This section describes the steps to create a new user with certificate authentication:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > Admin > Management User**.
4. Click **Show users with certificate authentication**.
5. Click + in the **Management Users with Certificate Authentication** table.
6. In the **Management Users with Certificate Authentication > New User** section, perform the following steps:
   a. Select one of the following options from the **Interface to connect** drop box:
      - **WebUI**—Select this option to enable only the WebUI authentication and configure **Username**, **Role**, **Trusted CA certificate name**, and **Client certificate serial number**.
      - **CLI through SSH**—Select this option to enable only CLI through SSH and configure **Username**, **Role**, **Certificate**, and **Revocation checkpoint**.
      - **WebUI & CLI through SSH**—Select this option to enable both WebUI authentication and CLI through SSH and configure all the required parameters.

   The default username and password to login to the device using the CLI or user interface are admin and admins respectively.

   b. Click **Save Settings**.

**Enabling Console Block**

To enable console block:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > Admin**.
4. Under **Management User** select **Enable console block**. Disabling this option locks down all console ports such as micro USB and mini USB on the SD-WAN Gateways to enable high level security.
5. Click **Save Settings**.

**Configuring Management User Authentication Options**

The SD-WAN Gateway supports client certificate authentication for users accessing the user interface. (The default is for username and password authentication.) You can use client certificate authentication only or client certificate authentication with username and password (if certificate authentication fails, the user can log in with a configured username and password).

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > Admin > Admin Authentication Options** and perform the following steps:
   a. Select a default role.
   b. Select **Enable**.
   c. Select **MSCHAPv2**, if it is the desired authentication method.
   d. Select a server group.
   e. Select **Management telnet access** to enable management access through Telnet.
4. Click **Save Settings**.

### Configuring WebUI Authentication

To configure the WebUI authentication for management users, complete the following tasks:
1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > Admin > Admin Authentication Options**.
4. Under **WebUI Authentication**, make the following changes:
   a. Select **Username/password** if you do not want to use certificate authentication for WebUI management.
   b. Select **Webui HTTPS port (443) access**.
   c. Select **Client certificate** to use certificate authentication for WebUI management.
   d. Select the server certificate to be used for this service.
   e. Enter a value for Idle session timeout in minutes or seconds.
   f. Enter a value for re-authentication timeout in minutes or seconds.
5. Click **Save Settings**.

### Configuring SSH Authentication for CLI Access

The SD-WAN Gateway allows public key authentication of users accessing the device using SSH. (The default is for username and password authentication).

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > Admin > Admin Authentication Options**.
4. Under **SSH (Secure Shell) Authentication Method**, select **Client public key**. You can optionally select **User credentials** to use both username and password and public key authentication for SSH access.

### Enabling Ciphers and MAC Algorithms

You can configure SSH to enable or disable the following ciphers and MAC algorithms based on your preference:

- AES-CBC
- AES-CTR
- HMAC-SHA1
- MAC-SHA1-96

By default, all the algorithms are enabled. However, the SD-WAN Gateway allows you to enable or disable a specific cipher or the HMAC-SHA1-96 authentication algorithm using the WebUI.

To enable or disable a cipher encryption:
1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click System > Admin > Admin Authentication Options.
4. Under SSH (Secure Shell) Authentication Method, select AES-CBC, AES-CTR, or Both as the encryption option.
5. Click Save Settings.

To enable or disable HMAC-SHA1-96 authentication:
1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click System > Admin > Admin Authentication Options.
5. Click Save Settings.

Configuring Servers for Management User Authentication
You can use an external authentication server or the internal user database of SD-WAN Gateways to authenticate management users.

For more information on configuring authentication servers and server groups, refer to the following topics:
- Configuring RADIUS Authentication Server on page 94
- Configuring Other External Authentication Servers on page 96
- Configuring Server Groups on page 99

Configuring Switching Parameters
To avoid bridge loops between network nodes and to maintain a single active path between the network nodes, you may want to enable Spanning Tree for the VLANs.

To enable Spanning Tree and other switching parameters on Branch Gateways:
1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the SD-WAN Gateway or the device group that you want to configure.
3. Click System > Switching.
4. Expand Spanning Tree and configure the parameters described in the following table:
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning Tree</td>
<td>Enable Spanning Tree.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select one of the following Spanning Tree modes:</td>
</tr>
<tr>
<td></td>
<td>■ Rapid — RSTP takes advantage of point-to-point links and provides rapid convergence of the Spanning Tree. RSTP is enabled by default on all Branch Gateway devices. RSTP provides rapid convergence when interfaces are configured as either edge ports or point-to-point links.</td>
</tr>
<tr>
<td></td>
<td>■ Rapid-PVST — Rapid-PVST provides load-balancing of VLANs across multiple ports, resulting in optimal usage of network resources. Rapid-PVST also ensures interoperability with industry-accepted Rapid-PVST protocols. Rapid-PVST is disabled by default.</td>
</tr>
<tr>
<td>Forward Time</td>
<td>Specify the number of seconds that the port must spend in listening and learning states before forwarding packets. The value must be within a range of 4–30.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specify a keep alive interval for BPDUs within a range of 1-10.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Specify a waiting interval in seconds for the root bridge to receive a hello packet before changing the STP topology. This allows the protocol to determine if a port is currently unusable for forwarding. The value must be within a range of 6-40.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specify a value for priority to determine if a bridge must act as a root. The priority value must be within a range of 0-65536, with 0 being the highest priority.</td>
</tr>
<tr>
<td>LACP</td>
<td>Specify a value for Priority. When the LACP priority is configured, the LACP data units exchange their corresponding system identifier or priority along with their port key or priority. This information determines the LAG of a port. The LAG for a port is selected based on its keys. The port is placed in that LAG only when its system ID or key and system ID or key of its partner matches the other ports in the LAG (if the group has ports). LACP is disabled by default.</td>
</tr>
</tbody>
</table>

**Configuring AMON Receivers for SD-WAN Gateways**

You can configure Aruba Monitoring (AMON) receivers, such as Aruba ALE for SD-WAN Gateways to provide better monitoring and diagnostic capabilities. SD-WAN Gateways constantly feed the configured receivers with the AMON data which is real-time application data. This data can be interpreted and presented to the users in various ways for monitoring purposes.

To configure the AMON receivers on SD-WAN Gateways, complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway to configure.
3. Click **System > Aruba Monitoring (AMON)**.
4. Click + from the **AMON Dest** table to add an AMON receiver.
5. Select the AMON receiver type from the **Type** drop-down.
6. Enter the IP address of the AMON receiver in the **IPv4 address** field.
7. Click **Save Settings**.
Configuring VLANs

As a layer 2 switch, the Branch Gateway requires an external router to route traffic between VLANs. The Branch Gateway can also operate as a layer 3 switch that can route traffic between VLANs.

You can configure one or more physical ports on the Branch Gateway to be a member of a VLAN. Additionally, each wireless client association constitutes a connection to a virtual port on the Branch Gateway, with membership in a specified VLAN. You can place all authenticated wireless users into a single VLAN or into different VLANs, depending on your network requirements. You can also configure an IP address and netmask for a VLAN. The IP address is up when at least one physical port in the VLAN is up. The VLAN IP address can be used as a gateway by external devices; packets that are not destined for the Branch Gateway and directed to a VLAN IP address are forwarded according to the Branch Gateway’s IP routing table.

For the SD-WAN deployment, each Branch Gateway requires VLAN interfaces for WAN uplinks and LANs. Each VLAN must have a unique VLAN ID assigned to it. By default, the Branch Gateways are pre-configured with the VLAN 4094.

See the following topics for instructions on configuring VLANs:

- Configuring VLANs for WAN Interfaces on page 43
- Configuring VLANs for LAN Interfaces on page 44

Adding VLANs for SD-WAN Gateways

Complete the following tasks to add VLANs to the SD-WAN Gateway and configure the VLAN parameters:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click Interfaces > VLANs.
4. Click + from the VLANs table to add a new VLAN interface.
5. In the New VLAN window, specify the following parameters and save the changes:
   - VLAN name
   - VLAN ID/Range

Configuring VLANs for WAN Interfaces

To configure VLAN for WAN interfaces on a Branch Gateway or a VPN Concentrator, complete the following steps:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the device to configure.
3. Click Interfaces > VLANs.
4. Select a VLAN from the VLANs table.
5. Select the WAN-facing VLAN ID from the VLAN IDs table.
6. Under the IPv4 tab configure the following parameters:
   a. Select the Enable routing option.
   b. Select one of the following options from the IP assignment drop-down list.
      - Static
      - DHCP
      - PPPOE
c. Select the **NAT outside** check box to enable NAT only for the outbound traffic on public-facing egress VLAN interfaces. When this feature is enabled on an uplink VLAN interface, the source address is translated with the IP address of the VLAN interface to all the outbound traffic. Ensure that the NAT pool is configured for source NAT IP allocation. For more information see, [Configuring NAT Pools on page 32](#).  

7. Save the changes.

### Configuring VLANs for LAN Interfaces

To configure VLAN for LAN interfaces on a Branch Gateway, complete the following steps:  
1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device to configure.
3. Click **Interfaces > VLANs**.
4. Select a VLAN from the **VLANs** table.
5. Select the WAN-facing VLAN ID from the **VLAN IDs** table.
6. Under the **IPv4** tab configure the following parameters:
   a. Select the **Enable routing** option.
   b. Select **Static** from the **IP assignment** drop-down list. If you configure the VLANs at the group level, you can also choose **Dynamic DHCP Pool**. This option is not applicable for device level configuration.
   c. Enable **Relay to external** option.
   d. Add the IP address of the RADIUS server to which you want to relay the DHCP requests in the **DHCP helper** table.
   e. Under **Other option**, ensure to apply a AAA profile to the VLAN from the **AAA Profile** drop-down list. Alternately, you can assign a AAA profile to the VLAN interface from the **Apply Policies** tab under **Gateway Management > Security**. For more information, see [Assigning AAA profile to VLAN Interfaces for Role Assignment on page 102](#).
7. Save the changes.

### Configuring Other Parameters for VLAN

Complete the following tasks to configure the VLAN parameters:  
1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click **Interfaces > VLANs**.
4. To configure the parameters for a VLAN ID, select the required VLAN from the **VLANs** table. The **VLAN IDs** table is displayed.
5. From the **VLAN IDs** table, select a VLAN that you want to configure. The VLAN details are displayed in the following tabs:
   - **IPv4**
   - **Port Members**
6. To add or modify the port members associated to a VLAN ID, complete the following tasks:
   a. Select the **Port Members** tab.
   b. Click **Edit**. The **Available/Selected Ports** window is displayed.
   c. Select the required ports from the list of available ports and click **OK**.
7. Select the **IPv4** tab to configure the other VLAN parameters as described in [Table 14](#) based on your network requirements.
8. Save the changes.
<table>
<thead>
<tr>
<th>Table 14: VLAN IPv4 Tab Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>IP Assignment</td>
</tr>
<tr>
<td>Enable routing</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>MTU</td>
</tr>
<tr>
<td>Suppress ARP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>VLAN status</td>
</tr>
<tr>
<td>NAT inside</td>
</tr>
<tr>
<td>NAT outside</td>
</tr>
<tr>
<td>Admin state</td>
</tr>
<tr>
<td>Other Option</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Configuring Ports

Physical ports on the Branch Gateways are trusted and are usually connected to internal networks by default. The untrusted ports connect to third-party APs, public areas, or other networks. When you define a physical port as untrusted, the traffic passing through that port needs to go through a predefined ACL policy.

Ports can also be classified as trusted or untrusted based on the VLAN interface associations. For example, traffic on the port is trusted only if the VLAN interface associated to that port is trusted. When a port and its associated VLANs are untrusted, any incoming and outgoing traffic must pass through a predefined ACL. For example, you can configure an Ethernet port as an untrusted access port; assign VLANs and classify them as untrusted; and designate a policy through which VLAN traffic on this port must pass. This configuration is useful if your business provides wired user guest access and you want the guest user traffic to pass through an ACL and connect to captive portal.

LAN ports are configured as untrusted so that users are authenticated using AAA profile. WAN ports do not require users to authenticate and hence are configured as trusted ports.

You can set a range of VLANs as trusted or untrusted in trunk mode.

The following table lists the trusted/untrusted port and VLAN configuration and the impact on the network:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Broadcast multicast optimisation</strong></td>
<td>Select this option to enable controlled flooding of broadcast or multicast traffic without compromising the client connectivity.</td>
</tr>
<tr>
<td><strong>Bandwidth contract</strong></td>
<td>Select the bandwidth contract policy to be applied to the VLAN interface. The selected contract policy limits both broadcast and multicast traffic on the interface.</td>
</tr>
<tr>
<td><strong>Enable OSPF</strong></td>
<td>Select this to enable OSPF protocol on the interface and configure the following OSPF parameters:</td>
</tr>
<tr>
<td></td>
<td>- Area network (eg. 0.0.0.0)</td>
</tr>
<tr>
<td></td>
<td>- Authentication</td>
</tr>
<tr>
<td></td>
<td>- Password</td>
</tr>
<tr>
<td></td>
<td>- Retype password</td>
</tr>
<tr>
<td></td>
<td>- Cost [1-65535]</td>
</tr>
<tr>
<td></td>
<td>- Dead interval [1-65535]</td>
</tr>
<tr>
<td></td>
<td>- Hello interval [1-65535]</td>
</tr>
<tr>
<td></td>
<td>- Priority [0-255]</td>
</tr>
<tr>
<td></td>
<td>- Retransmit interval [1-65535]</td>
</tr>
<tr>
<td></td>
<td>- Transmit delay [1-65535]</td>
</tr>
<tr>
<td><strong>AAA profile</strong></td>
<td>Select a AAA profile to be applied to the VLAN interface. Alternately, you can assign AAA profiles to the VLAN interfaces from the <strong>Apply Policies</strong> tab under <strong>Gateway Management &gt; Security</strong>. For more information, see Assigning AAA profile to VLAN Interfaces for Role Assignment on page 102.</td>
</tr>
<tr>
<td><strong>ACL</strong></td>
<td>Select a routing policy to be applied to the VLAN interface. Alternately, you can assign routing policies to the VLAN interfaces from the <strong>Apply Policies</strong> tab under <strong>Gateway Management &gt; Security</strong>. For more information, see Applying Route ACLs for VLAN Interfaces on page 102.</td>
</tr>
</tbody>
</table>
**Table 15: Classifying Trusted and Untrusted Traffic**

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN</th>
<th>Traffic Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>Trusted</td>
<td>Trusted</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Untrusted</td>
<td>Untrusted</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Trusted</td>
<td>Untrusted</td>
</tr>
<tr>
<td>Trusted</td>
<td>Untrusted</td>
<td>Untrusted</td>
</tr>
</tbody>
</table>

**Adding Ports**

Complete the following tasks to add ports to the SD-WAN Gateway and configure the port parameters:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click **Interfaces > Ports**.
4. Click + from the **Ports** table to add a new port.
5. From the **New Port** window, select the required ports to be added to the **Ports** table and save the changes.

**Configuring Ports for WAN Interfaces**

To configure port for WAN interfaces at the device or group level, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click **Interfaces > Ports**.
4. Select a port from the **Ports** table. The port details are displayed.
5. Select the port type as **WAN**.
6. Select the **Trust** check box.
7. To apply a policy to the WAN interface, select one of the following options from the **Policy** drop-down list:
   - **Inbound and Outbound**—Select this option to apply a firewall policy for the incoming and outgoing traffic.
   - **Per-Session**—Select this option to apply a firewall policy for the session.
8. Select the port mode. You can set ports to either access mode or trunk mode.
9. To apply a policy to the VLAN traffic on access port, see **Applying Policies for VLANs on Access Ports on page 101**.
   - **Access**—By default, ports are set to access mode to carry traffic only for the VLAN to which they are assigned. For Access mode, select the VLAN and the **VLAN trust** checkbox. To apply a policy for the VLAN traffic on access port, see **Applying Policies for VLANs on Access Ports on page 101**.
   - **Trunk**—In trunk mode, a port can carry traffic for multiple VLANs. When the **Trunk** mode is selected, specify whether the port must carry traffic for all VLANs configured for the branch or for specific VLANs only. You can also configure the native VLAN for a port. To apply a policy for VLANs in trunk mode, see **Applying Policies for VLANs on Trunk Ports on page 101**.
9. Save the changes.
Configuring Ports for LAN Interfaces

To configure ports for LAN interfaces at the device or group level, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click **Interfaces > Ports**.
4. Select the port from the **Ports** table.
5. Select the port type as **LAN**.
6. Clear the **Trust** check box to set the port to **Untrusted**.
7. To apply a policy to the LAN interface, select one of the following options from the **Policy** drop-down list:
   - **Inbound and Outbound**—Select this option to apply a firewall policy of the incoming and outgoing traffic.
   - **Per-Session**—Select this option to apply a firewall policy for the session.
8. Select the port mode. You can set ports to either access mode or trunk mode.
9. **Access**—By default, ports are set to access mode to carry traffic only for the VLAN to which they are assigned. For Access mode, select the VLAN and the **VLAN trust** checkbox. To apply a policy for the VLAN traffic on access port, see Applying Policies for VLANs on Access Ports on page 101.
10. **Trunk**—In trunk mode, a port can carry traffic for multiple VLANs. When the **Trunk** mode is selected, specify whether the port must carry traffic for all VLANs configured for the branch or for specific VLANs only. You can also configure the native VLAN for a port. To apply a policy for VLANs in trunk mode, see Applying Policies for VLANs on Trunk Ports on page 101.

---

Ensure to apply a AAA profile to the VLANs that are assigned to the port. For more information, see Assigning AAA profile to VLAN Interfaces for Role Assignment on page 102.

9. Save the changes.

Configuring Other Parameters for Port

Complete the following tasks to configure the port parameters:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click **Interfaces > Ports**.
4. To configure the port parameters, select the required port from the **Ports** table. The port details are displayed.
5. Configure the parameters described in **Table 16** as per your network requirements.
6. Save the changes.

---

**Table 16: Port Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Options</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select the port type as WAN or LAN for WAN interface and LAN interface respectively.</td>
</tr>
<tr>
<td><strong>Admin state</strong></td>
<td>Select this option to set the user state of the port interface as admin.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Speed** | Select one of the following values (Mbps) for speed operation of the port:  
- 10  
- 100  
- 1000  
- auto |
| **Duplex** | Select one of the following values for duplex operation of the port:  
- auto  
- half  
- full |
| **PoE** | Enable this option to set the port interface as a PoE source. |
| **Trust** | Enable this option to configure the port as a trusted interface. |
| **Policy** | Select one of the following options from the drop-down list:  
- **inbound and Outbound**—Select this option to apply a firewall policy for the incoming and outgoing traffic.  
- **Per-Session**—Select this option to apply a firewall policy for the session. |
| **Mode** | Select the port mode. You can set ports to either access mode or trunk mode.  
- **Access**—By default, ports are set to access mode to carry traffic only for the VLAN to which they are assigned. For Access mode, select the VLAN and the **VLAN trust** checkbox. To apply a policy for the VLAN traffic on access port, see Applying Policies for VLANS on Access Ports on page 101.  
- **Trunk**—In trunk mode, a port can carry traffic for multiple VLANS. When the **Trunk** mode is selected, specify whether the port must carry traffic for all VLANS configured for the branch or for specific VLANS only. You can also configure the native VLAN and session firewall policy on a port. To apply a policy for VLANS in trunk mode, see Applying Policies for VLANS on Trunk Ports on page 101. |
| **VLAN** | Select the VLAN interfaces that you want to associate to the port. |
| **VLAN trust** | Enable this option to set the VLAN interface as trusted. |
| **VLAN policy** | The firewall policy that is applied to the trusted VLAN which is associated to the port. You can apply firewall policies only for trusted VLANS.  
For more information on applying VLAN policies, see Applying Policies on SD-WAN Gateway Interfaces on page 101. |
| **Description** | Optional text string to describe the port interface. |
| **Tunneled node** | Select this option to enable tunneled node capability for the port interface. By default, this is disabled. The tunneled node connects to one or more client devices at the edge of the network to establish a secure GRE tunnel. |
| **Jumbo MTU** | Select this option to enable Jumbo frame MTU configured on the interface. This setting is functional only if the Jumbo frame processing is enabled in the firewall policies. |
| **Advanced Options** |  
**NOTE:** The following advanced options appear only if you click the **Show advanced options** link below the **Ports** table. |
<p>| <strong>Port monitoring</strong> | Test |
| <strong>Spanning tree</strong> | Select this option to enable spanning tree protocol on the port. This is enabled by default. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning tree cost</td>
<td>Specify the spanning tree path cost of the port. The allowed range is 1-65535. The default value is 2000.</td>
</tr>
<tr>
<td>Spanning tree priority</td>
<td>Specify the spanning tree priority of the port. The allowed range is 0-255. The default value is 128.</td>
</tr>
<tr>
<td>Spanning tree port fast</td>
<td>Select this option to enable forwarding of traffic from the port. By default, this option is disabled.</td>
</tr>
<tr>
<td>Spanning tree point-to-point</td>
<td>Select this option to enable the port as a point-to-point link. By default, this option is disabled.</td>
</tr>
<tr>
<td>Spanning tree BPDU guard</td>
<td>Enable BPDU guard to protect the port from receiving STP BPDUs. However, the port can transmit STP BPDUs.</td>
</tr>
<tr>
<td>LLDP transmission</td>
<td>Enable this option if you want the port to transmit LLDP packets and configure the following LLDP transmissions parameters:</td>
</tr>
<tr>
<td></td>
<td>- Transmit interval—Specify the interval between LLDP TLV transmission in seconds. The supported range is 1-3600 and the default value is 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>- Transmit hold—Enter a value from 1-100. This value is multiplied by the transmit interval to determine the number of seconds to cache the learned LLDP information before it is cleared. If the transmit-hold value is at the default value of 4, and the transmit interval is at its default value of 30 seconds, then the learned LLDP information is cached for 4 x 30 seconds, or 120 seconds.</td>
</tr>
<tr>
<td></td>
<td>- Fast transmit interval—Set the LLDP fast transmission interval in seconds. The supported range is 1-3600. The default value is 1.</td>
</tr>
<tr>
<td></td>
<td>- Fast transmit hold—Enter a value from 1-100. This value is multiplied by the fast transmit interval to determine the number of seconds to cache the learned LLDP information before it is cleared. If the fast transmit-hold value is at the default value of 4, and the fast transmit interval is at its default value of 1 second, then the learned LLDP information is cached for 4 x 1 seconds, or 4 seconds.</td>
</tr>
<tr>
<td>LLDP reception</td>
<td>Select this option to enable the port to receive LLDP packets.</td>
</tr>
<tr>
<td>LLPD-MED</td>
<td>Select this option to enable LLDP-MED on the port.</td>
</tr>
<tr>
<td>Port security</td>
<td>Set or limit the number of MAC addresses learnt on the port. The allowed range is 1-16384.</td>
</tr>
</tbody>
</table>

**Configuring Uplinks**

Uplinks connect Branch Gateways to underlay networks. By default, both wired and cellular uplinks are set as active links with load balancing enabled on Branch Gateways. Branch Gateways support a total of five uplinks which include four wired uplinks and one cellular uplink.

**Uplink Load Balancing**

An uplink can be configured as an active uplink or as standby. The uplink load balancing feature supports both active and standby uplinks, for example, traffic can be load balanced across two wired uplinks, while the backup cellular uplink remains idle and used when a wired link fails. When a Branch Gateway has multiple active uplinks, uplink load balancing can modify the Internet Key Exchange (IKE) parameters for the Branch Gateway to create multiple IPsec tunnels, one on each uplink. When multiple uplinks and IPsec tunnels are up,
the layer 3 traffic can be load-balanced across these uplinks using specially created internal routing ACLs and next hop lists.

**WAN Bandwidth Optimization**

Data compression reduces the size of data frames that are transmitted over a network link. This in turn reduces the time required to transmit the frame across the network. IP payload compression is one of the key features of the WAN bandwidth optimization solution, which consists of the following elements:

- IP Payload Compression
- Traffic Management and Quality of Service (QoS)
- Caching

---

**NOTE**

WAN optimization through IP payload compression is not supported on 7205 controllers.

---

The Branch Gateway can send traffic to destinations other than the corporate headquarters on the same link; so, payload compression is enabled on the IPsec tunnel between the Branch Gateway and VPN Concentrator. Dynamic compression is used for the IP payload to achieve a high compression ratio. No compression is applied to data such as an embedded image file that might already be in a compressed format. Such data does not compress well, and may even increase in size.

**Bandwidth Estimation**

Though bandwidth allocations are provisioned on the Branch Gateways, the actual available bandwidth for connections in the internet circuits may be different. The Bandwidth Estimation feature helps in calculating the available bandwidth for the uplinks and reporting it as estimated bandwidth through the Monitoring pages. For more information, see [Network Health on page 132](#).

The available bandwidth is measured by synthesizing traffic and then coming up with an average over a period of time.

To configure the Bandwidth Estimation feature on an SD-WAN Gateway, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Go to **WAN > Uplink**. The **Uplink** configuration page opens.
4. Select the **Bandwidth Estimation** check box.
5. Save the changes.

**Configuring Uplink Interfaces**

To configure uplink interfaces:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Go to **WAN > Uplink**. The **Uplink** configuration page opens.
4. To enable **data compression**, select the **Compression** check box.
5. Select any one of the following load balancing modes:

- **Round Robin**—To equally distribute traffic among all active uplinks.
- **Session Count**—To balance traffic among the uplinks based on the number of sessions managed by each link, so that the load for each active uplink stays within 5% of the other active uplinks.
- **Uplink utilization**—To distribute traffic according to the utilization of active uplinks.

6. To enable the Bandwidth Estimation feature, select the **Bandwidth Estimation** check box.

7. To add an uplink, click + in the **Uplink VLANs** table and enter the following values to define an uplink VLAN for an uplink interface on the Branch Gateway:

- **Link Type**—Select any one of the following types of uplink:
  - MPLS—MPLS network
  - INET—Internet
  - LTE—4G cellular network
  - Metro-Ethernet—Ethernet network in a metropolitan area

- **Link Name**— Specify the name of the uplink.

- If you have selected LTE uplink as the uplink type, specify the connection type. By default, the USB connection type is selected.

- **Interface VLAN ID**—If you have selected MPLS, Internet, Metro-Ethernet, or LTE as the uplink type, specify the VLAN ID that you want to assign to the uplink.

The VLAN ID assignment is not configurable for 4G LTE USB uplink. By default, VLAN ID 4095 is assigned to the 4G LTE USB uplinks.

- **Operation state**—Use this checkbox to disable or re-enable the uplink. By default, uplinks are enabled.

- **Use only as backup link**—By default, all uplinks operate as active uplinks. If you want to use the uplink in the standby mode, set the uplink only as a backup uplink.

- **Weight**—If you have enabled session count based load balancing, specify a value for **Weight** within a range of 1–100. In an active-active uplink scenario, an uplink with a higher weight is assigned more session traffic than an uplink with a lower weight.

8. Click **Save Settings**.

### Enabling WAN Health Check Probes

The health check feature uses ping-probes to measure WAN availability and latency on selected uplinks. Based on the results of this health check information, the Branch Gateway can continue to use its primary uplink, or fail over to a backup link.

Latency is calculated based on the Round-Trip Time (RTT) of ping responses. You can define ping-probe settings for the primary WAN uplink.

To enable WAN health check and configure ping-probe settings:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Go to **WAN > Health Check**.
4. Select the **Health Check** check box and configure the parameters described in the following table:
Table 17: WAN Health Check Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Host IP/FQDN</td>
<td>IP address or FQDN of a remote host to which the Branch Gateway is connected. Central uses this IP address to check the connectivity of the Branch Gateway uplink.</td>
</tr>
<tr>
<td>Probe Mode</td>
<td>Probe modes to use for connectivity checks. You can set the probe mode to Ping or UDP.</td>
</tr>
<tr>
<td>Probe Interval (sec)</td>
<td>Probe interval in seconds for sending probes. To change the default interval of 10 seconds, enter a new value within a range of 10–3600.</td>
</tr>
<tr>
<td>Packet Burst Per Probe</td>
<td>Number of probes to be sent during the probe interval. To change the default value of 5 probes, enter a new value within a range of 1–16.</td>
</tr>
<tr>
<td>Probe Retries</td>
<td>The number of times the Branch Gateway must attempt to resend a probe. You can set any value withing a range of 1-255. The default value is 3.</td>
</tr>
</tbody>
</table>

If you have configured uplink interfaces and enabled health check, the dashboard on the Monitoring & Reports > Network Overview > Gateways page displays WAN availability, usage, and compression details.

Configuring WAN Interface Bandwidth Priorities

You can apply bandwidth for priorities per traffic class for a minimum bandwidth guarantee. This allows critical delay-sensitive applications such as voice and video to use more bandwidth and be scheduled with higher priority. Each interface can be associated with a scheduler profile that supports four queues with different priority levels. When you use session ACLs to define traffic policies on the Branch Gateway, you can use the scheduler profile to automatically associate different priority levels assigned by these policies to a scheduler profile queue.

You can assign a priority level and one of the following scheduler discipline types for each scheduler profile queue:

- **Strict priority**—The queue service is based exclusively on the priority of the queue, where the lower-priority queues are not serviced until the higher-priority queue is clear. With this option, the highest-level priority is guaranteed as much bandwidth as possible, but there can be phases where the second, third, and fourth priority queues may receive little or no bandwidth.

- **Deficit Round Robin (DRR) Weight**—The queue is assigned a percentage of available bandwidth.

You can define both strict priority and DRR Weight discipline types for a single scheduler profile.

Enabling WLAN Interface Bandwidth Priorities

To enable WLAN interface bandwidth priorities using WAN Scheduler:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Go to WAN > WAN Scheduler.
4. Click + below the WAN Scheduler Profiles table to define a new scheduler profile.
   a. In the Profile name field, enter a profile name.
   b. In the Priority fields, enter one or more 802.1p priority levels (0–7) for each queue type. Each of the seven priority levels must be supported by one of the four queues.
c. For each queue, click the **Scheduler Discipline** drop-down list and select the **Strict Priority** or **DRR Weight** discipline type. If you selected the **DRR Weight** option, you must enter the percentage of bandwidth that should be made available to the traffic in the selected queue. This field appears to the right of the **DRR Weight** option.

If you configure both strict priority and DRR weighted queues, the strict priority queues should be specified in a sequential order, followed by the DRR weighted queues. For example, if you want to specify two strict priority queues and two DRR weighted queues, configure queues 0 and 1 with the strict priority type, and then configure queues 2 and 3 with a DRR priority type. Do not alternate between strict priority and DRR weighted queues.

Table 18 displays sample CoS values for each queue of a WAN scheduler profile.

**Table 18: Sample CoS Values for WAN Scheduler profile**

<table>
<thead>
<tr>
<th>Queue</th>
<th>Priority</th>
<th>Scheduler Discipline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue 0</td>
<td>6 7</td>
<td>Strict Priority</td>
</tr>
<tr>
<td>Queue 1</td>
<td>4 5</td>
<td>Strict Priority</td>
</tr>
<tr>
<td>Queue 2</td>
<td>2 3</td>
<td>Strict Priority</td>
</tr>
<tr>
<td>Queue 3</td>
<td>0 1</td>
<td>Strict Priority</td>
</tr>
</tbody>
</table>

5. To assign the scheduler profile to a cellular or Gigabit Ethernet interface, click + in the **Assignments** area. Do one of the following:

a. Select the **Port** option and from the **Ports** drop-down list, select an interface. In the **Transmit Rate** field, enter the maximum transmit rate in Mbps for the selected interface.

b. Click the **Cellular** option. In the **Transmit Rate** field, enter the maximum transmit rate in Mbps for the selected interface.

6. Create a firewall session policy that assigns a priority level to an application or application group. For details, see [Creating a Firewall Policy for Network Services on page 83](#).

**Configuring Hub and Spoke VPN**

SD-WAN supports and recommends the hub and spoke VPN topology for Aruba branch office solutions. In this topology, one or more VPN routers (remote branches or spokes) communicate with a central VPN router (VPN Concentrator or hub) using a secured tunnel. The VPN Concentrator identifies the endpoints using the TPM certificates to establish the secured tunnel. This topology allows users at remote sites to access the main network and is best suited for networks where the traffic between the remote sites and the main network is predominant with minimal inter-site traffic.

Figure 4 illustrates the hub and spoke VPN topology in an SD-WAN network:
Whitelisting Branch Gateways on VPN Concentrator

In a hub and spoke VPN topology, where remote branches connect to the VPN Concentrator, newer branches are added in a staggered way. Each time a Branch Gateway is added, the branch information needs to be populated in the VPN Concentrator to whitelist the branch device. With large-scale deployments, this method is error prone and very cumbersome. The automatic whitelisting feature enables automating the process of whitelisting the branch devices to avoid extra configuration for each device at the headend.

For automatic whitelisting of Branch Gateways in the VPN Concentrator, the authentication code method is used. In this method, the whitelisting of the device is achieved through the authentication token.

Configuring Passcode Based Whitelisting

You must configure the same VPN peer authentication passcode on the Branch Gateway as well as the VPN Concentrator to whitelist the device in the database.

To whitelist a Branch Gateway automatically on a VPN Concentrator, complete the following steps:

1. From the app selector, click Gateway Management.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click VPN > Hub and Spoke.
4. Click Connect automatically to whitelisted Branch Gateways.
5. Enter the same passphrase that is configured on the Branch Gateway for automatic whitelisting in the **Passphrase** field.
6. Select an encryption method from the **Encryption** drop-down list.
7. For **Custom Cert** encryption method, enter the **CA cert** and **Server cert** details.
8. Select **Route** or **Session** from the **ACL type** drop-down list based on your requirement and then select the appropriate ACL.
9. If you have overlapping uplink IP address across branches, then enter the branch pool details.
10. Save the changes.

**Configuring MAC Address Based Whitelisting**

To whitelist a Branch Gateway manually on a VPN Concentrator, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click **VPN > Hub and Spoke**.
4. Click + from the **Branch Gateway Table** to add the MAC address of the Branch Gateways:
   - **MAC ADDRESS**—Enter the MAC address of the primary VPN Concentrator.
   - **ENCRYPTION**—Specify the encryption method. It can be **Factory Cert** or **Custom Cert**.
   - **CA CERT**—Select the CA certificate for the custom certificate.
   - **SERVER CERT**—Select the server certificate for the custom certificate.
5. Save the changes.

**Configuring VPN Tunnels on Branch Gateways**

You can configure the Branch Gateways to establish a VPN tunnel with the VPN Concentrator using one of the following methods:

- By configuring Auto-VPN to automatically establish a VPN tunnel with a VPN Concentrator by advertising the Branch Gateways.
- By configuring a VPN endpoint for the Branch Gateways to establish a VPN tunnel.

**Configuring Auto-VPN on Branch Gateways**

To configure Auto-VPN using branch advertisement, perform the following task on the Branch Gateways:

1. From the app selector, click **Gateway Management**.
2. Select a group in which the Branch Gateway is provisioned.
3. Click **VPN > Hub and Spoke**.
4. Click **Connect automatically to VPNC**.
5. Enter the same passphrase that is configured on the VPN Concentrator for automatic whitelisting in the **Passphrase** field.
6. (Optional) Enable the **Advertise branch subnets to hub** option and specify the branch VLANs of the subnets to be advertised in the **Advertise branch VLANs** field.
7. Save the changes.
Configuring VPN Endpoint for Branch Gateways

To configure a specific VPN endpoint for the Branch Gateways, perform the following tasks on the Branch Gateways:

1. From the app selector, click **Gateway Management**.
2. Select a group to which Branch Gateways are provisioned.
3. Click **VPN > Hub and Spoke**.
4. Click + from the **Hubs** table to add the following VPN Concentrator hub information:
   - **Primary VPNC**—Enter the MAC address of the primary VPN Concentrator.
   - **Backup VPNC**—(Optional) Enter the MAC address of the backup VPN Concentrator.
   - **IP Address**—Enter the IP address of the VPN Concentrator.
   - **Source VLAN**—Specify the source VLAN of the Branch Gateway if more than one IP address is configured for the same VPN Concentrator.
   - **Encryption**—Specify the encryption method. It can be **Factory Cert** or **Custom Cert**.
5. Save the changes.

Configuring IKE Policies

Branch Gateways support both IKEv1 and IKEv2 protocols to establish IPsec tunnels. Though both IKEv1 and IKEv2 support the same suite-B cryptographic algorithms, IKEv2 is a simpler, faster, and more reliable protocol than IKEv1.

This section covers the following topics:

- **Configuring IKEv1 Policies and Dynamic Maps**
- **Configuring IKEv2 Policies and Dynamic Maps**

Configuring IKEv1 Policies and Dynamic Maps

SD-WAN allows you to add or edit an existing IKEv1 policy or an IKEv1 dynamic map that can be used for an IPsec connection. Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. You can also define the authentication method and server addresses on the Branch Gateway.

The IKE policy selections, along with any preshared key, must be reflected in the VPN client configuration. When using a third-party VPN client, set the VPN configuration on clients to match the choices made above.

Use the following procedure to configure the authentication method, IKEv1 policies and dynamic IPsec maps on the Branch Gateway:

1. From the app selector, click **Gateway Management**.
2. Select a group to which Branch Gateways are provisioned.
3. Click **VPN > IKEv1**.
4. To configure the authentication method, enable the required option:
   - a. To enable L2TP, select **L2TP**.
   - b. To enable XAuth, select **XAuth**.
5. Select an authentication method for IKEv1 clients. Currently, supported methods include:
   - **PAP**
   - **EAP**
- CHAP
- MSCHAP
- MSCHAPv2

6. In the IKEv1 Policies table, click an existing policy to edit it, or click + to open the Add IKEv1 Policy section. Configure the required parameters as described in Table 19.

Table 19: IKEv1 Policy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Specify the priority number for this policy. Set the value to 1 for the configuration to take priority over the default setting.</td>
</tr>
<tr>
<td>Enable policy</td>
<td>Select the check box to enable the IKEv1 policy when it is saved.</td>
</tr>
<tr>
<td>Encryption</td>
<td>select one of the following encryption types:</td>
</tr>
<tr>
<td></td>
<td>• DES</td>
</tr>
<tr>
<td></td>
<td>• 3DES</td>
</tr>
<tr>
<td></td>
<td>• AES128</td>
</tr>
<tr>
<td></td>
<td>• AES192</td>
</tr>
<tr>
<td></td>
<td>• AES256</td>
</tr>
<tr>
<td>Hash algorithm</td>
<td>select one of the following hash types:</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td></td>
<td>• SHA</td>
</tr>
<tr>
<td></td>
<td>• SHA1-96</td>
</tr>
<tr>
<td></td>
<td>• SHA2-256-128</td>
</tr>
<tr>
<td></td>
<td>• SHA2-384-192</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select one of the following authentication types for the IKE rule:</td>
</tr>
<tr>
<td></td>
<td>• Pre-Share</td>
</tr>
<tr>
<td></td>
<td>• RSA (for clients using certificates)</td>
</tr>
<tr>
<td></td>
<td>• ECDSA-256 (for clients using certificates)</td>
</tr>
<tr>
<td></td>
<td>• ECDSA-384 (for clients using certificates)</td>
</tr>
<tr>
<td>Diffie-Hellman group</td>
<td>Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie–Hellman Group for the ISAKMP policy, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Group 1: 768-bit Diffie–Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>• Group 2: 1024-bit Diffie–Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>• Group 14: 2048-bit Diffie–Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>• Group 19: 256-bit random Diffie–Hellman ECP modulus group</td>
</tr>
<tr>
<td></td>
<td>• Group 20: 384-bit random Diffie–Hellman ECP modulus group</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Set the lifetime of the IKE security association in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds.</td>
</tr>
</tbody>
</table>

7. In IKEv1 IPSec Dynamic Maps, click an existing dynamic map to edit it or click + to open the Add IKEv1 Dynamic Map section. Configure the required parameters as described in Table 20.
Table 20: IKEv1 Dynamic IPsec Map Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Set the priority level for the IPsec map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next highest-priority map until a match is found.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the dynamic map.</td>
</tr>
<tr>
<td>Dynamic map</td>
<td>Select the check box to enable the dynamic map. This is enabled by default.</td>
</tr>
<tr>
<td>PFS group</td>
<td>(Optional) Configure PFS settings for the dynamic peer by assigning a Diffie-Hellman prime modulus group. PFS group provides an additional level of security by ensuring that the IPsec SA key was not derived from any other key, and therefore, cannot be compromised if another key is broken. Select one of the following groups: Group 1: 768-bit Diffie–Hellman prime modulus group Group 2: 1024-bit Diffie–Hellman prime modulus group Group 14: 2048-bit Diffie–Hellman prime modulus group Group 19: 256-bit random Diffie–Hellman ECP modulus group Group 20: 384-bit random Diffie–Hellman ECP modulus group</td>
</tr>
<tr>
<td>Transforms</td>
<td>Click + to open the New Transform section. 1. To add an existing transform, select Add existing transform 2. Select a transform from the list. 3. Click Save Settings. 4. To add a new transform, select Add new transform. 5. From the Encryption drop-down list, select one of the following encryption types: DES 3DES AES128 AES192 AES256 6. From the Hash algorithm drop-down list, select one of the following hash types: MD5 SHA SHA1-96 SHA2-256-128 SHA2-384-192 7. Click Save Settings.</td>
</tr>
<tr>
<td>Lifetime(seconds)</td>
<td>Set the lifetime of the security association for the dynamic peer in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds.</td>
</tr>
<tr>
<td>Lifetime(kilobytes)</td>
<td>Set the lifetime of the security association for the dynamic peer in kilobytes</td>
</tr>
</tbody>
</table>

8. Save the changes.

Configuring IKEv2 Policies and Dynamic Maps

Use the following procedure to configure the EAP passthrough, IKEv2 policies and dynamic IPsec maps on the Branch Gateway:

1. From the app selector, click Gateway Management.
2. Select a group to which Branch Gateways are provisioned.
3. Click **VPN >IKEv2**.

4. In **EAP passthrough**, select the EAP passthrough for IKEv2 clients. The currently supported methods include:
   - EAP-TLS
   - EAP-PEAP
   - EAP-MSCHAPv2

5. In the **IKEv2 Policies** table, click an existing policy to edit it, or click + to open the **Add IKEv2 Policy** section. Configure the required parameters as described in Table 21.

### Table 21: IKEv2 Policy Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Specify the priority number for this policy. Set the value to 1 for the configuration to take priority over the default setting.</td>
</tr>
<tr>
<td>Enable policy</td>
<td>Select the check box to enable the IKEv1 policy when it is saved.</td>
</tr>
<tr>
<td>Encryption</td>
<td>select one of the following encryption types:</td>
</tr>
<tr>
<td></td>
<td>- DES</td>
</tr>
<tr>
<td></td>
<td>- 3DES</td>
</tr>
<tr>
<td></td>
<td>- AES128</td>
</tr>
<tr>
<td></td>
<td>- AES192</td>
</tr>
<tr>
<td></td>
<td>- AES256</td>
</tr>
<tr>
<td>Hash algorithm</td>
<td>select one of the following hash types:</td>
</tr>
<tr>
<td></td>
<td>- MD5</td>
</tr>
<tr>
<td></td>
<td>- SHA</td>
</tr>
<tr>
<td></td>
<td>- SHA1-96</td>
</tr>
<tr>
<td></td>
<td>- SHA2-256-128</td>
</tr>
<tr>
<td></td>
<td>- SHA2-384-192</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select one of the following authentication types for the IKE rule:</td>
</tr>
<tr>
<td></td>
<td>- Pre-Share (for IKEv1 clients using pre-shared keys)</td>
</tr>
<tr>
<td></td>
<td>- RSA (for clients using certificates)</td>
</tr>
<tr>
<td></td>
<td>- ECDSA-256 (for clients using certificates)</td>
</tr>
<tr>
<td></td>
<td>- ECDSA-384 (for clients using certificates)</td>
</tr>
<tr>
<td>Diffie-Hellman group</td>
<td>Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie-Hellman Group for the ISAKMP policy, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Group 1: 768-bit Diffie-Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>- Group 2: 1024-bit Diffie-Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>- Group 14: 2048-bit Diffie-Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>- Group 19: 256-bit random Diffie-Hellman ECP modulus group</td>
</tr>
<tr>
<td></td>
<td>- Group 20: 384-bit random Diffie-Hellman ECP modulus group</td>
</tr>
<tr>
<td>PRF</td>
<td>This algorithm is an HMAC function used to hash certain values during the key exchange. Set this to one of the following values based on the value selected for Hash algorithm:</td>
</tr>
<tr>
<td></td>
<td>- PRF-HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>- PRF-HMAC-SHA1</td>
</tr>
<tr>
<td></td>
<td>- PRF-HMAC-SHA256</td>
</tr>
<tr>
<td></td>
<td>- PRF-HMAC-SHA384</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Set the lifetime of the IKE security association in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds.</td>
</tr>
</tbody>
</table>
6. In **IKEv2 IPSec Dynamic Maps**, click an existing dynamic map to edit it or click + to open the **Add IKEv2 Dynamic Map** section. Configure the required parameters as described in [Table 22](#).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Set the priority level for the IPSec map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next highest-priority map until a match is found.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the dynamic map.</td>
</tr>
<tr>
<td>Dynamic map</td>
<td>Select the check box to enable the dynamic map. This is enabled by default.</td>
</tr>
</tbody>
</table>
| PFS group     | (Optional) Configure PFS settings for the dynamic peer by assigning a Diffie-Hellman prime modulus group. PFS group provides an additional level of security by ensuring that the IPSec SA key was not derived from any other key, and therefore, cannot be compromised if another key is broken. Select one of the following groups:  
|               | - Group 1: 768-bit Diffie-Hellman prime modulus group  
|               | - Group 2: 1024-bit Diffie-Hellman prime modulus group  
|               | - Group 14: 2048-bit Diffie-Hellman prime modulus group  
|               | - Group 19: 256-bit random Diffie-Hellman ECP modulus group  
|               | - Group 20: 384-bit random Diffie-Hellman ECP modulus group  
| Transforms    | Click + to open the **New Transform** section.   
|               | 1. To add an existing transform, select **Add existing transform**  
|               | 2. Select a transform from the list and save the changes.  
|               | 3. To add a new transform, select **Add new transform**.  
|               | 4. From the **Encryption** drop-down list, select one of the following encryption types:   
|               | - DES  
|               | - 3DES  
|               | - AES128  
|               | - AES192  
|               | - AES256  
|               | 5. From the **Hash** algorithm drop-down list, select one of the following hash types:   
|               | - MD5  
|               | - SHA  
|               | - SHA1-96  
|               | - SHA2-256-128  
|               | - SHA2-384-192  
|               | 6. Click **Save Settings**.  
| Lifetime(seconds) | Set the lifetime of the security association for the dynamic peer in seconds. The supported range is 300-86400 seconds. The default value is 7200 seconds. |
| Lifetime(kilobytes) | Set the lifetime of the security association for the dynamic peer in kilobytes |

7. Save the changes.

### Configuring Site-to-Site VPN

A site-to-site VPN allows the branch sites to establish secure connections with one another over a public network, for example, the internet. A site-to-site VPN allows users from different locations to access network resources hosted within the corporate network.
Figure 5 illustrates the site-to-site VPN topology in which a tunnel connects Network A to Network B across the internet.

**Figure 5  Site-to-Site VPN Configuration Components**

As shown in Figure 5, the following parameters must be configured to set up a site-to-site VPN tunnel on a Branch Gateway A:

- The source network (Network A)
- The destination network (Network B)
- The VLAN on which Branch Gateway A's interface to the layer 3 network is located (Interface A in Figure 5)
- The peer gateway, which is the IP address of Branch Gateway B's interface to the layer 3 network (Interface B in Figure 5).

For the site-to-site VPN, you must configure VPN settings on Branch Gateways deployed at both the local and remote sites.

Site-to-site VPNs allow sites in different locations to securely communicate with one another over a layer 3 network such as the internet. You can use a Branch Gateway instead of a VPN Concentrator to connect the sites.

Branch Gateway supports the following IKE SA authentication methods for site-to-site VPNs:

- Pre-shared key—The same IKE shared secret must be configured on both the local and remote sites. The MAC address of the VPN Concentrator should be added as the peer MAC address in the Branch Gateway to establish the IKE/IPsec tunnel with the VPN Concentrator.
- Suite-B cryptographic algorithms—Branch Gateways support Suite-B cryptographic algorithms when the Advanced Cryptography license is installed.
- Digital certificates—You can configure an RSA or ECDSA server certificate and a CA certificate for each site-to-site VPN IPsec map configuration. If you use certificate-based authentication, the peer must be identified by its certificate subject name, distinguished name (for deployments using IKEv2), or peer's IP address (for IKEv1).

**Configuring IPsec Map for Site-to-Site VPNs**

To configure IPsec map parameters for a site-to-site VPN, complete the following steps:

1. From the app selector, click Gateway Management.
2. Select a group to which Branch Gateways are provisioned.
3. Click VPN > Site to Site.
4. In the IPsec Maps section, click + to open the Create New Ipsec section.
5. Configure the required parameters as described in Table 23.
6. Save the changes.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the VPN connection in the field.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the check box.</td>
</tr>
<tr>
<td>Priority</td>
<td>In the <strong>Priority</strong> field, enter a priority level for the IPsec map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next highest-priority map until a match is found.</td>
</tr>
<tr>
<td>Source network type</td>
<td>Select one of the following options to identify the source, the local VPN network connected to the Branch Gateway:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>IP Address</strong>—The source is identified by an IP address.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Source network</strong>—If you selected <strong>IP Address</strong>, you must enter the IP address of the source network.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Source subnet mask</strong>—Enter the netmask for the source network.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>VLAN</strong>—The source is identified by a VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>VLAN</strong>—If you selected the VLAN ID for the source network type, you must specify the VLAN ID from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Any</strong>—The source can be any network.</td>
</tr>
<tr>
<td>Destination network type</td>
<td>Select one of the following options to identify the destination, the remote network to which the local network communicates:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>IP Address</strong>—The destination is identified by an IP address.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Destination network</strong>—If you selected <strong>IP Address</strong>, you must enter the IP address of the destination network.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Destination subnet mask</strong>—Enter the netmask for the destination network.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Any</strong>—The destination can be any network.</td>
</tr>
<tr>
<td>SA lifetime (seconds)</td>
<td>The specified value (in seconds) defines the lifetime of the IPsec security association. The default value is 7200 seconds. The allowed range is 300-86,400 seconds.</td>
</tr>
<tr>
<td>SA lifetime (kb)</td>
<td>The specified value (in kilobytes) defines the lifetime of the IPsec security association. The allowed range is 1000-1,000,000,000 kilobytes.</td>
</tr>
<tr>
<td>IKE version</td>
<td>Select <strong>v1</strong> to configure the VPN for IKEv1, or <strong>v2</strong> for IKEv2. For more information on configuring an IKE policy, see Configuring IKE Policies</td>
</tr>
<tr>
<td>IKE policy</td>
<td>(Optional) Click the <strong>Policies</strong> drop-down list and select a predefined or custom IKE policy to apply to the IPsec map.</td>
</tr>
<tr>
<td>IP compression</td>
<td>This option appears only if you selected <strong>v2</strong> as <strong>IKE version</strong>. IKEv2 site-to-site VPNs between VPN Concentrators and Branch Gateways support traffic compression between those devices. Set <strong>IP compression</strong> to <strong>Enabled</strong> to enable compression for traffic in the site-to-site tunnel. Enabling this feature reduces the size of data frames transmitted over a site-to-site VPN between 7200 Series or 7000 Series controllers using IKEv2 authentication. IP compression can reduce the time required to transmit the frame across the network. When this hardware-based compression feature is enabled, the quality of unencrypted traffic (such as Lync or Voice traffic) is not compromised by increased latency or decreased throughput. IP compression is disabled by default. <strong>NOTE:</strong> This feature is only supported in an IPv4 network using IKEv2. This feature cannot be enabled on a 7205controller or on a site-to-site VPN that is established using IKEv1.</td>
</tr>
</tbody>
</table>
Table 23: IPSec Map Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factory certificate authentication</td>
<td>Select the check box to enable the Factory certificate authentication.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is applicable only if you selected v2 as IKE version.</td>
</tr>
<tr>
<td>PFS</td>
<td>If you enable PFS mode, new session keys are not derived from previously</td>
</tr>
<tr>
<td></td>
<td>used session keys. Therefore, if a key is compromised, that compromised key</td>
</tr>
<tr>
<td></td>
<td>does not affect any previous session keys. PFS mode is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>To enable this feature, click the PFS drop-down list and select one of the</td>
</tr>
<tr>
<td></td>
<td>following PFS modes:</td>
</tr>
<tr>
<td></td>
<td>* group1—768-bit Diffie–Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>* group2—1024-bit Diffie–Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>* group 14—2048-bit Diffie–Hellman prime modulus group</td>
</tr>
<tr>
<td></td>
<td>* group19—256-bit random Diffie–Hellman ECP modulus group</td>
</tr>
<tr>
<td></td>
<td>* group20—384-bit random Diffie–Hellman ECP modulus group</td>
</tr>
<tr>
<td>Inbound Route ACL</td>
<td>Select the inbound route ACL from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is applicable only if you selected v2 as IKE version.</td>
</tr>
<tr>
<td>Pre-connect</td>
<td>Select the Pre-connect check box to establish the VPN connection, even if</td>
</tr>
<tr>
<td></td>
<td>there is no traffic being sent from the local network. If you do not select</td>
</tr>
<tr>
<td></td>
<td>this, the VPN connection is established only when traffic is sent from the</td>
</tr>
<tr>
<td></td>
<td>local network to the remote network.</td>
</tr>
<tr>
<td>Trusted tunnel</td>
<td>Select Trusted Tunnel if the traffic between the networks is trusted.</td>
</tr>
<tr>
<td></td>
<td>If you do not select this, then the traffic between the networks is</td>
</tr>
<tr>
<td></td>
<td>untrusted.</td>
</tr>
<tr>
<td>Enforce NATT</td>
<td>Select the check box to enforce UDP 4500 for IKE and IPSec. This option is</td>
</tr>
<tr>
<td></td>
<td>disabled by default.</td>
</tr>
<tr>
<td>Force tunnel mode</td>
<td>Select the check box to enforce tunnel mode. This option is disabled by</td>
</tr>
<tr>
<td></td>
<td>default.</td>
</tr>
<tr>
<td>Transforms</td>
<td>Add one or more transform sets to be used by the IPSec map. Click + and</td>
</tr>
<tr>
<td></td>
<td>select an existing transform set or create a new one. Then click Apply to</td>
</tr>
<tr>
<td></td>
<td>add that transform set to the IPSec map.</td>
</tr>
<tr>
<td>Remote peer addressing</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>* Static—For site-to-site VPNs with peers that have static IP address.</td>
</tr>
<tr>
<td></td>
<td>* Dynamic—For site-to-site VPNs with dynamically addressed peers.</td>
</tr>
<tr>
<td>Peer gateway type</td>
<td>The peer gateway type can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>* IP address—If you selected this option, then specify an IP address in</td>
</tr>
<tr>
<td></td>
<td>the Peer gateway IPv4 field.</td>
</tr>
<tr>
<td></td>
<td>* FQDN—If you selected this option then specify a value in the Destination</td>
</tr>
<tr>
<td></td>
<td>gateway FQDN field.</td>
</tr>
<tr>
<td>Destination gateway</td>
<td>This field is applicable only if you selected Dynamic in the Remote peer</td>
</tr>
<tr>
<td></td>
<td>addressing field. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>* Initiator—Select this if the dynamically addressed switch is the initiator</td>
</tr>
<tr>
<td></td>
<td>of IKE Aggressive-mode for site-to-site VPNs</td>
</tr>
<tr>
<td></td>
<td>* Responder—Select this option if the dynamically addressed switch is</td>
</tr>
<tr>
<td></td>
<td>the responder for IKE Aggressive-mode.</td>
</tr>
<tr>
<td>Source FQDN</td>
<td>Enter an FQDN for the Branch Gateway if the Branch Gateway is defined as a</td>
</tr>
<tr>
<td></td>
<td>dynamically addressed responder,</td>
</tr>
<tr>
<td></td>
<td>* All Peers Select this option to make the Branch Gateway a responder for</td>
</tr>
<tr>
<td></td>
<td>all VPN peers.</td>
</tr>
<tr>
<td></td>
<td>* Per Peer ID Select this option to make the Branch Gateway a responder</td>
</tr>
<tr>
<td></td>
<td>for one specific initiator. Specify the FQDN id of the specific initiator to</td>
</tr>
</tbody>
</table>
### Table 23: IPsec Map Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink VLAN</td>
<td>Select the VLAN containing the interface of the Branch Gateway that connects to the layer 3 network. This determines the source IP address used to initiate IKE. If you selected 0 or None, the default is the VLAN of the Branch Gateway's IP address. <strong>NOTE:</strong> This field is not applicable if you have enabled Load balance.</td>
</tr>
</tbody>
</table>
| Authentication method | Select one of the following authentication options:  
  - **PSK**—Select this option for PSK authentication:  
    - **Representation type**—Select either **Text-based** or **Hex-based**.  
    - **IKE shared secret**—Enter a shared secret value. This authentication type is generally required in IPsec maps for a VPN with dynamically addressed peers, but can also be used for a static site-to-site VPN.  
    - **Retype shared secret**—Retype the shared secret value.  
  - **Certificate**—Select this option for certificate authentication:  
    - **Server certificate**—For certificate authentication, select the server certificates previously imported into the Branch Gateway  
      - **CA certificate**— select the CA certificates previously imported into the Branch Gateway  
      - **Peer certificate subject name**—Enter the Peer certificate subject name.  

---

**Enabling Dead Peer Detection**

DPD is enabled by default on the Branch Gateway for site-to-site VPNs. DPD, as described in RFC 3706, uses IPsec traffic patterns to minimize the number of IKE messages required to determine the liveliness of an IKE peer.

After a dead peer is detected, the Branch Gateway tears down the IPsec session. When the network path or other failure condition has been corrected, a new IPsec session is automatically re-established.

**Configuring Dead Peer Detection Parameters**

Use the following procedures to enable Dead Peer Detection:

1. From the app selector, click **Gateway Management**.
2. Select a group to which Branch Gateways are provisioned.
3. Click **VPN > DPD**.
4. Click **DPD**.
5. Enter the idle timeout, retry timeout, and retry attempts in the respective fields.
6. Save the changes.

**Configuring Site-to-Site VPN with GRE Tunnel**

Site-to-site tunnel with GRE can be used to setup connections between Branch Gateways and their Enterprise headend. In this topology the IPsec traffic is encapsulated and routed through a GRE tunnel to the headend gateway. The headend gateway can even be a non-Aruba device.

To set up a site-to-site VPN with GRE tunnel, perform the following tasks:

1. Configure a site-to-site VPN—For more information, see [Configuring Site-to-Site VPN](#).
2. Configure GRE tunnel—For more information, see Configuring GRE Tunnels.
3. Route the IPsec traffic into the GRE tunnel—For more information, see Directing Traffic into the GRE Tunnel.

Configuring GRE Tunnels

The headend gateway supports GRE tunnels between Branch Gateways and other network devices that support GRE tunnels.

This section contains the following information:
- Layer 2 GRE Tunnels
- Layer 3 GRE Tunnels on page 66
- Configuring a Layer 2 GRE Tunnel on page 66
- Configuring a Layer 3 GRE Tunnel on page 67
- Configuring Tunnel Keepalives on page 68
- GRE Tunnel Groups on page 69

Layer 2 GRE Tunnels

Layer 2 GRE tunnels allow you to have the same VLAN in multiple locations (separated by a layer 3 network) and be connected. The forwarding method for a layer 2 GRE tunnel is bridging.

However, the drawback of using layer 2 GRE tunnels is that all broadcasts are flooded through the tunnel, adding traffic load to the network and the Branch Gateway.

Layer 3 GRE Tunnels

The benefit of layer 3 GRE tunnels is that broadcasts are not flooded through the tunnel, so there is less wasted bandwidth and less load on the Branch Gateway. The forwarding method for a layer 3 GRE tunnel is routing.

Configuring a Layer 2 GRE Tunnel

To configure a layer 2 GRE tunnel for a source Branch Gateway and destination Branch Gateway:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the group or device for which you want to configure a layer 2 GRE tunnel.
3. Click + from the GRE Tunnel table to add a GRE tunnel. The Add GRE Tunnel section is displayed.
4. Select the IP version as IPv4.
5. Specify a tunnel ID in the Tunnel ID field.
6. Select the Mode as L2.
7. Specify the layer 2 protocol to be used on the tunnel in the Protocol field.
8. In the Vlans field, specify the VLAN IDs of all the interfaces from which the traffic to be encapsulated originate.
9. To enable OpenFlow on the tunnel, select the Enable check box.
10. To make the tunnel interface as trusted, select the Trusted check box.
11. Specify the MTU size for the tunnel interface in the MTU field.
12. Select one of the following options as the local endpoint of the tunnel from the **Tunnel Source** drop-down list based on your requirements:
   - **loopback**—Select this option to set the loopback IP as your tunnel source.
   - **ipaddr**—Select this option if you have a specific IP address as the tunnel source and specify the IP address in the **IP address** field.
   - **system-ip**—Select this option if your tunnel source is the IP address of the SD-WAN Gateway being configured.
   - **vlan**—Select this option if your tunnel source is a specific VLAN interface and specify the VLAN ID in the **VLAN** field.

13. Specify the destination IP address of the tunnel in the **Tunnel destination** field.

14. To enable tunnel keepalives, select **Enable keepalive** and configure the following Keepalive options:
   a. Specify a value for **Heartbeat interval (secs)**.
      The default value is 10 seconds.
   b. Specify a value for **Heartbeat retries**.
      The default value is 3 retries.
      For more information on tunnel keepalive feature, see Configuring Tunnel Keepalives on page 68.

15. Save the changes

### Configuring a Layer 3 GRE Tunnel

To configure a layer 3 GRE tunnel for a source Branch Gateway and destination Branch Gateway:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or device for which you want to configure a layer 3 GRE tunnel.
3. Click + from the **GRE Tunnel** table to add a GRE tunnel. The **Add GRE Tunnel** section is displayed.
4. Select the **IP version** as **IPv4**.
5. Specify a tunnel ID in the **Tunnel ID** field.
6. Select the **Mode** as **L3**.
7. Select the **IPv4 address type** as one of the following options based on your requirements:
   - **Dynamic**—Select this option if you are configuring the tunnel ID for a device group. Then, select the required tunnel pool from the **Dynamic IP address pool** drop-down list. For more information on creating a tunnel pool, see Configuring Tunnel Pools for SD-WAN Gateways on page 33.
   - **Static**—Select this option if you are configuring the tunnel ID for a specific Branch Gateway. Then, enter the tunnel IP and the IP mask in the **IP address** and **IP mask** fields, respectively.
8. To enable OpenFlow on the tunnel, select the **Enable** check box.
9. To make the tunnel interface as trusted, select the **Trusted** check box.
10. Specify the MTU size for the tunnel interface in the **MTU** field.
11. Select one of the following options as the local end point of the tunnel from the **Tunnel Source** drop-down list based on your requirements:
   - **loopback**—Select this option to set the loopback IP as your tunnel source.
   - **ipaddr**—Select this option if you have a specific IP address as the tunnel source and specify the IP address in the **IP address** field.
   - **system-ip**—Select this option if your tunnel source is the IP address of the SD-WAN Gateway being configured.
- **vlan**—Select this option if your tunnel source is a specific VLAN interface and specify the VLAN ID in the VLAN field.

12. Specify the destination IP address of the tunnel in the **Tunnel destination** field.

13. Select a route ACL name from the **Route ACL name** drop-down list to attach a route ACL to the inbound traffic on the L3 GRE tunnel interface.

14. To enable tunnel keepalives, select **Enable keepalive** and configure the following Keepalive options:
   a. (Optional) To interoperate with Cisco network devices, select the **Cisco compatible** check box.
   b. Specify a value for **Heartbeat interval (secs)**.
      The default value is 10 seconds.
   c. Specify a value for **Heartbeat retries**.
      The default value is 3 retries.

For more information on tunnel keepalive feature, see section on Configuring Tunnel Keepalives on page 68.

15. To enable OSPF on the tunnel, select **Enable OSPF** and configure the following options:

   - **Area network (eg. 0.0.0.0)**—Specify the IP address of the OSPF.
   - **Authentication**—Select this option for enabling OSPF authentication mode for MD5 and then configure the following authentication details:
     - **Message-digest key [1-255]**—Specify a key identification to enable OSPF MD5 authentication.
     - **Password**—Enter a character string password for OSPF.
     - **Retype password**—Retype the password for confirmation.
   - **Cost [1-65535]**—Specify the cost associated with the OSPF traffic on the tunnel interface. The default value is 1.
   - **Dead interval [1-65535]**—Specify the time interval in seconds after which a router is declared dead if hello packets are not received. This timer gets set or reset whenever a hello packet is received from the router. After the interval elapses, the neighboring routers declare the router as dead. The default value is 40.
   - **Hello interval [1-65535]**—Specify the time interval between the hello packets to be sent on the interface. The default value is 10.
   - **Priority [0-255]**—Specify the priority of the interface to determine the default router. The default value is 1.
   - **Retransmit interval [1-65535]**—Specify the retransmit interval time for link state advertisements. The default value is 5.
   - **Transmit delay [1-65535]**—Specify the delay time allowed for retransmitting link state update packets on the tunnel interface. The default value is 1.

16. Save the changes.

### Configuring Tunnel Keepalives

The headend gateway determines the status of a GRE tunnel by sending periodic keepalive frames on the layer 2 or layer 3 GRE tunnel. When you enable tunnel keepalives, the tunnel is considered down when the keepalives fail repeatedly.

If you configure a firewall policy rule to redirect traffic to the tunnel, traffic is not forwarded to the tunnel until it is up. When the tunnel comes up or goes down, an SNMP trap and logging message is generated. The remote endpoint of the tunnel does not need to support the keepalive mechanism.
The headend gateway sends keepalive frames at 60-second intervals by default and retries keepalives up to three times before the tunnel is considered down. You can change the default values of the intervals:

- For the **interval**, specify a value between 1 and 86400 seconds.
- For the **retries**, specify a value between 0 and 1024.
- To interoperate with Cisco network devices, select the **Cisco compatible** check box. This option is applicable only for layer 3 GRE tunnels.

To configure keepalives (Heartbeats), complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device for which you want to configure keepalives.
3. To enable tunnel keepalives, select **Enable keepalive** and configure the following Keepalive options.
   a. (Optional) To interoperate with Cisco network devices, select the **Cisco compatible** check box. This option is not applicable for layer 2 GRE tunnels.
   b. Specify a value for **Heartbeat interval (secs)**.
      The default value is 10 seconds.
   c. Specify a value for **Heartbeat retries**.
      The default value is 3 retries.
4. Click **Save Settings**.

**GRE Tunnel Groups**

Branch Gateways support redundancy of GRE tunnels for both layer 2 and layer 3 GRE tunnels. This feature enables automatic redirection of the user traffic to a standby tunnel when the primary tunnel goes down.

A tunnel group is identified by a name or number. You can add multiple tunnels to a tunnel group. The order of the tunnels defined in the tunnel-group configuration specifies their standby precedence. The first member of the tunnel-group is the **primary tunnel**.

A GRE tunnel group combines two tunnels created on a Branch Gateway, where one tunnel is active and the other tunnel is the standby. Traffic forwarding can occur on the active tunnel, and the standby tunnel can become active once the active tunnel is down. When the first tunnel fails, the second tunnel carries the traffic. The third tunnel in the tunnel-group takes over if the second tunnel also fails. In the meantime, if the first tunnel comes up, it becomes the most eligible standby tunnel.

You can also enable or disable preemption as part of the tunnel-group configuration. Preemption is enabled by default. This **preemptive-failover** option automatically redirects the traffic whenever it detects an active tunnel with a higher precedence in the tunnel group. When preemption is disabled, the traffic gets redirected to a higher precedence tunnel only when the tunnel carrying the traffic fails.

When creating a tunnel group, keep in mind the following points:

- When a tunnel is added to the tunnel group, the tunnel is used for data traffic only if it is the active tunnel in the group.
- Standby tunnels do not carry any data traffic. However, all tunnels in the group continue to send and receive keepalive packets.
- Only one type of tunnel can be placed into a tunnel group—either layer 2 or layer 3. That is, you cannot have a tunnel group consisting of both layer 2 and layer 3 tunnels.
- The default value of tunnel group type is layer 3.
- All tunnels in a layer 2 tunnel group must be tunneling the same VLAN.
- A layer 2 tunnel can only be part of one tunnel group.
The Branch Gateway layer 2 tunnel-group is not interoperable with other vendors. You must set up layer 2 tunnel groups between Aruba devices only.

**Configuring Tunnel Groups**

To configure a layer 2 or layer 3 GRE tunnel group, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or device for which you want to configure a tunnel group.
3. Click + in the **Tunnel Group** table.
4. Specify a name for the tunnel group in the **Tunnel Group Name** field.
5. In the **Tunnel Group Members** text box, click + to add one or more tunnel IDs.
6. Select the IDs and click **OK**.
7. To enable preemption, select the **Enable Preemptive-Failover Mode** check box. This option is enabled by default.
8. In the **Mode** section, identify the tunnel group type as a layer 2 or layer 3 group.
9. Click **Save Settings**.

**Directing Traffic into the GRE Tunnel**

You can direct traffic into a GRE tunnel by configuring a Static route, which directs traffic to the IP address of the tunnel, or a firewall policy (session-based ACL), that redirects traffic to the specified tunnel ID.

**Configuring Static Routes**

You can configure a static route that specifies the IP address of a tunnel as the next hop for traffic for a specific destination. See **Configuring Static IP Routes on page 71** for detailed information on how to configure a static route.

While redirecting traffic into a layer 3 GRE tunnel via a static route, be sure to use the tunnel IP address of the source Branch Gateway as the next hop, instead of providing the tunnel IP address of the destination Branch Gateway.

**Configuring a Firewall Policy Rule**

You can configure a firewall policy rule to redirect selected traffic into a GRE tunnel.

Traffic redirected by a firewall policy rule is not forwarded to a tunnel that is down (see, **Configuring Tunnel Keepalives on page 68**, for more information on how GRE tunnel status is determined).

To configure a firewall policy for directing traffic into a GRE tunnel using session based ACLs, see **Creating a Firewall Policy for Network Services on page 83**.

**Configuring Routes**

The Branch Gateway and VPN Concentrator in an SD-Branch network must have IPv4 routes to determine how each device must reach Central and its VPN peers over any intermediate public or private IPv4 networks (underlay routes). Routes are also required to determine the internal networks that must be reached by the SD-WAN Gateways through the overlay VPN tunnels (overlay routes).

**Underlay Routes**

To reach WAN or the internet, the VPN Concentrators in data centers can use static routes. In case of private WAN deployments, the administrators can configure Open Shortest Path First (OSPF) routes.
Building Configuring Static
Static Using Aruba
Using Forwarding
Using Configuring

Branch Gateways, however, use the default routes obtained from service providers through DHCP or PPPoE. For private WAN deployments or MPLS routing, the administrators can configure static routes.

Overlay Routes
For overlay routes, the administrators can use IKEv2 extensions to dynamically learn networks from each connected branch. The routes can be populated in the forwarding table for each VPN Concentrator as static routes. These routes can also be redistributed into OSPF. The administrators can define static routes for each destination network and VPN Concentrator, and then configure VPN Concentrators to redistribute routes at different costs to prevent routing loops.

See the following topics for information on how to configure routes:
- [Configuring Static IP Routes on page 71](#)
- [Configuring Default Gateways for Routing on page 71](#)
- [Configuring OSPF on page 72](#)

Configuring Static IP Routes
For overlay routing using static IP routes, ensure that you define static routes for each branch network and data center as follows:
- Static routes for each branch network must be defined on the router in the data center.
- Static routes for each branch network must be defined on the VPN Concentrator for each remote network, peer, and link.
- Static routes for each data center or a hub site must be defined for each Branch Gateway.

Creating a Static IP Route
To configure a static IP route, complete the following steps:
1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Routing**.
4. Under **IP Routes**, click + to add a static route to a destination network or host.
5. Enter the IP address and netmask for the **Destination IP address** and **Destination network mask**, respectively.
6. Configure a forwarding setting:
   - **Using Forwarding Router Address**—Enter the next hop IP address in dotted decimal format (A.B.C.D). You can also enter the distance metric (cost) for this route. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.
   - **Using IPsec Tunnel to VPC**—Select the VPN Concentrator and the uplink to use. Select this option for a Hub and Spoke VPN. For more information, see Configuring Hub and Spoke VPN on page 54.
   - **Using Site-to-Site IPsec**—Enter the IPsec map name to use in a static IPsec route map. Select this option for a site-to-site VPN. For more information, see Configuring Site-to-Site VPN on page 61.
   - **Using Null Interface**—Designate a null interface.
7. Specify a value for the **Cost**.
8. Save the changes.

Configuring Default Gateways for Routing
To configure default gateways for routing, complete the following steps:
1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click Routing.
4. Under IP Routes, configure any of the following actions:
   - To configure a static default gateway:
     a. Click the + icon under Static Default Gateway.
     b. Select Ipv4 from the IP version drop-down list.
     c. In the IP Address field, enter an IP address with dot separators.
     d. In the Cost field, enter a value for the path cost.
     e. Save the changes.
   - To configure a dynamic default gateway:
     a. Click the + icon under Dynamic Default Gateway.
     b. In the Dynamic Default Gateway section, select the DHCP, PPPoE, or Cellular check box to enable the corresponding dynamic gateway type. If you selected more than one dynamic gateway type you must ensure that the cost for each gateway route is also defined. The Branch Gateway first tries to obtain a gateway IP address using the option with the lowest cost. If the Branch Gateway is unable to obtain a gateway IP address, it then tries to obtain a gateway IP address using the option with the next lowest path cost.
     c. Save the changes.

**Configuring OSPF**

Open Shortest Path First (OSPF) is a routing protocol used for distributing routing information. Aruba supports OSPFv2 on SD-WAN Gateways; it allows devices functioning as default gateways to forward user packets to the upstream router.

In an SD Branch setup, OSPF is primarily used for redistributing routes learned through the IKE-based routing in the enterprise data center network. All the OSPF control packets that are exchanged between the SD-WAN Gateways undergo GRE encapsulation before entering the IPsec tunnels. The Branch Gateways advertise all the user subnet addresses as stub addresses in router Link-State Advertisement (LSA). VPN Concentrators in turn forward these router LSAs to the upstream routers.

**Prerequisites**

To use OSPF for routing, you must configure the following:

- Enable IKEv2 extensions at each branch to redistribute branch routes to each VPN Concentrator.
- Configure VPN Concentrators to redistribute their static routes in OSPF at different costs.
- Define static routes on each Branch Gateway for each network.

**Enabling and Configuring OSPF Parameters**

To enable OSPF routing parameters, complete the following tasks:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the group or Branch Gateway for which you want to configure OSPF routing.
3. Click Routing > OSPF.
4. Enable OSPF and configure the following parameters:
   - **Configure router ID**—IPv4 address of the router.
   - **Redistribute VLAN ID**—VLAN ID that connects to the OSPF domain.
5. If required, enable **Redistribute overlay routes**, and then specify a cost for the overlay routes.
6. If required, enable **Redistribution of static routes**, and then specify a cost of static routes. This option is not applicable if you enabled **Redistribute overlay routes**

7. To add an OSPF area, click the + icon under the **Area** table and configure the following parameters:
   - **Area ID** (eg. 0.0.0.0)—Specify the IP address of the area to be used.
   - **Area type (select normal for backbone/regular)**—Select the area type as Normal, Stub or NSSA as per your network requirements. For Stub and NSSA area types, you can configure the default cost and default information. You can also choose to disable redistribution and link state advertisement summary for NSSA.

8. To add an excluded subnet, click the + icon under the **Excluded Subnet** table, and specify the required values.

9. Save the changes.

### Configuring Policies for PBR

For most SD-WAN deployments, Branch Gateways forward traffic through the overlay network or to the Internet using destination-based routing. Each Branch Gateway includes static routes for the corporate subnets that point to their respective VPN overlay tunnels as well as default gateways for each WAN uplink.

However, for some deployments, you may need to forward traffic from a subset of devices through a specific VPN overlay tunnel or to a specific Internet WAN uplink. Alternatively, you may require all traffic (corporate and Internet) to be forwarded through the overlay VPN tunnels or force all traffic to be forwarded locally using Policy Based Routing (PBR). A typical use case for PBR would be to force all traffic to a specific VPN Concentrator or a tunnel endpoint.

PBR allows your network administrators to create policies for making routing decisions. You can create a PBR rule that can forward traffic as normal, or route traffic over a VPN tunnel specified by an IPsec map. The PBR rules can also route traffic to a next hop router on a next hop list, or redirect it over an L3 GRE tunnel or tunnel group. PBR rules allow administrators to make use of all available uplinks.

### PBR Policies for WAN Networks

In the SD Branch solution, the administrators can create PBR policies to configure preferred VPN traffic routing paths for different types of traffic based on their source and destination IPs and ports.

To use PBR policies or rules on WAN networks, you must configure the following features and parameters on SD-WAN Gateways:

- **PBR next hop**—The PBR next hop can be physical links such as the Ethernet or 3G/4G uplinks. The administrators can also use logical links like site-to-site VPN tunnel.
- **Route ACL**—The administrators can define traffic match conditions and the next hop for the traffic in the ACL.
- **Attach Points**—To apply the PBR rules, the administrators associate the ACL rules to a user role or VLAN.

After the next hop list is configured and attached to route ACL, the active IP address for the next hop is selected based on the reachability and priority.

When the user traffic hits the route ACL, the following actions are applied:

- If PBR is disabled on the user-role or VLAN, traffic is directly sent to the routing block where the regular routing takes place.
- If the PBR is enabled, the traffic is evaluated against the route ACL and the appropriate PBR next hop is selected for routing.
- If traffic does not match any rule in route ACL, it is passed to the routing module for regular forwarding.
If Dynamic Path Steering selects an uplink that is not provided by PBR, the PBR forwarding path takes precedence.

**Configuring Policies for PBR**

To configure a policy for PBR on Branch Gateways, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or the device group.
3. Click **Routing > Policy-Based Routing**.
4. Click + below the **Policies** table to create a new routing policy.
5. Enter name for the policy and save the changes.
6. Select the policy from the **Policies** table.
7. Click + to add ACL rules. For more information on ACL rule configuration, see Configuring Access Rules on page 84.
8. Save the changes.
9. Assign the policy to a user role or VLAN. For more information, see Assigning PBR Policies to User Role or VLAN on page 74.

**Assigning PBR Policies to User Role or VLAN**

To assign a PBR policy to a user role or a VLAN, complete the following steps:

1. To assign a policy to a user role, see Assigning a Policy to a Role on page 92.
2. To assign a policy to a VLAN, complete the following steps:
   a. From the app selector, click **Gateway Management**.
   b. From the group selection filter bar, select the SD-WAN Gateway or the device group.
   c. Click **Interfaces > VLANs** tab.
   d. Select a VLAN from the **VLANs** table.
   e. Select the VLAN ID to which you want to assign a routing policy from the **VLAN IDs** table.
   f. Under the **IPv4** tab, expand **Other option**.
   g. Select a routing policy from the **ACL** drop-down list.
3. Save the changes.

**Configuring Next Hop Lists for PBR**

You can configure SD-WAN Gateway to use policy-based routing and forward packets to a next hop device. With the next hop list, the administrators can ensure that when the next hop device becomes unreachable, the packets matching the policy can still reach their destination.

To define a next hop list, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or the device group.
3. Click **Routing > Next Hop Configuration**.
4. Click + to add a new next hop list and configure the following parameters:
**Figure 6  Next Hop Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHop-list name</td>
<td>Name of the new next hop list.</td>
</tr>
</tbody>
</table>

**NextHop IP/DHCP**

IP address of the next hop device or the VLAN ID of the VLAN used by the next hop device. If the VLAN gets an IP address using DHCP and the default gateway is determined by the VLAN interface, the gateway IP is used as the next hop IP address. When you click + to define a next hop IP or DHCP value, a pop-up list with a field that requires you to select either the **IP** or **DHCP** option is displayed.

- If you selected **IP**, enter the IP address and priority of the next hop device in the **IP** and **Priority** fields, respectively.
- If you selected **DHCP**, enter the VLAN ID and priority of the next hop device in the **VLAN ID** and **Priority** fields, respectively.

Priorities of next hops define which next hop should get a higher priority to carry the session traffic. A higher number indicates a higher priority (1 – 255). If two next hops have the same priority, they will be load-balanced.

**IPsec name map**

A next hop list may require policy-based redirection of traffic to different VPN tunnels. To add an IPsec name map, complete the following steps:

1. Click + from the **IPsec name map** table. The **Add New IPsec Map** pop-up is displayed.
2. Select one of the following options from the **Forward settings** drop-down list based on your requirement:
   - **Using Site-to-Site IPsec**—Select this option for a site-to-site VPN or Zscaler tunnel and select the required IPsec map from the **Using site-to-site IPsec** drop-down list. If uplink VLAN is configured for the selected IPsec map, then you can select the required uplink from the **Uplink** field.
   - **NOTE**: The **Uplink** field does not appear for IPsec maps that are not configured with uplink VLAN.
   - **Using IPsec Tunnel to VPNC**—Select this option for a Hub and Spoke VPN and select the required MAC address and the uplink of the VPN Concentrator from the **Using IPsec tunnel to VPNC** and **Uplink** options lists respectively. You can also select **None** if you want to use Auto-VPN. For more information, see Configuring Hub and Spoke VPN on page 54.
3. Enter the priority value for the forward setting in the **Priority** field.
   - **NOTE**: Use the same priority for different paths from the same SD-WAN Gateway but different priorities for different Zscaler data centers.
4. Click **OK**.

**Preemptive failover**

If preemptive failover is disabled and the highest-priority device on the next hop list is disabled, the new primary next hop device functions as the primary device even when the original device comes back online.

- **NOTE**: Ensure that preemptive failover is enabled for Zscaler tunnels.

5. Click **Save Settings**.

**Configuring Policies for Dynamic Path Steering**

For a transport-independent SD-WAN fabric, the SD Branch devices form IPsec tunnels over all WAN circuits. For your branch setup to work across asymmetric links, a path selection criteria is required to enable Branch Gateways to dynamically choose an upstream path in real-time. To enable Branch Gateways to dynamically steer traffic to an upstream path, you can create WAN policies with specific performance criteria for different types of traffic, so that the best local uplink or optimal path (MPLS or the internet) is used for a given traffic flow.

The dynamic path selection feature allows you to steer and route traffic in real-time and load-balance traffic across available uplinks. For example, you can create policies that would route the most critical traffic, such as voice traffic, through the MPLS network, while the rest of the traffic is load-balanced. You could also set policies...
to route the voice traffic over uplinks with the least amount of packet loss, while the other types of traffic can be routed to uplinks with the lowest latency.

For optimal use of uplink resources, you can configure path steering policies with specific match criteria to choose an uplink. The uplink choice is driven by the parameters in the threshold profile, which include latency, jitter, packet loss, and bandwidth utilization metrics.

**How Dynamic Path Selection Works**

A dynamic path steering policy serves as a global policy that determines paths for the outgoing corporate and Internet traffic. The policy consists of the following configurable components:

- **Rules**—The policy includes a sequential list of rules for traffic steering.
- **Service Level Agreements (SLAs) and Threshold Settings**—Each of these rules can be configured with specific threshold settings that are based on SLAs.
- **Probe**—Based on the type of the SLA (threshold profiles), a probe criteria can be defined to determine the SLAs.
- **WAN path preferences**—The policy also allows you to set a path preference and enable load balancing of sessions among multiple paths.

**Example**

The following example illustrates the path selection workflow:

1. A client device tries to connect to the network.
2. The authentication server authenticates the client, assigns the employee role, and then directs the client to the SD-WAN Gateway.
3. The firewall classifies the session as Skype.
4. The routing for an employee using Skype states that the next-hop is a VPN Concentrator and that the paths available are MPLS, INET1, and LTE.
5. As Skype is classified as UCC, the policy categorizes it as voice traffic. The policy is configured to use MPLS as the preferred path with an SLA criterion.
6. If the threshold metrics for MPLS meet the SLA for the voice policy, the session goes through the tunnel that is established using the MPLS uplink.
7. If at any point in time the measured SLA for MPLS drops, the SD-WAN Gateway steers traffic to another active tunnel.

**Configuring a Dynamic Path Steering Policy**

The Dynamic Path Steering policy configuration procedure includes the following tasks:

1. Creating a Dynamic Path Steering Policy on page 77
2. Configuring Traffic Specification Rules on page 77
3. Configuring SLA Parameters on page 77
4. Configuring WAN Path on page 78

---

**Note**

Ensure that you configure health check probe destinations and uplinks before configuring the dynamic path steering policies.
Creating a Dynamic Path Steering Policy

To create a dynamic path steering policy, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or Branch Gateway for which you want to create a dynamic path steering policy.
3. Click **WAN > Dynamic Path Steering**.
4. To create a new policy, click +.
5. Enter the name of the policy.
6. Click **Save Settings**.

Configuring Traffic Specification Rules

To add traffic specification rules, complete the following steps:

1. Go to **Gateway Management > WAN > Dynamic Path Steering**.
2. From the list of policies, select the policy to edit.
3. Click the edit icon in **Traffic Specification Rules**.
4. To add a new rule, click +, and then configure the following parameters:
   - **Source**—You can set the source to any of the following options:
     - *Any*—For the traffic coming from any source.
     - *User*—For the traffic originating from a specific user role.
     - *Host*—For the traffic that has a specific source IP from a subnet of IP addresses.
     - *Network*—For the traffic that has a specific source IP from a subnet of IP addresses.
     - *User Role*—For the traffic originating from an alias of a host or network.
   - **Destination**—You can set the destination as any, specific host, or network.
   - **Application/Port**—You can select any of the following options:
     - *Application*—To set rules for a specific application, for example, Facebook.
     - *Application Category*—To set traffic rules for application category, for example, social networking.
     - *Web Categories/Reputations*—To set rules for web categories, for example, travel.
     - *UDP*—To set rules for TCP.
     - *TCP*—To set rules for UDP.
     - *Service*—To set rules for any specific network service.
5. Click **Save Settings**.

Configuring SLA Parameters

To set SLA parameters for the traffic type configured for the policy, complete the following steps:

1. Click the edit icon in **SLA**.
2. In the policy definition, configure the following SLA categories and parameters:
   - **Name**—Name of the service. The default services are **BestForInternet**, **BestForVoice**, and **HighlyAvailable**. Click + to add a new service.
   - **Latency**—To measure the round-trip ping time. You can set a threshold value in milliseconds.
Jitter—To measure if the packets are delivered in a proper order. You can set a threshold value in milliseconds to observe jitters in packet transmission.

Loss—To measure packet loss. You can set a specific percentage of packet loss allowed for the traffic type.

Utilization—To measure the percentage of bandwidth utilization. You can set a specific percentage of bandwidth utilization as a metric to prioritize and load-balance the traffic.

3. Click **Save Settings**.

**Configuring WAN Path**

To configure a WAN path for traffic types defined in the policy, complete the following steps:

1. Click the edit icon in **WAN Path Selection**.
2. In the policy definition, set the following parameters for WAN path selection:
   - **Primary Path**—Routes the traffic through the primary path. For example, if you are configuring policies for critical traffic such as voice or VoIP, you can set MPLS as the primary path. The list shows the IDs of the uplink types that are already configured. You can select multiple uplink IDs in a sequential order. The uplinks are selected based on load balancing when multiple uplinks are configured.
   - **Secondary Path**—Routes the traffic through the secondary path in the event of failover or for load balancing. The session continues on the link as long as it is good irrespective of the status of the primary uplink. Select the uplink types or IDs for the secondary path.
   - **Tertiary Path**—Routes the traffic through another path as a last attempt (when both primary and secondary paths are down) to deliver traffic packets. The session is steered back to the primary or secondary path as soon as one of them becomes active.
3. Click **Save Settings**.

**Routing Traffic After Path Selection**

After path selection, the next hop is determined by the IP forwarding table. When a path is selected, the IP forwarding table determines the next hop. Based on the routes configured on the Branch Gateway, the next hop can be an IPsec map or the router IP address.

- If the next hop is an IPsec map, the session is forwarded to the IPsec map that is configured in the forwarding table associated with the selected path.
- If the next hop is a router IP address, the session is forwarded to the default gateway that is associated with the selected path.

**Enforcing a Common Security Policy for Wired and Wireless Users**

The Aruba SD Branch solution supports dynamic segmentation of the branch network based on device profiles. The solution also supports diverting client traffic from selected devices to Branch Gateways.

If your SD Branch has Aruba Switches deployed and provisioned to function along with the Branch Gateways, your network administrators can configure common set of security policies for wired and wireless clients on the ClearPass server and use Branch Gateway as policy enforcement points to inspect every communication in the branch.

The **Tunneled Node** feature on Aruba switches allows wired traffic entering a switch port to be routed to Branch Gateway through the GRE tunnel. An Aruba switch can also initiate a GRE tunnel with the Branch Gateway from its management IP address associated to an underlay VLAN that is different from the user VLANs.
To allow policy enforcement for the wired traffic, the port-based tunnels must be configured and the IP address of the Branch Gateway must be set as a primary tunneled node on the switches. For more information on the configuration procedure, see the *HPE ArubaOS-Switch Management and Configuration Guide*.

**Configuring Policies for Website Content Classification**

WebCC service supports network security and complements the existing application visibility and role based security for mobile enterprises. It is a policy enforcement feature that includes URL filtering, IP reputation, and geolocation filtering.

When a Branch Gateway receives a new session request, it fetches the source and destination IP addresses and does a table lookup for both the IP addresses to get the reputation or geolocation information of these IPs. If the table lookup succeeds, then the session is marked as classified and is subjected to IP classification based firewall policies. If the table lookup fails, then the classification for these IPs are downloaded from Webroot’s Brightcloud service.

The Branch Gateways leverage the collaboration with Webroot’s Brightcloud service to fetch an IP reputation and geolocation database. The IP reputation database contains known IP addresses associated with various malicious activities or threats such as botnet, DOS, and spam sources. The geolocation IP database contains the geographical location of the IP address from where the traffic is received or to which the traffic is sent. This allows the Branch Gateways to provide geolocation and reputation filtering as part of the security suite.

This topic includes the following sections:
- [Enabling WebCC Visibility on page 79](#)
- [Configuring WebCC Services on page 79](#)
- [Configuring ACLs for Web Content Classification on page 86](#)

**Enabling WebCC Visibility**

To enable WebCC visibility, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selector, select a group or a device.
3. Click **Security > Applications**.
4. Click **Application Visibility**.
5. For enabling traffic analysis for WebCC, select the **Web content classification (webcc)** check box.
6. Click **Save Settings**.
7. From the app selector, click **Monitoring & Reports** and go to **Network Overview > Gateways**. The **Gateways** page displays the Website categories and Website reputation charts.

For more information, see [Analyzing Application Usage on page 131](#).

**Configuring WebCC Services**

You can configure the following WebCC services on your SD-WAN Gateways. The following sections describe the procedures to enable and configure various WebCC services on the SD-WAN Gateways:
Drop Unclassified Web Content
To drop the packets that do not match any web content category or reputation levels in the Branch Gateway's internal web content cache, complete the following task:
1. From the app selector, click **Gateway Management**.
2. From the group selector, select a group or a device.
3. Click **Security > Applications**.
4. Click **Application Visibility**.
5. For website URL filtering, select the **Web Content Classification (WebCC)** check box.
6. Select the **Drop packets during webcc miss** check box.
7. Click **Save Settings**.

Configure URL to Redirect Blocked Session
To configure a URL to redirect the users when they access blocked sessions, complete the following tasks:
1. From the app selector, click **Gateway Management**.
2. From the group selector, select a group or a device.
3. Click **Security > Applications**.
4. Click **Application Visibility**.
5. For website URL filtering, select the **Web Content Classification (WebCC)** check box.
6. Specify a URL to which the users should be redirected when they access blocked session in the **URL to redirect blocked session** field.
7. Click **Save Settings**.

Configure IP Reputation and Filtering
IP reputation policies can be applied to Branch Gateways. These policies are useful in preventing traffic from or to malicious websites.

Before configuring this feature, ensure that you configure the WebCC or Web reputation policies. For more information, see Configuring ACLs for Web Content Classification on page 86.

To enable IP reputation and filtering, complete the following tasks:
1. From the app selector, click **Gateway Management**.
2. From the group selector, select a group or a device.
3. Click **Security > Applications**.
4. Click **Application Visibility**.
5. For website URL filtering, select the **Web Content Classification (WebCC)** check box.
6. Enable **IP classification and reputation**.
7. To deny incoming traffic from malicious IP addresses, select the **Deny inbound connections from malicious IP address**.
8. To deny outgoing traffic to malicious IP addresses, select the **Deny outbound connections to malicious IP address**.
9. To whitelist any trusted IP address or a range of IP addresses that may be misclassified as malicious IP addresses, complete the following tasks:
a. Click + from the **IP ADDRESS** table under the **Whitelisted IP addresses** field.
b. Enter the IP address to be whitelisted in the **IP address** field. If you want to whitelist a range of IP addresses, enter the starting IP address of the range in this field.
c. Enter the ending IP address of the range to be whitelisted in the **End IP address** field.
d. Specify any description of the IP address or the IP address range in the **Description** field.

The IP addresses included in this table are considered trusted IP addresses even if they are classified as malicious IP address by the IP reputation database.

10. Click **Save Settings**.

**Configure Geolocation-Based Filtering**

The Geolocation filtering policies allow you to filter traffic based on the geographic location of the source or destination IP addresses. You can configure these policies to permit or deny outgoing or incoming traffic from specific countries.

To enable geolocation-based filtering, complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. From the group selector, select a group or a device.
3. Click **Security > Applications**.
4. Click **Application Visibility**.
5. For website URL filtering, select the **Web Content Classification (WebCC)** check box.
6. Enable **Geo location**.
7. Click + in the **GeoLocation** table to add a new geolocation rule.
8. In the **New GeoLocation Rule** section, configure the following parameters:
   - **Action**—Select the action as **Permit** or **Deny**.
   - **Direction**—Select the direction as **To** or **From**.
   - **Country**—Select the required country for which you want to apply this rule.
   - **Log**—Select the check box to enable logging for this rule.
9. Click **Save Settings**.

**Configuring Firewall Policies and ACLs**

To secure your branch, you must configure a policy with a set of ACLs and apply these policies to user roles or user-facing VLAN interfaces.

For an SD Branch setup, the general recommendation is to set the WAN-facing ports as trusted and LAN-facing ports as untrusted. Although WAN-facing ports are trusted, Aruba recommends that you apply a restrictive firewall policy to the WAN interfaces.

As LAN-facing ports are untrusted, it is very important to secure your branch by applying a AAA profile to the VLANs configured for the LAN interfaces. When a AAA policy is applied, SD-WAN Gateways assign the user roles based on the role preferences configured in a AAA profile.
Firewall Policies for SD Branch

The SD Branch solution supports identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for the WAN network. You can configure firewall policies on Branch Gateways to define user access to network, set priority queue for Quality of Service (QoS), and assign bandwidth contracts.

A firewall policy identifies specific characteristics about a data packet and performs one of the following actions: The action can be one of the following types:

- Firewall-type action such as permitting or denying the packets.
- Administrative action such as logging the packets.
- QoS action such as setting 802.1p bits or placing the packet in a priority queue.

Types of ACLs

Central allows you to configure the following types of ACLs on Branch Gateways.

- **Standard ACLs**—Permit or deny any traffic based on the source IP address of the packet. Standard ACLs can be either named or numbered, with valid numbers in the range of 1–99 and 1300–1399. Standard ACLs use a bit-wise mask to specify the portion of the source IP address to be matched.

- **Extended ACLs**—Permit or deny any traffic based on source or destination IP address, source or destination port number, or IP protocol. Extended ACLs can be named or numbered, with valid numbers in the range 100–199 and 2000–2699.

- **MAC ACLs**—Filter the traffic on a specific source MAC address or range of MAC addresses. MAC ACLs can be either named or numbered, with valid numbers in the range of 700–799 and 1200–1299.

- **Ethertype ACLs**—Filter the traffic based on the Ethertype field in the frame header. Ethertype ACLs can be either named or numbered, with valid numbers in the range of 200–299. These ACLs can be used to permit IPs while blocking other non-IP protocols, such as IPX or AppleTalk.

- **Session ACLs**—Restrict all services from specific hosts and subnets. Rules with this ACL are applied to all traffic on the Branch Gateway regardless of the ingress port or VLAN.

- **Route ACLs**—Forward all packets to a device defined by an IPsec map, a next hop list, a tunnel or a tunnel group.

Configuring Aliases for Firewall Policies

Aliases allow you to name your network ports, protocols, and services in a simple yet understandable way. When configuring multiple ACLs, you can use a common alias instead of providing details of the network ports, protocols, and services each time.

Creating a Network Alias

A network alias defines a TCP, UDP, or IP protocol and a list or range of ports supported by that service. You can use a network alias when specifying a network service for multiple session ACLs.

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or device for which you want to create a network service alias.
3. Click **Security > Aliases**.
4. Click + to create a network alias.
5. Enter a name and description for this alias.
6. Click **Save Settings**.
7. Under **Destination** click + to add a new user rule.
8. Select **Network** from the **Rule type** drop-down list.
9. Enter a IPv4 address and Network mask.
10. Click **Save Settings.**

**Creating a Service Alias**

To create a service alias:

1. From the app selector, click **Gateway Management.**
2. From the group selection filter bar, select the group or device for which you want to create a network service alias.
3. Click **Security > Aliases.**
4. Click + to create a service alias.
   a. Enter a value in the **Service name** field.
   b. In the **Protocol** drop-down list, select either **TCP** or **UDP**, or select **protocol** and enter the IP protocol number and **Application level gateway (alg)** of the protocol for which you want to create an alias.
   c. In the **Port type** drop-down list, specify whether you want to define the port by a contiguous range of ports, or by a list of non-contiguous port numbers.
      - If you selected **range**, enter the starting and ending port numbers in the **Starting port** and **End port** fields, respectively.
      - If you selected **list**, enter a comma-separated list of port numbers in the **Port list** field.
   d. To limit the service alias to a specific application, select one the of the following service types from the **Application Level Gateway (alg)** drop-down list:
      - ftp: Service is FTP
      - tftp: Service is TFTP
      - dns: Service is DNS
      - dhcp: Service is DHCP
      - sip: Service is SIP
      - sips: Service is Secure SIP
      - svc: Service is SVP
      - scvp: Service is SCCP
      - rtsp: Service is RTSP
      - vocera: Service is VOCERA
      - noe: Service is Alcatel NOE
      - h323: Service is H323
      - jabber: Service is Jabber
      - facetime: Service is Facetime
   5. Click **Save Settings.**

**Creating a Firewall Policy for Network Services**

To create a firewall policy:

1. From the app selector, click **Gateway Management.**
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Click **Security > Policies.**
4. Click + to create a new policy.
5. Select a policy type from the Policy type drop-down list. You can select Session, Ethertype, MAC, Route, Extended, or Standard.
6. Enter the policy name in the Policy name field.
7. Click Save Settings.

Configuring Access Rules

1. From the list of policies, select the policy that you created and click + in the Policy <policy name> table.
2. Select the Access Control option in the Rule Type field and click OK.
3. To add a rule to restrict packet flow or permit access to network or services, configure the following parameters:

Table 24: Firewall Policy Rule Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP version</td>
<td>Specifies the IP version that the policy applies to. Select IPv4.</td>
</tr>
<tr>
<td>Source (required)</td>
<td>Source of the traffic, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Any—Acts as a wildcard and applies to any source address.</td>
</tr>
<tr>
<td></td>
<td>- User—Refers to the traffic from the wireless client.</td>
</tr>
<tr>
<td></td>
<td>- Host—Refers to the traffic from a specific host. When this option is</td>
</tr>
<tr>
<td></td>
<td>selected, specify the IP address of the host.</td>
</tr>
<tr>
<td></td>
<td>- Network—Refers to the traffic that has a source IP from a subnet of</td>
</tr>
<tr>
<td></td>
<td>IP addresses. When this option is selected, specify the IP address and</td>
</tr>
<tr>
<td></td>
<td>network mask of the subnet.</td>
</tr>
<tr>
<td></td>
<td>- Alias—Refers to using an alias for a host or network.</td>
</tr>
<tr>
<td></td>
<td>- Local IP—Refers to the local IP address.</td>
</tr>
<tr>
<td></td>
<td>- User Role—Refers to the user role to be assigned.</td>
</tr>
<tr>
<td>Destination (required)</td>
<td>Destination of the traffic.</td>
</tr>
<tr>
<td>Service/app (required)</td>
<td>Type of traffic, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Any—This option specifies that this rule applies to any type of traffic.</td>
</tr>
<tr>
<td></td>
<td>- TCP—Using this option, you configure a range of TCP ports to match the</td>
</tr>
<tr>
<td></td>
<td>rule to be applied.</td>
</tr>
<tr>
<td></td>
<td>- UDP—Using this option, you configure a range of UDP ports to match the</td>
</tr>
<tr>
<td></td>
<td>rule to be applied.</td>
</tr>
<tr>
<td></td>
<td>- Service—Using this option, you use one of the pre-defined services (</td>
</tr>
<tr>
<td></td>
<td>common protocols such as HTTPS and HTTP) as the protocol to match for</td>
</tr>
<tr>
<td></td>
<td>the rule to be applied.</td>
</tr>
<tr>
<td></td>
<td>- Protocol—This option specifies the routing protocol.</td>
</tr>
<tr>
<td>Action (required)</td>
<td>The action that you want the Branch Gateway to perform on a packet that</td>
</tr>
<tr>
<td></td>
<td>matches the specified criteria.</td>
</tr>
<tr>
<td></td>
<td>- Deny—Denies traffic not matching this rule.</td>
</tr>
<tr>
<td></td>
<td>- Reject—Drops the packet and sends an ICMP notification to the traffic</td>
</tr>
<tr>
<td></td>
<td>source.</td>
</tr>
<tr>
<td></td>
<td>- Permit—Permits the traffic matching this rule.</td>
</tr>
<tr>
<td></td>
<td>- Redirect—This option redirects the traffic to a GRE tunnel. This option</td>
</tr>
<tr>
<td></td>
<td>is used primarily to redirect all guest traffic to a GRE tunnel and then</td>
</tr>
<tr>
<td></td>
<td>to a DMZ router or switch.</td>
</tr>
<tr>
<td></td>
<td>- Destination NAT—Redirects traffic to the configured IP address and</td>
</tr>
<tr>
<td></td>
<td>destination port. An example of this option is to redirect all HTTP</td>
</tr>
<tr>
<td></td>
<td>packets to the captive portal port on the Branch Gateway as used in the</td>
</tr>
<tr>
<td></td>
<td>predefined policy called captive portal. This action functions in tunnel</td>
</tr>
<tr>
<td></td>
<td>or decrypt-tunnel forwarding mode. User should configure the NAT pool in</td>
</tr>
<tr>
<td></td>
<td>the Branch Gateway.</td>
</tr>
<tr>
<td></td>
<td>- Source and Destination NAT—This option performs both source and</td>
</tr>
<tr>
<td></td>
<td>destination NAT on packets matching the rule. This action forwards</td>
</tr>
<tr>
<td></td>
<td>packets from the source network to the destination network and re-</td>
</tr>
<tr>
<td></td>
<td>marks them with destination IP of the target network. This action</td>
</tr>
<tr>
<td></td>
<td>functions in tunnel or decrypt-tunnel forwarding mode. User should</td>
</tr>
<tr>
<td></td>
<td>configure the NAT pool in the Branch Gateway.</td>
</tr>
</tbody>
</table>
Table 24: Firewall Policy Rule Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSCP (optional)</strong></td>
<td>Option to re-tag the traffic with the specified DSCP tag in the IP header of the packet that matches this rule when it leaves the Branch Gateway.</td>
</tr>
<tr>
<td><strong>Time Range</strong></td>
<td>You can allow or deny access during specific time range. You can either create an absolute time range with a single fixed start and end date and time; or a periodic (recurring) time range that starts and ends at a specified time on a weekday, weekend, or selected day.</td>
</tr>
<tr>
<td><strong>802.1p Priority (optional)</strong></td>
<td>When this parameter is enabled, the value of 802.1p priority bits are marked in the frame of a packet matching this rule when it leaves the Branch Gateway. 0 represents the lowest priority (background traffic) and 7 represents the highest priority (network control).</td>
</tr>
<tr>
<td><strong>Log (optional)</strong></td>
<td>Logs a match to this rule. This is recommended when a rule indicates a security breach, such as a data packet on a policy that is meant only to be used for voice calls.</td>
</tr>
<tr>
<td><strong>Mirror (optional)</strong></td>
<td>Mirrors session packets to datapath or remote destination.</td>
</tr>
<tr>
<td><strong>Blacklist (optional)</strong></td>
<td>Automatically blacklists a client that is the source or destination of the traffic matching this rule. This option is recommended for rules that indicate a security breach where the blacklisting option can be used to prevent access to clients that are attempting to breach the security.</td>
</tr>
<tr>
<td><strong>Disable scanning (optional)</strong></td>
<td>Disable AP scanning other channels.</td>
</tr>
</tbody>
</table>

Configuring ACLs for Deep Packet Inspection

Branch Gateways support AppRF, Aruba’s custom-built layer 7 firewall capability. It consists of an onboard Deep Packet Inspection (DPI) service that allows creating firewall policies based on the types of application and application categories.

You can configure ACLs to restrict user access to an application or application category. You can also define traffic-shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth-monopolizing applications on a guest role within an enterprise.

Creating ACLs for Application Usage

To create ACL rules for Deep Packet Inspection, complete the following steps:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the group or device for which you want to create DPI user rules.
4. Click + to create a new policy.
5. Enter the policy name in the Policy name field.
6. From the list of policies, select the policy you just created and click +.
7. Select one of the following options from the Service/app drop-down list.
   - Application—To allow or deny access to a specific application.
   - Application Category—To allow or deny access to a specific application category.
8. Specify an action.
9. Click Save Settings.

Configuration Example

This example shows a DPI rule along with a layer 3 or layer 4 rule with forwarding action in the same ACL. Both ACL policies can be applied to a single user role.

- Rule 1
  - source: any
  - destination: any
  - service or application: application facebook
  - action: permit
  - DSCP value: 45

- Rule 2
  - source: any
  - destination: any
  - service or application: application YouTube
  - action: deny

- Rule 3
  - source: any
  - destination: any
  - service or application: application category peer-to-peer
  - action: deny

- Rule 4
  - source: any
  - destination: any
  - service or application: TCP 23
  - action: permit

- Rule 5
  - source: network 40.1.0.0/16
  - destination: any
  - service or application: TCP 80
  - action: permit
  - DSCP: 60

Configuring ACLs for Web Content Classification

The WebCC feature in Branch Gateways allows your network administrators to analyze the website usage by clients. Branch Gateways classify the usage pattern based on web categories and website reputation scores; it allows your network administrators to take appropriate measures to prevent malicious malware, spyware, or adware by blocking dangerous websites.

To configure an ACL rule for website content classification, complete the following steps:

1. From the app selector, click Gateway Management.
2. From the group selection filter, select the group or device for which you want to configure a new policy and create a WebCC rule.
3. Click **Security > Policies**.
4. Click + to create a new policy. Select a policy type from the **Policy type** drop-down list.
5. Enter the policy name in the **Policy name** field.
6. From the list of policies, select the policy you just created and click +.
7. In the **Rules of this Role only** section, perform the steps:
8. Select **Web Category/Reputation** from the **Service/app** drop-down list:
   a. From the **Web reputation** drop-down list, select one of the following reputation scores based on your requirement:
      - **high-risk**—These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads.
      - **low-risk**—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
      - **moderate-risk**—These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
      - **suspicious**—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
      - **trustworthy**—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.
   b. From the **Action** drop-down list, select **Deny** to not allow user to access this web category; else, select **Permit** to allow user to access the web category.
   c. For **DSCP**, enter a value.
   d. From the **Time range** drop-down list, select a suitable time range during which you want the policy to be active or valid. Alternatively, you can also create a new time range by clicking the + icon.
   e. From the **802.1p priority** drop-down list, select a priority from 1-7.
   f. For **Options**, select **Log**, **Mirror**, and **Blacklist**, or any other option that is applicable.
9. Click **Save Settings**.

**Configuring Global Firewall Parameters**

The SD-WAN Gateways support stateful firewall for stateful inspection of packets. Stateful firewalls provide an additional layer of security by tracking the state of network connections and using the state information from previous communications to monitor and control new communication attempts. To protect your network from external attacks and unauthorized communication attempts, you can configure match conditions and packet filtering criteria for the SD-WAN Gateways.

To configure global firewall parameters for protection against external attacks:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Click **Security > Firewall**.
4. Configure the parameters described in Table 25 as per your network requirements.
5. Click **Save Settings**.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor ping attack</td>
<td>Number of ICMP pings per 30 seconds, which if exceeded, can indicate a DoS attack. Valid range is 1-16384 pings per 30 seconds. Recommended value is 120.</td>
</tr>
<tr>
<td>Monitor TCP SYN attack rate</td>
<td>Number of TCP SYN messages per 30 seconds, which if exceeded, can indicate a DoS attack. Valid range is 1-16384 pings per 30 seconds. Recommended value is 960.</td>
</tr>
<tr>
<td>Monitor IP sessions attack</td>
<td>Number of TCP or UDP connection requests per 30 second, which if exceeded, can indicate a DoS attack. Valid range is 1-16384 requests per 30 seconds. Recommended value is 960.</td>
</tr>
</tbody>
</table>
| Monitor/police non-gratuitous ARP attacks     | Enable monitoring and policing non-gratuitous ARP attacks and configure the following parameters:  
  - **Monitor/police non-gratuitous ARP attack rate**—Specify the number of ARP packets (other than Gratuitous ARP packets) per 30 seconds, which if exceeded, can indicate a DoS attack. Valid range is 1-16384 packets per 30 seconds. Recommended value is 960.  
  - **Monitor/police non-gratuitous ARP attack action**—Select an action to be taken upon detection of ARP attacks. The options are **Blacklist** and **Drop**.                                             |
| Monitor/Police Gratuitous ARP Attack rate (per 30 seconds) | Number of Gratuitous ARP packets per 30 seconds, which if exceeded, can indicate DoS attack. Valid range is 1-16384 packets per 30 seconds. Recommended value is 50.                                                   |
| Monitor/police gratuitous ARP attack action   | The action to be taken upon detection of ARP attacks. The options are **Blacklist** and **Drop**. The default value is **Drop**.                                                                                           |
| Monitor/police CP attack rate                 | Rate limit for control plane traffic policing. Recommended value is 3000 frames per 30 seconds.                                                                                                                     |
| Deny inter user bridging                      | Prevents the forwarding of layer 2 traffic between wired or wireless users. You can configure user role policies that prevent layer 3 traffic between users or networks but this does not block layer 2 traffic. This option can be used to prevent traffic, such as Appletalk or IPX, from being forwarded. |
| Deny inter user traffic                       | Denies traffic between untrusted users by not allowing layer 2 and layer 3 traffic.                                                                                                                                 |
| Deny source routing                           | Permits firewall to reject and log packets with the specified IP options loose source routing, strict source routing, and record route.                                                                           |
| Deny all IP fragments                         | Drops all IP fragments. **NOTE**: Do not enable this option unless instructed to do so by an Aruba Support representative.                                                                                         |
| Enforce TCP handshake before allowing data    | Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option may affect mobility.               |
### Table 25: Firewall Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prohibit IP spoofing</strong></td>
<td>Enables detection of IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, source and destination IP and MAC addresses are checked for each ARP request or response. Traffic from a second MAC address using a specific IP address is denied, and the entry is not added to the user table. Possible IP spoofing attacks are logged and an SNMP trap is sent. This is enabled by default.</td>
</tr>
<tr>
<td><strong>Prohibit RST replay attack</strong></td>
<td>When enabled, closes a TCP connection in both directions if a TCP RST is received from either direction. Do not enable this option unless instructed to do so by an Aruba Customer Support representative.</td>
</tr>
<tr>
<td><strong>Log all received ICMP errors</strong></td>
<td>Enables logging of received ICMP errors. Do not enable this option unless instructed to do so by an Aruba Customer Support representative.</td>
</tr>
<tr>
<td><strong>Allow tri-session with DNAT</strong></td>
<td>Allows three-way session when performing destination NAT. This option should be enabled when the Branch Gateway is not the default gateway for wireless clients. This option is typically used for captive portal configuration.</td>
</tr>
<tr>
<td><strong>AMSDU configuration</strong></td>
<td>Enables handling AMSDU traffic from clients.</td>
</tr>
<tr>
<td><strong>Session idle timeout</strong></td>
<td>Set the time, in seconds, that a non-TCP session can be idle before it is removed from the session table. Specify a value in the range 16-300 seconds. Do not set this option unless instructed to do so by an Aruba Customer Support representative.</td>
</tr>
<tr>
<td><strong>Disable FTP server</strong></td>
<td>Disables the FTP server. Enabling this option prevents FTP transfers. Do not enable this option unless instructed to do so by an Aruba Customer Support representative.</td>
</tr>
<tr>
<td><strong>GRE call ID processing</strong></td>
<td>Creates a unique state for each PPTP tunnel. Do not enable this option unless instructed to do so by an Aruba Customer Support representative.</td>
</tr>
<tr>
<td><strong>Optimize duplicate address detection frames</strong></td>
<td>Enables optimization of duplicate address detection frames with respect to IPv4 gratuitous ARPs.</td>
</tr>
<tr>
<td><strong>Stall detection</strong></td>
<td>Enable this to detect if there is any hardware issue with forwarding engine and to take necessary mitigating steps. Do not modify this option unless instructed by an Aruba Customer Support representative</td>
</tr>
<tr>
<td><strong>Immediate freeback</strong></td>
<td>Enables immediate freeback of hardware buffers from datapath to the interface. Do not modify this option unless instructed by an Aruba Customer Support representative</td>
</tr>
<tr>
<td><strong>Stateful ICMP processing</strong></td>
<td>Enables stateful ICMP processing for all kinds of ICMP traffic. This is used to selectively control different kinds of ICMP traffic through ACLs.</td>
</tr>
<tr>
<td><strong>Mcast RED</strong></td>
<td>Enables the multicast random early detection algorithm parameters.</td>
</tr>
<tr>
<td><strong>Per-packet logging</strong></td>
<td>Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged.</td>
</tr>
<tr>
<td><strong>Prohibit ARP spoofing</strong></td>
<td>Detects and prohibits ARP spoofing. When this option is enabled, possible arp spoofing attacks are logged and an SNMP trap is sent.</td>
</tr>
</tbody>
</table>
### Table 25: Firewall Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent DHCP exhaustion</td>
<td>Enables verification DHCP client hardware address against the packet source MAC address. This command checks the frame’s source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. Enabling this feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.</td>
</tr>
<tr>
<td>Only allow local subnets in user table</td>
<td>Adds only IP addresses, which belong to a local subnet, to the user table.</td>
</tr>
<tr>
<td>Session-tunnel FIB</td>
<td>Enable session-tunnel-based forwarding. Enable this parameter only during maintenance window or off-peak production hours.</td>
</tr>
<tr>
<td>Multicast automatic shaping</td>
<td>Enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used.</td>
</tr>
<tr>
<td>Enforce bw contracts for broadcast traffic</td>
<td>Applies bandwidth contracts to local subnet broadcast traffic.</td>
</tr>
<tr>
<td>Enforce TCP sequence numbers</td>
<td>Enforces the TCP sequence numbers for all packets.</td>
</tr>
<tr>
<td>Public-access mode</td>
<td>Enables public access mode for all packets.</td>
</tr>
<tr>
<td>WMM content enforcement</td>
<td>If traffic to or from the user is inconsistent with the associated QoS policy for WMM content, the traffic is reclassified to best effort.</td>
</tr>
<tr>
<td>Rate limit CP untrusted ucast traffic (pps)</td>
<td>The rate limit value of untrusted unicast traffic. Range is 1-65535 packets pps.</td>
</tr>
<tr>
<td>Rate limit CP untrusted mcast traffic (pps)</td>
<td>The rate limit value of untrusted multicast traffic. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Rate limit CP trusted ucast traffic (pps)</td>
<td>The rate limit value of trusted unicast traffic. Range is 1-98304 pps.</td>
</tr>
<tr>
<td>Rate limit CP trusted mcast traffic (pps)</td>
<td>Specifies the trusted multicast traffic rate limit. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Rate limit CP route traffic (pps)</td>
<td>The rate limit value of route traffic that needs ARP requests. Range is 1-65535 pps.</td>
</tr>
</tbody>
</table>
### Table 25: Firewall Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate limit CP session mirror traffic (pps)</td>
<td>The rate limit value of session mirrored traffic forwarded to the SD-WAN Gateway device. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Rate limit CP VRRP traffic (pps)</td>
<td>The rate limit value of VRRP traffic that hits the control plane. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Rate limit CP ARP traffic (pps)</td>
<td>The rate limit value of ARP traffic that hits the control plane. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Rate limit CP L2 protocol/other traffic (pps)</td>
<td>The rate limit value of other L2 traffic that hits the control plane. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Rate limit CP auth process traffic (pps)</td>
<td>The rate limit value of the traffic that is forwarded to the authentication process. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Rate limit CP IKE traffic (pps)</td>
<td>The rate limit value of IKE traffic that hits the control plane. Range is 1-65535 pps.</td>
</tr>
<tr>
<td>Jumbo frames processing</td>
<td>Enables Jumbo frames processing for data frames that are larger than 1500 bytes. You can specify a value in the Jumbo MTU[1789-9216] bytes field. The range is 1789-9216 bytes. The default value is 9216 bytes.</td>
</tr>
<tr>
<td>Mark management frames</td>
<td>Enables marking of management frames.</td>
</tr>
</tbody>
</table>

### Configuring User Roles

A client device in an Aruba user-centric network is associated with a user role that determines the access privileges, bandwidth contract assignments, and frequency of client authentication.

A client device is assigned a user role by several methods. The following list shows the role assignment preferences for a branch network:

1. Initial user role—The initial user role or VLAN for unauthenticated clients is configured in the AAA profile.
2. User-derived role—The user role can be derived from user attributes when a client connects to an AP. You can configure access rules to assign a user role to the clients that match a specific criteria. For example, you can configure a rule to assign the role **VoIP-Phone** to any client that has a MAC address that starts with bytes xxyy:zz. The user-derived roles are applied before client authentication.
3. Default user role—The user role can be the default user role configured for an authentication method, such as 802.1X or VPN. For each authentication method, you can configure a default role for the clients that successfully authenticate based on the specified authentication method.
4. Server-derived role—The user role can be derived from attributes returned by the authentication server and certain client attributes. If the client authenticates through an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication, or on client
attributes such as SSID (even if the attribute is not returned by the server). Server-derived roles are applied after client authentication.

5. VSA-Derived Role—Many NAS vendors, including Aruba, use vendor-specific attributes to provide features that are not supported in standard RADIUS attributes. The Aruba VSAs allow deriving user roles and VLAN for the clients that authenticate to the RADIUS server. A role derived from a VSA takes precedence over other types of user roles.

For more information on types of the user roles and the assignment criteria, see *ArubaOS User Guide*.

### Creating a Role

To create a user role:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter, select the group or device for which you want to create a user role.
3. Click **Security > Roles**.
4. Click + from the *Roles* table to create a new role.
5. Enter a name for the new role and click **Save Settings**.
6. To add access rules, click + under **RULES of this Role only** and configure access rules.
7. Click **Save Settings**.

### Assigning a Policy to a Role

To add a policy to a role:

1. Select the role name from the *Roles* table.
2. Click + under the **Policies** tab.
3. Select the **Add an existing policy** option.
4. Select a policy type from the Policy type drop-down list. Select the policy type as **Route** to apply PBR policies.
5. Select a policy from the Policy name drop-down list.
6. Click **Save Settings**.

### Assigning User Roles in AAA Profiles

AAA profiles define user roles for unauthenticated clients (initial role) as well as the default user role for MAC and 802.1X authentication.

To assign user roles in a AAA profile:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or device for which you want to assign user role in AAA profile.
3. Click **Security > AAA Profiles**.
4. Click + to create a new role.
5. Select a profile under **AAA Profiles**.
6. Select the default profile or a user-defined AAA profile.
7. Select the desired user role for unauthenticated users, from the **Initial Role** drop-down list.
8. Select the desired user role for users who have completed 802.1X authentication, from the **802.1X Authentication Default Role** drop-down list.
9. Select the desired user role for clients who have completed MAC authentication, from the **MAC Authentication Default Role** drop-down list.

10. Click **Save Settings**.

**Configuring a Default Role Based on Authentication Methods**

You can configure a default role for the clients that authenticate using the specified authentication that method. To configure a default role for an authentication method:

1. From the app selector, click **Gateway Management**.

2. From the group selection filter bar, select the group or device for which you want to configure a default role for a specific authentication method.

3. Click **Security > AAA Profiles**.

4. Click + to create a new role.

5. To configure the default user role for MAC or 802.1X authentication, select the **AAA Profiles** tab.

6. Select an AAA profile under **AAA Profiles** and select the desired user role for **MAC Authentication Default Role** or **802.1X Authentication Default Role**.

7. To configure the default user role for other authentication methods, select the **L2 Authentication** or **L3 Authentication** tab.
   a. Select the authentication type (Stateful 802.1X for L2 Authentication, Captive Portal or VPN Authentication for L3 Authentication)
   b. Select the profile.
   c. Enter the user role for **Default Role**.

8. Click **Save Settings**.

**Configuring Bandwidth Contracts**

Central allows you to configure application specific bandwidth contracts for clients connected to your branch network. By default, bandwidth contracts for applications are applied on a per-role basis.

You can also configure an exclude list to exclude applications or application categories on which a generic user or role bandwidth-contract is not applied. Use the exclude list option to prioritize mission-critical applications over other user traffic. An enterprise may have well known applications such as Microsoft Exchange, SAP, Oracle, accounting and finance applications, and other enterprise resource planning or customer relationship management applications.

Instead of enumerating bandwidth limits for each application individually on a per-user or per-role basis, you can configure a single bandwidth contract to limit all non-mission-critical applications. You can then exclude all mission-critical applications by placing them in an exclude list. This way, mission-critical applications will not be rate-limited.

**Assigning Bandwidth Contracts to User Roles**

To configure bandwidth contract, complete the following steps:

1. From the app selector, click **Gateway Management**.

2. From the group selection filter bar, select the group or device for which you want to configure the role-specific bandwidth contract.

3. Click **Security > Roles**.

4. Select a role name from the **Roles** table and select the **Bandwidth** tab.
5. To add an application or application category to a bandwidth contract, click + under **Per-Application Limits for This Role**.
   a. Select the application bandwidth type from the **Type** drop-down list.
   b. Select the name of the bandwidth contract from the **Name** drop-down list.
   c. Enter values in Kbits or Mbits in the **Upstream** and **Downstream** fields.
   d. Click **Submit**.
6. To add an exception, click + under **Per-Application Limit Exceptions for This Role**.
   a. Enter the name of the application or application category.
   b. Click **Save Settings**.

**Configuring Global Bandwidth Contracts**

To configure bandwidth contract, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or device for which you want to configure global bandwidth contract.
3. Click **Security > Applications**.
4. Expand **Per-Application Limits**.
5. To add an application or application category to a bandwidth contract, click + under **Global Per-Application Limits**. The **Add Application Limit** section is displayed.
6. Select the application bandwidth type from the **Type** drop-down list.
7. Select the name of the bandwidth contract from the **Name** drop-down list.
8. Enter values in Kbits or Mbits in the **Upstream** and **Downstream** fields.
9. Click **Save Settings**.

**Configuring Authentication Profiles**

The Aruba SD Branch solution supports multiple types of authentication methods. Based on your network goals, security requirements, user types, and the type client devices, you can configure a AAA profile with a specific authentication method that is suitable for your Layer 2 and Layer 3 security infrastructure.

For example, you can choose to configure an authentication profile with 802.1X or MAC authentication, and configure an authentication server or server group to allow role assignment to client devices.

See the following topics for more information how to set up authentication sources and profiles.

- Configuring RADIUS Authentication Server on page 94
- Configuring Other External Authentication Servers on page 96
- Configuring Server Groups on page 99
- Creating a AAA Profile on page 99

**Configuring RADIUS Authentication Server**

To configure a RADIUS authentication server, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Security > Auth Servers**.
4. Click + under **All Servers**.
5. Enter a name for the new server.
6. Enter the IP address for the new server.
7. To configure a RADIUS server, select RADIUS as the server type.
8. In the All Servers table, select the name of the new RADIUS server and configure parameters described in Table 26.

Table 26: RADIUS Server Configuration Parameters

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the RADIUS server.</td>
</tr>
<tr>
<td>IP address / hostname</td>
<td>IP address or FQDN of the authentication server. The maximum supported FQDN length is 63 characters. Default: N/A</td>
</tr>
</tbody>
</table>
| Secure radius       | Enable this option to secure communication between the RADIUS server and the Branch Gateway. Specify values for the following parameters:  
|                     | - Secure auth port—The destination port for RADIUS over TLS. By default, the value is set to 2083.  
|                     | - Radsec trusted CA name—The CA certificate that is uploaded as a Trusted CA if the Radsec server uses a certificate signed by a CA.  
|                     | - Radsec server cert name—The server certificate that is uploaded.  
|                     | - Radsec client cert—The client certificate sent to the Radsec server.    |
| Auth port           | Authentication port of this server. The default value is 1812.              |
| Acct port           | Accounting port of this server. The default value is 1813.                  |
| Shared key          | Shared secret between the Branch Gateway and the authentication server. The maximum length is 128 characters. |
| Retype key          | Retype shared secret key.                                                  |
| Timeout             | Maximum time, in seconds, that the Branch Gateway waits before timing out the request and resending it. The default value is 5 seconds. |
| Retransmits         | Maximum number of retries sent to the server by the Branch Gateway before the server is marked as down. The default value is 3. |
| NAS ID              | NAS identifier to use in RADIUS packets.                                   |
| NAS IP              | The NAS IP address to be sent in RADIUS packets from that server.          |
| Use MD5             | Use MD5 hash of cleartext password.                                         |
| Enable              | Enable the use of IPv4 address for the server.                              |
| Lowercase MAC addresses | Send MAC address with lowercase in the authentication and accounting requests to this server. |
| Use IP address for calling station ID | Enables using the IP address as the calling station ID. |
| MAC address delimiter | Send MAC address with the following delimiters in the authentication and accounting requests of this server:  
|                     | - colon: Send MAC address as XX:XX:XX:XX:XX:XX |
Table 26: RADIUS Server Configuration Parameters

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dash:</td>
<td>Send MAC address as XX-XX-XX-XX-XX-XX</td>
</tr>
<tr>
<td>none:</td>
<td>Send MAC address as XXXXXXXXXXXXXX</td>
</tr>
<tr>
<td>oui-nic:</td>
<td>Send MAC address as XXXXXX-YYYYY</td>
</tr>
<tr>
<td>Service-type of FRAMED-USER</td>
<td>Send the service-type as FRAMED-USER instead of LOGIN-USER. For more information, see RADIUS Service-Type Attribute on page 176.</td>
</tr>
<tr>
<td>CPPM credentials</td>
<td>If you are using ClearPass Policy Manager as the RADIUS server, provide user credentials for ClearPass Policy Manager server.</td>
</tr>
</tbody>
</table>

9. Click **Save Settings**.

**Configuring an RFC 3576 Server**

You can configure a RADIUS server to send user disconnect, CoA, and session timeout messages as described in RFC 3576, “Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS).”

To configure an RFC 3576 server, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway device that you want to configure.
3. Click **Security > Auth Servers**.
4. Click + under **All Servers**.
5. Select **RFC 3576** from the **Type** drop-down list.
6. Enter the IP address for the new server.
7. Enter the server authentication key into the **Key** and **Retype key** fields.
8. Click **Save Settings**.

**Configuring Other External Authentication Servers**

This section describes how to configure external authentication servers:

**Configuring an LDAP Server**

To configure an LDAP server, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Security > Auth Servers**.
4. Under **All Servers**, click the + icon to add a new server.
5. Set the **Type** to **Ldap** and click **Submit**.
6. From the **All Servers** list, select the server to configure server parameters.
7. Configure the parameters described in the following table:
Table 27: LDAP Server Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the LDAP server.</td>
</tr>
<tr>
<td>Admin-dn</td>
<td>Distinguished name for the admin user who has read or search privileges across all the entries in the LDAP database (the user does need write privileges, but can search the database, and read attributes of other users in the database).</td>
</tr>
<tr>
<td>Admin-passwd</td>
<td>Password for the admin user.</td>
</tr>
<tr>
<td>Re-type admin-passwd</td>
<td>Retype the password for the admin user for confirmation.</td>
</tr>
<tr>
<td>Allow clear-text</td>
<td>Allows clear text (unencrypted) communication with the LDAP server. Default: disabled</td>
</tr>
<tr>
<td>Auth port</td>
<td>Port number used for authentication. Default: 389</td>
</tr>
<tr>
<td>Base-dn</td>
<td>Distinguished Name of the node that contains the entire user database.</td>
</tr>
<tr>
<td>Filter</td>
<td>A string search for users in the LDAP database. The default filter string is: <strong>(objectclass=*)</strong>.</td>
</tr>
<tr>
<td>Key attribute</td>
<td>A string search for an LDAP server. For Active Directory, the value is sAMAccountName. Default: sAMAccountName</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout period of an LDAP request, in seconds. Default: 20 seconds</td>
</tr>
<tr>
<td>Enable</td>
<td>Option to enable or disable the server. Default: enabled</td>
</tr>
</tbody>
</table>
| Preferred connection type | Preferred type of connection between a Branch Gateway and the LDAP server. The default order of connection type is:  
1. ldap-s  
2. start-tls  
3. clear-text  
The Branch Gateway first attempts to contact the LDAP server using the preferred connection type, and only attempts to use a lower-priority connection type if the first attempt is not successful.  
**NOTE:** If you selected clear-text as the preferred connection type, you must also enable the allow-cleartext option. |
| Maximum number of non-admin connections | Configure the maximum number of non-admin connections to the server. Default: 4                                                             |
| Chase referrals    | Chase referrals anonymously.                                                                                                                 |

4. Select the **Enable** check box to activate the authentication server.
5. Click **Submit**.

**Configuring a TACACS+ Server**

To configure a TACACS+ server, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Click Security > Auth Servers.
4. Under All Servers, click the + icon to add a new server.
5. Set the Type to Tacacs.
6. Enter the server Name and its IP address.
7. Click Submit.
8. From the All Servers list, select the server to configure server parameters.
9. Configure the parameters described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the server.</td>
</tr>
<tr>
<td>Key</td>
<td>Shared secret to authenticate communication between the TACACS+ client and server.</td>
</tr>
<tr>
<td>Retype key</td>
<td>Retype the shared secret for confirmation.</td>
</tr>
<tr>
<td>TCP port</td>
<td>TCP port used by server.</td>
</tr>
<tr>
<td>Retransmits</td>
<td>Maximum number of times a request is retried. Default: 3</td>
</tr>
<tr>
<td>Timeout</td>
<td>Timeout period for TACACS+ requests (in seconds). Default: 20 seconds</td>
</tr>
<tr>
<td>Mode</td>
<td>Option to enables or disable the server. Default: enabled</td>
</tr>
<tr>
<td>Session authorization</td>
<td>Option to enable or disable session authorization. Session authorization turns on the optional authorization session for admin users. Default: disabled</td>
</tr>
</tbody>
</table>

**Configuring a Windows Server**

To configure a Windows server, complete the following steps:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click Security > Auth Servers.
4. Under All Servers, click the + icon to add a new server.
5. Set the Type to Windows.
6. Enter the server Name and its IP address fields, respectively.
7. Click Submit.
8. From the All Servers list, select the server to configure server parameters.
9. Configure the parameters described in the following table:
Table 29: Windows Server Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the server.</td>
</tr>
<tr>
<td>Mode</td>
<td>Option to enable or disable the server. Default: enabled</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>Name of the Windows Domain assigned to the server.</td>
</tr>
</tbody>
</table>

Configuring XML Server

To configure an XML server, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Security > Auth Servers**.
4. Under **All Servers**, click the + icon to add a new server.
5. Set the **Type** to **XML**.
6. Enter the server **IP address**.
7. Enter the server authentication key in the **Key** and **Retype key** fields.
8. Click **Submit**.

Configuring Server Groups

You can create server groups to distinguish authentication servers and for the ease of use. For example, you can configure a server group based on the following criteria:

- User authentication—Servers that authenticate client devices.
- Management authentication—Servers that authenticate management users such as the Branch Gateway admin.
- Accounting—Servers that support accounting.

Accounting is supported only with RADIUS and TACACS servers.

To add a server group:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the group or the SD-WAN Gateway that you want to configure.
3. Click **Security > Auth Servers**.
4. Under **Server**, click the + icon to add a new server.
5. Enter the **Name** of the server group.
6. Click **Submit**.
7. From the **Server Groups** list, select a server group and assign the servers.
8. Click **Save Settings**.

Creating a AAA Profile

To configure a AAA profile:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **Security > AAA Profiles**.
4. Click + to define AAA profile settings.
5. Enter a name for the profile in the **Profile name** field, then configure the AAA profile parameters described in **Table 30**.

**Table 30: AAA Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial role</td>
<td>Assigns role for the unauthenticated users. The default role for unauthenticated users is logon.</td>
</tr>
<tr>
<td>MAC authentication default role</td>
<td>Assigns role after the client device completes MAC authentication. The default role for MAC authentication is the guest user role.</td>
</tr>
<tr>
<td>802.1X authentication default role</td>
<td>Assigns role after the client device completes 802.1X authentication.</td>
</tr>
<tr>
<td>Download role from CPPM</td>
<td>Allows SD-WAN Gateways to download roles from Clear Pass Policy Manager.</td>
</tr>
<tr>
<td>Set username from dhcp option 12</td>
<td>Assigns a user name from DHCP option 12.</td>
</tr>
<tr>
<td>I2 authentication fail through</td>
<td>When MAC authentication fails and if 802.1X authentication method is configured, client devices are assigned roles after they complete 802.1x authentication.</td>
</tr>
<tr>
<td>Multiple server accounting</td>
<td>Enables SD-WAN Gateways to sen accounting messages to all the servers configured in the server group in a sequential order.</td>
</tr>
<tr>
<td>User idle timeout</td>
<td>Configures a session time out value for inactive user sessions. A value of 0, deletes the user immediately after disassociation from the wireless network. Valid range is 30-15300 in multiples of 30 seconds. Specifying a value overrides the global settings configured in the AAA timers.</td>
</tr>
<tr>
<td>RADIUS roaming accounting</td>
<td>Creates an accounting session for each client. The records in the session contain the same set of RADIUS attributes as compared to the timer-based RADIUS Interim-Update Accounting record, except the statistics attributes.</td>
</tr>
<tr>
<td>RADIUS interim accounting</td>
<td>Enables Branch Gateway to send Interim-Update messages with current user statistics to the server at regular intervals. This option is disabled by default, allowing the Branch Gateway to send only start and stop messages to the RADIUS accounting server.</td>
</tr>
<tr>
<td>User derivation rules</td>
<td>Specifies a profile from which the user role or VLAN is derived.</td>
</tr>
<tr>
<td>Device type classification</td>
<td>Allows SD-WAN Gateways to parse user-agent strings and attempt to identify the type of device connecting to the AP.</td>
</tr>
<tr>
<td>Enforce DHCP</td>
<td>Allows clients to obtain IP from DHCP before associating to an AP. Enable this option when you create a user rule that assigns a specific role or VLAN based upon the client device's type.</td>
</tr>
<tr>
<td>PAN firewalls Integration</td>
<td>Requires IP mapping at Palo Alto Networks firewalls.</td>
</tr>
</tbody>
</table>

6. Click **Save Settings**.
7. **Assign AAA policy to VLAN interfaces**.
Applying Policies on SD-WAN Gateway Interfaces

After configuring the firewall policies, ACLs, and AAA profile, you need to apply the appropriate policies on the WAN and LAN interfaces of the SD-WAN Gateways.

For trusted (WAN) interfaces, apply the firewall policies directly. For untrusted (LAN) interfaces, assign AAA profiles (role assignment policies) to the VLANs.

This section includes the following topics that describe how to apply policies on appropriate ports and VLAN interfaces of the SD-WAN Gateways:

- Applying Policies for VLANs on Access Ports on page 101
- Applying Policies for VLANs on Trunk Ports on page 101
- Applying Route ACLs for VLAN Interfaces on page 102
- Assigning AAA profile to VLAN Interfaces for Role Assignment on page 102

Applying Policies for VLANs on Access Ports

Complete the following tasks to apply a firewall policy for a trusted VLAN on access port:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click Security > Apply Policies.
4. To apply a firewall policy, select an access port from Interface table.
5. Under the POLICY column, select the policy to be applied from the drop-down list.

You can apply firewall policies only for trusted VLAN interfaces.

6. Save the changes.

Applying Policies for VLANs on Trunk Ports

Complete the following tasks to apply firewall policies for trusted VLANs on trunk port:

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click Security > Apply Policies.
4. Click Edit Policies from the POLICY column of Interface table for the trunk port on which you want to apply a firewall policy. The Interface > <port-number> table appears which lists all the VLANs configured for the selected trunk port.
5. Select any trusted VLAN from the Interface <port-number> table for which you want to apply a firewall policy.

You can apply firewall policies only for trusted VLAN interfaces.

6. Under the POLICY column, select the policy to be applied from the drop-down list.
7. Save the changes.
8. Repeat step 6 to step 8 to apply policies for multiple VLANs.
Applying Route ACLs for VLAN Interfaces

Complete the following tasks to apply Route ACLs for the configured VLAN interfaces:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click **Security > Apply Policies**.
4. From the **VLANs** table, select the VLAN for which you want to apply a route ACL.
5. Under the **ROUTE ACL** column, select the ACL to be applied from the drop-down list.
6. Save the changes.

Assigning AAA profile to VLAN Interfaces for Role Assignment

Complete the following tasks to apply a AAA profile on a VLAN interface for role assignment:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway or group that you want to configure.
3. Click **Security > Apply Policies**.
4. From the **VLANs** table, select the VLAN for which you want to apply a AAA profile.
5. Under the **ROLE ASSIGNMENT** column, select the AAA profile to be applied to the VLAN interface from the drop-down list.
6. Save the changes.

Configuring SD-WAN Gateways for Certificate-Based Authentication

Certificates provide a secure way of authenticating devices and eliminate the need for less secure password-based authentication. In certificate-based authentication, digital certificates are used to identify a user or device before granting access to a network or application.

Digital certificates use PKI that requires a private-public key pair. A digital certificate is associated with a private key, known only to the certificate owner, and a public key. A certificate encrypted with a private key is decrypted with its public key. For example, party A encrypts its certificate with its private key and sends it to party B. Party B decrypts the certificate with the public key of party A.

Server certificates and the digital certificates issued by a CA validate the identities of servers and clients. For example, when a client connects to a server for the first time, or the first time since its previous certificate has expired or been revoked, the server requests that the client transmit its authentication certificate and verifies it. Clients can also request and verify the authentication certificate of the server.

Branch devices use digital certificates for authenticating a client’s access to user-centric network services such as VPN, the device UI or CLI. Branch Gateways include a server certificate by default for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Adding Certificates to Certificate Store in Central

The **Global Settings > Certificates** page in the Central UI allows you to add certificates to the Central's certificate store. If the certificates are added in the Central's certificate store, you can import or map the certificates required for SD-WAN configuration.
For more information on adding certificates to Central, see [Uploading Certificates on page 22](#).

**Installing Certificates**

To enable branch devices to use certificate-based authentication, you must install the certificates loaded in the Central's certificate store on branch devices.

**Installing Certificates for Server Authentication**

To install certificates for web server, captive portal or VIA server authentication:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device or a device group.
3. Click **System > Certificates**.
4. Click **Server Certificates** and select the required certificate to apply:
5. Under **Web server certificate**, select a certificate for captive portal server authentication
6. Under **VIA server certificate**, select a certificate for VIA server authentication
7. Under **Configure SSL/TLS protocol**, select a security protocol. By default, all TLS protocols are selected.
8. Click **Save Settings**.

**Installing Certificates for VPN Clients**

To install a certificate for VPN client authentication:

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the device or a device group.
3. Click **System > Certificates > Certificates for VPN Clients**.
   - To add a CA certificate, click + in the **CA Certificate Assigned for VPN Clients** table.
   - To add certificate group, click + in the **Certificate Groups for VPN Clients** table.
4. The **Add New Certificate** table is displayed at the bottom of the page.
5. Select the certificate to add from a list of certificates uploaded in the Central's certificate store.
6. Click **Save Settings**.

**Configuring Revocation Checkpoint**

The Certificate Revocation feature enables the SD-WAN Gateways to perform real-time certificate revocation checks using OCSP server, or traditional certificate validation using the CRL client.

OCSP (RFC 2560) is a standard protocol that consists of an OCSP client and an OCSP responder. This protocol determines revocation status of a given digital public-key certificate without downloading the entire CRL.

CRL is the traditional method of checking certificate validity. A CRL provides a list of certificate serial numbers that have been revoked or are no longer valid. CRLs let the verifier check the revocation status of the presented certificate while verifying it. CRLs are limited to 512 entries.

When configured as an OCSP responder, the SD-WAN Gateways provide revocation status information to applications that use CRLs.

---

Ensure that the required OCSP signer and responder certificates are available in the Central certificate store.
Configuring Revocation Checkpoint Using OCSP

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the device or a device group.
3. Click System > Certificates > Revocation Checkpoint.
4. In the Revocation Checkpoint table, click + to add the record for which you want to configure the revocation checkpoint. The Add Revocation Checkpoint section is displayed.
5. From the Name drop-down list, select the CA cert for which you want to configure the revocation check point.
6. Select ocsp from the Revocation method 1 drop-down list as the primary check method.
7. Specify the OCSP server URL in the OCSP URL field.
8. Optionally, select a backup check method (crl) from the Revocation method 2 drop-down list.
   a. Select the Enable OCSP responder check box to configure the SD-WAN Gateway as an OCSP responder for the selected CA certificate.
   b. Select the required OCSP signer certificate from the OCSP signer cert drop-down list.
   c. Select the required OCSP responder certificate from the OCSP responder cert drop-down list.
9. Optionally, you can configure one of the following actions to be taken when the configured server is unreachable:
   - Fail-Over—Fails over to the revocation method 2, if configured.
   - Allow Cert—Allows the certificate.
   - Revoke Cert—Revolves the certificate.
10. Save the changes.

Configuring Revocation Checkpoint Using CRL

Perform the following steps to configure the SD-WAN Gateway as an OCSP responder to provide revocation status information using CRL.

1. From the app selector, click Gateway Management.
2. From the group selection filter bar, select the device or a device group.
3. Click System > Certificates > Revocation Checkpoint.
4. Optionally, if you want to globally enable the OCSP responder service on the SD-WAN Gateway, complete the following tasks:
   a. Click the Enable OCSP responder option to enable the OCSP responder service on the SD-WAN Gateways.
   
   Enable OCSP responder is a global option that enables or disables the OCSP responder service on the SD-WAN Gateways. By default, it is disabled.
   b. Select the OCSP signer certificate to be used to sign OCSP responses for this revocation checkpoint from the OCSP certificates drop-down list.
5. In the Revocation Checkpoint table, click + to add the record for which you want to configure the revocation checkpoint. The Add Revocation Checkpoint section is displayed.
6. From the Name drop-down list, select the CA cert for which you want to configure the revocation check point.
7. Select crl from the Revocation method 1 drop-down list as the primary check method.
8. Select the CRL that you want to use for this revocation checkpoint from the CRL location drop-down list. The CRLs listed are files that have already been imported onto the SD-WAN Gateways.
9. Optionally, select a backup check method as follows:
   a. Select `ocsp` from the Revocation method drop-down list.
   b. Specify the OCSP server URL in the OCSP URL field.
10. If you want to override the global OCSP responder settings and configure specific settings for the selected CA certificate, complete the following tasks:
   c. Select the Enable OCSP responder check box to configure the SD-WAN Gateway as an OCSP responder for the selected CA certificate.
   d. Select the required OCSP signer certificate from the OCSP signer cert drop-down list.
   e. Select the required OCSP responder certificate from the OCSP responder cert drop-down list.
11. Optionally, you can configure one of the following actions to be taken when the configured server is unreachable:
   - Fail-Over—Fails over to the revocation method 2, if configured.
   - Allow Cert—Allows the certificate.
   - Revoke Cert—Revolves the certificate.
12. Save the changes.

**Integrating Zscaler Security Service**

Zscaler is a third-party cloud security service which provides fast and secure connections between users and applications, regardless of device, location, or network. Branch Gateways in the SD Branch can inter-operate with Zscaler to provide a secure remote branch network connectivity with advanced IPS and IDS capabilities to clients.

SD-WAN allows traffic to flow directly between devices in the branch and the internet. This enables the traffic to reach the destination much faster, thereby saving some bandwidth. However, allowing traffic directly between devices in the branch and the internet may introduce security issues.

To secure this traffic, the Aruba Branch Gateway allows you to redirect selected traffic through a cloud-based security platform. The integration between the Aruba Branch Gateways and Zscaler Internet Access (ZIA) allows you to set up a secure connection between the branch networks and one or several cloud-hosted enforcement points. These cloud-hosted enforcement points are called the Zscaler Enforcement Nodes (ZEN).

**Integrating with ZIA**

Integration with ZIA requires configurations on both the Zscaler admin interface as well as in Aruba Central. Complete the following tasks before enabling Zscaler cloud security support for the SD Branch:

1. Locate the FQDN of the ZIA instance to be used.
2. Set up the customer information, VPN credentials, and site information in the ZIA portal.
3. Set up the API key to be used for Zscaler REST APIs.

For more information, refer to the Zscaler documentation.

**Configuring the Branch Gateway for Zscaler Integration**

Before configuring the Branch Gateways, ensure that the devices are capable of resolving (and reaching) the FQDN of the selected ZENs.

Perform the following tasks on the Branch Gateway to enable Zscaler integration:

4. **Configuring IPsec Maps for Zcaler on page 106**
Configuring IPsec Maps for Zscaler

To configure an IPsec map for Zscaler, complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. Select a Branch Gateway or a device group.
3. Click **VPN > Cloud Security**.
4. Ensure that Zscaler is set as the cloud security provider.
5. In the **IPsec Maps** section, click + to open the **Create New Ipsec** section.
6. Enter a name for the IPsec map.
7. Enter a priority number for the IPsec map within a range of 1 to 10,000. A priority value of 1 indicates the highest priority.
8. Select the VLAN ID to which you want apply the IPsec map.
9. Configure a transform set. Transform sets allow you to define a combination of security protocols and algorithms that you can apply to the IPsec traffic flow. To add a transform set:
   a. Click + under **Transforms**.
   b. Specify the encryption methods to use in the transformation set.
   c. Click **Save Settings**.
10. Enter the FQDN of the Zscaler Enforcement Node (ZEN) as **Destination gateway FQDN**.

   Ensure that the destination gateway FQDN value contains the string, `zscaler` in it.

11. Enter the FQDN of the VPN source in **Source FQDN**.
12. Select an uplink VLAN from the Uplink VLAN drop-down list. You can select multiple uplink VLANs to enable load balancing between multiple uplinks.
13. Enter IKE pre-shared secret key that you configured on the ZIA portal.
14. Click **Save Settings**.
15. Save the changes.

Configuring Zscaler Nexthop List

Configure Zscaler nexthop list with Zscaler active and standby IPsec tunnels on different uplinks. For more information on configuring a nexthop list, see **Configuring Next Hop Lists for PBR on page 74**.

Adding Nexthop List to PBR Policy

Add the nexthop list to a PBR policy and ensure that the policy is applied to a user role or VLAN. For more information on adding a nexthop list to a global PBR policy, see **Configuring Policies for PBR on page 73**.

Integrating GlobalProtect Cloud Service

The GlobalProtect cloud service infrastructure is managed by Palo Alto Networks. It is a cloud-based security infrastructure based on next generation security platform. It provides security to remote networks and mobile users by allowing organizations to set up regional, cloud-based firewalls.
SD-WAN Gateways can establish IPsec tunnels to a regional firewall in GlobalProtect cloud service for policy enforcement. These firewalls can run the organization’s security policies to provide traffic inspection and threat prevention capabilities.

**Deploying Palo Alto Networks - GlobalProtect Cloud Service Dashboard**

To deploy the GlobalProtect cloud service dashboard for managing the process of adding locations, users and security policy deployment, complete the following tasks:

1. Ensure to deploy the Panorama VM in your data center.
2. To access the GlobalProtect cloud service dashboard, install the cloud service plug-in on Panorama.

For more information on planning the cloud service infrastructure and service connection, refer to the Palo Alto Network documentation.

**Configuring GlobalProtect Cloud Service for Aruba SD-WAN**

To enable cloud security for your SD branch, configure the following parameters on the GlobalProtect cloud service dashboard:

1. Configure the public IP address or the FQDN of the Aruba SD-WAN Gateways.
2. Use route summary to advertise the branch local subnets to GlobalProtect cloud service.

For more information, refer to the Palo Alto Network documentation.

---

**NOTE**

From the Cloud services dashboard, you can get the IP address of the required cloud service region. This IP address is configured as the peer gateway IP address of the SD-WAN Gateway on ArubaCentral.

**Configuring the Branch Gateways for GlobalProtect Cloud Service Integration**

Before configuring the Branch Gateways, ensure that the devices can reach the IP address of the selected cloud region on the GlobalProtect cloud service.

Perform the following tasks on the Branch Gateway to enable GlobalProtect cloud service integration:

1. Configure IPsec Maps for GlobalProtect Cloud Service on page 107
2. Configuring GlobalProtect Cloud Service Nexthop List on page 108
3. Adding Nexthop List to PBR Policy on page 108

**Configure IPsec Maps for GlobalProtect Cloud Service**

To configure an IPsec map for GlobalProtect cloud service, complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. Select a Branch Gateway or a device group.
3. Click **VPN>Cloud Security**.
4. Ensure that **Palo Alto Networks - GPCS** is set as the cloud security provider.
5. In the **IPsec Maps** section, click + to open the **Create New Ipsec** section.
6. Enter a name for the IPsec map. The allowed character limit is 123.

---

**NOTE**

By default, the IPsec tunnel name created for GlobalProtect cloud service is suffixed with the text, _gpcs._
7. Enter a priority number for the IPsec map within a range of 1 to 10,000. A priority value of 1 indicates the highest priority.
8. Configure a transform set. Transform sets allow you to define a combination of security protocols and algorithms that you can apply to the IPsec traffic flow. To add a transform set:
   a. Click + under **Transforms**.
   b. Specify the encryption methods to use in the transformation set.
   c. Click **Save Settings**.
9. Select one of the following options in **Tunnel source** based on your requirement.
   - **VLAN**—Select a VLAN from the **VLAN** drop-down list.
   - **Uplink VLAN**—Select an uplink VLAN from the **Uplink VLAN** drop-down list. You can select multiple uplink VLANs to enable failover between multiple uplinks.

   Ensure that you assign different priorities for different uplinks in the next-hop list configuration.

10. Specify the FQDN of the tunnel source in the **Source FQDN** field.
11. Specify the IP address of the cloud region elected from the GlobalProtect cloud service dashboard in the **Tunnel destination IP** field.
12. Select one of the following options in the **Representation** type drop-down list:
   - **Text-Based**
   - **Hex-Based**
13. Enter IKE pre-shared secret key that you configured on the GlobalProtect cloud service dashboard in the **IKE shared secret** and **Retype shared secret** fields.
14. Click **Save Settings**.

**Configuring GlobalProtect Cloud Service Nexthop List**

Configure GlobalProtect cloud service nexthop list with active and standby IPsec tunnels on different uplinks. For more information on configuring a nexthop list, see [Configuring Next Hop Lists for PBR on page 74](#).

**Adding Nexthop List to PBR Policy**

Add the nexthop list to a PBR policy and ensure that the policy is applied to a user role or VLAN. For more information on adding a nexthop list to a global PBR policy, see [Configuring Policies for PBR on page 73](#).

**Viewing Configuration Status**

Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The **Configuration Audit** menu in the **Gateway Management** application allows you to view the configuration template errors, configuration sync, and device level configuration overrides.

**Configuration Synchronization Errors**

The devices managed by Central receive the configuration changes from Central. Occasionally, a Central-managed device may fail to receive a configuration change from Central. Such instances are marked as **Failed changes** in the **Configuration Audit** dashboard. If the condition persists, contact ArubaCentral Technical Assistance.
Local Overrides
In Central, devices are assigned to groups that serve as the primary configuration elements. Occasionally, based on the network provisioning requirements, the administrators may need to modify the configuration of a specific device in a group. As these modifications override the configuration settings that the device has inherited from the group, Central marks these as local overrides.

Viewing Configuration Status for a UI Group
On selecting a UI group, the Configuration Audit page displays the options listed in Table 31.

Table 31: Configuration Audit Status for a UI Group

<table>
<thead>
<tr>
<th>Data Pane Content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Changes</td>
<td>Displays the number of devices with configuration sync errors for the selected UI group. To view and resolve the configuration sync errors, click the Failed Config Difference link.</td>
</tr>
</tbody>
</table>
| Local Overrides    | Displays the number of devices with local overrides. To view a complete list of overrides, click the Manage Local Overrides link. The Local Overrides pop-up window opens.  
  - To preserve the overrides, click Close.  
  - To remove the overrides, select the group name with local override, click Remove and click OK. |
| All Devices        | The All Devices table provides the following device information for the selected group:  
  - Name—The name of the device.  
  - Type—The type of the device.  
  - Config Sync—Indicator showing configuration sync errors.  
  - Local Override—Indicator showing configuration overrides for the devices deployed in UI groups. |

Viewing Configuration Status for Devices
On selecting a device assigned to a UI group, the Configuration Audit page displays the options listed in Table 31.

Table 32: Configuration Audit Status for a Device Assigned to a UI Group

<table>
<thead>
<tr>
<th>Data Pane Content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Changes</td>
<td>Displays the number of devices with configuration sync errors for the selected device. To view and resolve the configuration sync errors, click the Failed Config Difference link.</td>
</tr>
</tbody>
</table>
| Local Overrides    | Displays the number of local overrides. To view a complete list of overrides, click the Manage Local Overrides link. The Local Overrides pop-up window opens.  
  - To preserve the overrides, click Close.  
  - To remove the overrides, click Remove, and click OK. |
Configuring SD-WAN Gateways for SNMP-Based Reporting

The SD-WAN Gateways support versions 1, 2c, and 3 of SNMP for reporting purposes. For SNMP-based data collection and management, configure the following SNMP parameters:

**Community String for SNMPv1 and SNMPv2**

Community strings are used to authenticate requests for SNMP versions before version 3. This is needed only when using SNMP v2c and is not needed if using version 3.

**SNMP Trap Receivers**

This table contains information on a trap receiver. This host needs to be running a trap receiver to receive and interpret the traps sent by the Branch Gateway. Configure the following for each host or trap receiver:

- **IP address**: This is the IP address of the new trap receiver.
- **SNMP version**: The SNMP version can be 1, 2c, or 3.
- **Security string**: Choose from the community strings that was created for SNMPv1 and SNMPv2.
- **Type**: Trap or Inform (SNMPv2c or SNMPv3 only)
- **Engine ID**: (SNMPv3 only)
- **UDP port**: This is the port on which the trap receiver is listening for traps. The default is the UDP port number 162. This is optional, and will use the default port number if not modified by the user.
For small and micro branch deployments, Aruba offers an Instant AP-based SD-WAN solution. In a micro branch deployment, you do not require a Branch Gateway. If you have an Instant AP cluster deployed, the Instant AP acting as a Virtual Controller or a master AP can establish secure VPN connections with VPN Concentrators.

Instant APs that are managed by AirWave or Aruba Central can only establish Instant AP-VPN tunnels to a cloud-managed VPN Concentrator.

The following topics describe the various configurations that need to be done on Instant APs and VPN Concentrators for deploying a Micro Branch solution:

- Configuring VPN Concentrators for Micro Branch Solution on page 111
- Configuring Instant APs for Micro Branch Solution on page 111

## Configuring Instant APs for Micro Branch Solution

For a single data center without redundancy, perform the following configuration tasks on the Instant AP:

1. Configure a single VPN using an IPsec tunnel. For more information, see the Configuring IPsec Tunnel section under Managing WLAN Networks in Aruba Central Help Center.
2. Configure a routing profile for split-tunneling of client traffic. For more information, see the Configuring Routing Profiles section under Managing WLAN Networks in Aruba Central Help Center.
3. Configure the Enterprise domains for split-tunneling of DNS traffic from clients. For more information, see the Configuring Enterprise Domains section under Managing WLAN Networks in Aruba Central Help Center.
4. Configure DHCP scope in Distributed, L3 and Centralized, L2 modes. For more information, see the Configuring DHCP Scopes section under Managing WLAN Networks in Aruba Central Help Center.

## Configuring VPN Concentrators for Micro Branch Solution

For a successful Instant AP VPN termination on the SD-WAN Gateway, you need to perform the following configuration tasks on the SD-WAN Gateway:

- Configuring Instant AP VPN Pool for SD-WAN Gateways on page 111
- Configuring Authentication Server on page 112
- Redistributing Branch Subnets on page 113

## Configuring Instant AP VPN Pool for SD-WAN Gateways

The VPN local pool is used to assign an IP Address to the Instant AP after successful XAUTH VPN. Complete the following tasks to configure the Instant AP VPN Pool:

1. From the app selector, click Gateway Management.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click VPN > Dynamic-VPN IP Pool.
4. Click + from the Address Pools table to open the Add New Address Pool section.
5. Enter the following information in the **Add New Address Pool** section to create a new address pool:
   - **Pool name**—Name of the pool
   - **Start address(ipv4)**—The starting IPv4 address of the pool
   - **End address(ipv4)**—The ending IPv4 address of the pool
6. Configure the following additional VPN parameters based on your requirements:
   - **Source-NAT**—Enable this option if the IP addresses of VPN clients must be translated to access the network and select a NAT pool to be used for address translation from the **NAT pool** drop-down list.
   - **VIA SSL fallback**—Enable this option to allow VIA SSL fallback.
   - **Primary DNS server**—Specify the IP address of the Primary DNS Server to be pushed to the VPN client.
   - **Secondary DNS server**—Specify the IP address of the Secondary DNS Server to be pushed to the VPN client.
   - **Primary WINS server**—Specify the IP address of the Primary WINS Server to be pushed to the VPN client.
   - **Secondary WINS server**—Specify the IP address of the Secondary WINS Server to be pushed to the VPN client.
7. Save the changes.

### Configuring Authentication Server

Instant APs identify themselves using the internal TPM certificate, which has the MAC address as the CN. The Micro Branch solution can use the internal server or an external RADIUS server with the database of all the Instant APs, so that the VPN Concentrators accept the incoming connection from the Instant APs.

### Configuring Internal Server

When you use the internal server for authenticating the Instant AP, the VPN Concentrator validates if the Instant AP is in the same user account with valid subscription assigned and automatically whitelists it.

To enable internal server authentication, complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click **Security > L3 Authentication**.
4. Select the **default-iap** profile under **VPN Authentication**.
5. In the **default-iap** profile, select Internal from **Server group**.
6. Save the changes.

### Configuring and Mapping External RADIUS Server

To use an external RADIUS server for authentication, you must configure the server on the VPN Concentrator. To configure an external RADIUS server for authentication, see **Configuring RADIUS Authentication Server on page 94**

---

**Aruba recommends to use the ClearPass Policy Manager as it can download the list of Instant APs owned by the customer from the Activate server to automate the whitelisting process. For information on configuring the ClearPass Policy Manager, see **ClearPass Policy Manager User Guide**.**
Map the configured RADIUS server to the Instant AP VPN server group using the following procedure:

1. From the app selector, click **Gateway Management**.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click **Security > L3 Authentication**.
4. Select the **default-iap** profile under **VPN Authentication**.
5. In the **default-iap** profile, select the configured RADIUS server from **Server group**.
6. Save the changes.

### Redistributing Branch Subnets

Micro branch solution supports learning of branch subnets using dynamic routing protocol. To redistribute the branch networks in L3 mode, complete the following tasks:

1. From the app selector, click **Gateway Management**.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click **Routing > OSPF**.
4. Enable OSPF for routing and configure the area to be used. For more information on configuring OSPF area and other parameters, see [Enabling and Configuring OSPF Parameters on page 72](#).
5. Enable **Redistribute overlay routes**, and then specify a cost for the overlay routes. The cost set here applies only to the routes that are learnt from the SD-WAN Gateways.
6. Save the changes.
7. Click **Interfaces > VLANs** and select the uplink VLAN interface from the **VLAN IDs** table.
8. From the **IPv4** tab, select **Enable OSPF** under **Other Options** and configure the OSPF area to be used.
9. Save the changes.
Chapter 7
Aruba VIA Solution

Aruba VIA refers to Aruba Virtual Intranet Access solution for establishing a virtual private network connection. VIA has two primary purposes:

- to provide secure corporate access to employee laptops and smartphones from anywhere
- to provide ease-of-use for the end users and network administrators

The ease-of-use is what differentiates VIA from other VPN solutions. VIA offers a zero-touch end-user experience and removes the complexity that is associated with configuring VPN clients on end-user devices. VIA provides not only provides ease-of-use for end users but also simplifies configuration and management for the IT team.

The VIA client that is available for Microsoft Windows computers (Windows XP, Vista, and Windows 7), Apple Mac OS X, and Apple iOS devices is a hybrid Internet Protocol Security (IPsec)/ Secure Sockets Layer (SSL) VPN client. If the user is connected to an untrusted network, the VIA client scans network connections and automatically establishes a secure connection back to the corporate network. Some additional features include Content Security Services (CSS), single-logon, SSL fallback when IPsec is blocked, and the ability to configure Wireless Local Area Network (WLAN) settings using the supplicant provided by the operating system.

Configuring VIA

Complete the following tasks to configure an Aruba VIA solution:

1. Configure VPN IP Pool
2. Define the shared secret for the VPN clients.
3. Configure the VIA user-role
4. Configure a VIA server group for authenticating VIA users
5. Configure the VIA authentication profile
6. Configure the VIA web authentication
7. Load and apply server or CA certificates
8. Configure the VIA connection profile
9. Attach the VIA connection profile to the user role
10. Upload the VIA installer to the VPN Concentrator or an external server

Configuring VPN IP Pool

The first step to configure VIA is to create a VPN IP Pool on the VPN Concentrator. To configure the VPN IP Pool, complete the following steps:

1. From the app selector, click Gateway Management.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click VPN > Dynamic-VPN IP Pool.
4. Click + from the Address Pools table to open the Add New Address Pool section.
5. Enter the following information in the Add New Address Pool section to create a new address pool:
   - Pool name—Name of the pool
   - Start address(ipv4)—The starting IPv4 address of the pool
- **End address(ipv4)**—The ending IPv4 address of the pool
6. Configure the following additional VPN parameters based on your requirements:
- **Source-NAT**—Enable this option if the IP addresses of VPN clients must be translated to access the network and select a NAT pool to be used for address translation from the **NAT pool** drop-down list.
- **VIA SSL fallback**—Enable this option to allow VIA SSL fallback.
- **Primary DNS server**—Specify the IP address of the Primary DNS Server to be pushed to the VPN client.
- **Secondary DNS server**—Specify the IP address of the Secondary DNS Server to be pushed to the VPN client.
- **Primary WINS server**—Specify the IP address of the Primary WINS Server to be pushed to the VPN client.
- **Secondary WINS server**—Specify the IP address of the Secondary WINS Server to be pushed to the VPN client.
7. Save the changes.

Ensure that the configured IP addresses are reachable.

### Defining IKEv1 Shared Secret

If you are configuring a VPN to support IKEv1 and clients using pre-shared keys, you can configure a global IKE key or IKE key for each subnet. Make sure that this key matches the key on the VPN client.

1. From the app selector, click **Gateway Management**.
2. Select a group to which VPN Concentrators are provisioned.
3. Click **VPN > Shared Secrets**.
4. In the **IKE Shared Secrets for VPN Clients** table, click + to open the **Create IKE Group** section.
5. Enter the **Subnet** and **Subnet** mask. To make the IKE key global, enter 0.0.0.0 for both values.
6. Select the **Representation type** from the drop-down list.
7. Enter a value for **Shared key** and repeat it in the **Retype shared key** field.

### Configuring VIA User Role

The VIA user role is the role that is assigned to the users who successfully authenticate through their VIA client. The user role defines the access rights of the users that connect using VIA. Aruba recommends that network administrators configure custom user roles that depict the network access policy of their respective organizations. You can also use the predefined **default-via-role** and edit it according to your requirements. For more information on creating user roles, see the [Configuring User Roles on page 91](#).

### Creating VIA Server Group for Authenticating VIA Users

A server group is a collection of servers that are used for authentication. By default, the first server on the list is used for authentication unless it is unavailable. A server group can have different types of authentication servers. For example, you can create a server group that uses an LDAP server as a backup for a RADIUS server.

To configure a custom server group for authenticating VIA users, see the [Configuring Server Groups on page 99](#).
Configuring VIA Authentication Profile

The VIA authentication profile defines the authentication server group used and the default role assigned to the authenticated users. Multiple authentication profiles can be created. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile.

The VIA authentication profile is a critical part of VIA configuration and it is used for these purposes:

- To determine the authentication server for the XAUTH authentication phase of IKEv1 and EAP authentications of IKEv2.
- To determine the authentication server for the VIA web authentication. The VIA authentication profile is an integral part of the VIA web authentication, which determines the authentication server used for VIA bootstrap process and for authenticating users on the VIA installer download page of the VPN Concentrator. For more information on VIA web authentication see Configuring VIA Web Authentication.

To configure a VIA authentication profile, complete the following steps:

1. From the app selector, click Gateway Management.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click Security > L3 Authentication.
4. Select VIA Authentication.
5. Click + to create a new VIA authentication profile or select an existing profile. You can also use the predefined default VIA authentication profile.
6. After selecting the required profile, select the role that you defined for the VIA users in the Default role field. For more information on configuring the other parameters for this profile, see Table 33.
7. Select the required server group for authentication from the appropriate server group option under the selected profile. The server group options are RADIUS Accounting Server Group, RFC 3576 Server, and Server Group. Optionally you can configure the following options for the selected server group:
   - Fail through—Enables the fail through option for the server group.
   - Load balance—Enables load balancing among the servers for authentication requests.
8. Save the changes.

Table 33: VIA Authentication Profile Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Role</td>
<td>Select the role that you want to be assigned as the default role for the client when authenticating using this profile. By default, the default-via-role is assigned.</td>
</tr>
<tr>
<td>Max Authentication failures</td>
<td>Maximum number of authentication failures allowed for the client. Allowed range is 1-10 and the default value is 0.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the authentication profile.</td>
</tr>
<tr>
<td>Check certificate common name against AAA server</td>
<td>Select this option to check for certificate common name against the AAA server. Default: enabled.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client-certificate based authentication for VIA Profile download</td>
<td>Select this option to enable client-certificate based authentication for VIA Profile download. By default, this is disabled.</td>
</tr>
<tr>
<td>Authentication protocol</td>
<td>Select the authentication protocol to be used. The default value is PAP.</td>
</tr>
<tr>
<td>Download Role from CPPM</td>
<td>Select this option to download the default role from ClearPass Policy Manager, if the default role is not defined.</td>
</tr>
</tbody>
</table>

**Configuring VIA Web Authentication**

The VIA web authentication is a list of VIA authentication profiles. The web authentication list allows the users to login to the VIA download page `<https://<VPN Concentrator IP address>/via>` to download the VIA client. To successfully login to the VIA download page, the users must authenticate successfully against the VIA authentication profile in the list. If more than one VIA authentication profile is configured in the web authentication list, the users can view the list and select one authentication profile before authenticating to the VIA installer download page.

The web authentication list is also used during the initial user authentication process that determines the VIA user role. The Branch Gateway has a default web authentication list to which multiple VIA authentication profiles can be added. Additional VIA web authentication lists cannot be created.

To configure the VIA web authentication list, add one or more VIA authentication profiles to the default web authentication list and order them according to the priority. Configuring more than one VIA authentication profile in the VIA web authentication list allows the users to use the backup authentication server when the primary server becomes unavailable temporarily.

To configure the VIA web authentication profile, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click **Security > L3 Authentication**.
4. Select **VIA Web Authentication > default**.
5. Click + to add a VIA authentication profile in the **VIA authentication profiles** table.
6. Save the changes.

**Loading and Applying VIA Certificates**

VIA configuration requires server certificates for both HTTPS as well as VPN. It also requires CA certificates if certificate-based authentication is used on the client devices.

To load and apply VIA certificates, complete the following tasks:

1. Load the required VIA certificates to the certificates store in Aruba Central. For more information on loading certificates using Aruba Central, see [Aruba Central Help Center](https://www.arubacentral.com/help-center/).
2. Configure the VPN Concentrator to use the required VIA certificate. For more information on configuring certificates for a device, see [Configuring SD-WAN Gateways for Certificate-Based Authentication on page 102](https://www.arubacentral.com/). 

**Configuring VIA Connection Profile**

The VIA connection profile is a collection of all the configurations required by a VIA client. The VIA connection
profile contains all the details required for the VIA client to establish a secure IPsec connection to the VPN Concentrator. A VIA connection profile also defines other optional parameters. Such optional parameters can be client auto-login, split-tunnel settings, and Content Security Services (CSS) settings. You can configure multiple VIA connection profiles.

A VIA connection profile is always associated to a user role, and all users that belong to that role use the configured settings. When a user authenticates successfully to a server in an authentication profile, the VIA client downloads the VIA connection profile that is attached to the role assigned to that user.

Table 34 summarizes the various parameters of a VIA connection profile.

To configure a VIA connection profile, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click **Security > L3 Authentication**.
4. Select **VIA Connection**.
5. Click + to create a new VIA connection profile or select an existing profile. You can also use the predefined default VIA connection profile.
6. After selecting the required profile, configure the various VIA connection profile parameters as described in Table 34.
7. Save the changes.

| Table 34: VIA Connection Profile Parameters |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| VIA servers                        | This parameter has the following fields:  
  ■ **Addr**—Add the public IP or DNS hostname of the VPN Concentrator. This is the host name or IP address that the users enter as the remote server information on the VIA client.  
  ■ **Internal IP**—Add the IP address of any of the internal VLAN interfaces of the VPN Concentrator. This IP address should not be reachable from the public Internet. The VIA client uses this IP address to determine whether or not the user is connected to a trusted network.  
  ■ **Description**—Add a human-readable description of the VIA server.  
  NOTE: More than one VIA server can be added to the list. |
| Client auto-login                  | Enabling client auto-login makes the VIA client detect untrusted network and connect automatically. If you disable auto-login, VIA stays idle after it comes up and the user has to manually click **Connect** to establish a VPN connection even though an untrusted network is detected.  
  Default: enabled |
| VIA authentication profiles to provision | This VIA authentication profile is used to determine the authentication server used for the IKE authentication process. If more than one VIA authentication profile is added to this list, the users can choose the VIA authentication profile to be used during IKE authentication. If no VIA authentication profile is defined, the users are authenticated against the server group that is specified by the default VIA authentication profile (predefined). |
| Allow client to auto-upgrade       | This parameter allows the VIA client to automatically upgrade if a newer version of VIA is available on the VPN Concentrator. By default this is enabled. |
| VIA tunneled networks              | When split-tunneling is enabled, the VIA client tunnels traffic to the VPN Concentrator for all the network destinations (IP address and netmask) listed in this parameter. All other network destinations are bridged appropriately on the client.  
  If split-tunnel is disabled, all the traffic is tunneled to the VPN Concentrator irrespective of the destination. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable split tunneling</td>
<td>When enabled, all traffic to the VIA tunneled networks goes through the VPN Concentrator and the rest is bridged directly on the client. If split-tunnel is disabled, all the traffic is tunneled to the VPN Concentrator irrespective of the destination.</td>
</tr>
<tr>
<td>Allow client-side logging</td>
<td>This parameter determines whether client side logging is allowed or not. If enabled, VIA client collects logs that can be sent to the support email address for troubleshooting. Default: Enabled</td>
</tr>
<tr>
<td>VIA IKEv2 Policy</td>
<td>This IKE policy is used for IKEv2 connections by the VIA client. Remember that IKEv2 using PSK is not supported for VIA. For more information on configuring IKE policies, see Configuring IKE Policies.</td>
</tr>
<tr>
<td>VIA IKE Policy</td>
<td>This IKE policy is used for IKEv1 connections by the VIA client. This policy determines whether IKEv1 phase 1 authentication uses PSK or certificates. For more information on configuring IKE policies, see Configuring IKE Policies.</td>
</tr>
<tr>
<td>Use windows credentials</td>
<td>This parameter determines whether the Windows credentials are used automatically to login to VIA. If enabled, the single sign-on feature can be utilized by remote users to connect to internal resources. Default: Enabled</td>
</tr>
<tr>
<td>Enable IKEv2</td>
<td>This parameter enables or disables IKEv2.</td>
</tr>
<tr>
<td>Use suite B cryptography</td>
<td>This parameter enables or disables Suite B cryptographic methods.</td>
</tr>
</tbody>
</table>
| IKEv2 authentication method     | This parameter indicates the IKEv2 client authentication method. It can be one of these settings: \[\]
|                                 | I user-cert \[\]
|                                 | I EAP-TLS \[\]
|                                 | I EAP-MSCHAPv2 \[\]
<p>|                                 | Remember that EAP termination on the VPN Concentrator is not supported.                                                                                                                              |
| VIA IPSec v2 crypto map         | This IPSec map is used by IKEv2 VIA client to connect to the VPN Concentrator.                                                                                                                      |
| VIA IPSec crypto map            | This IPSec map is used by IKEv1 VIA client to connect to the VPN Concentrator.                                                                                                                      |
| Allow user to save passwords    | This parameter determines whether the users can save the passwords entered in VIA or not. If this is enabled, the user credentials that were able to successfully establish a VIA connection are saved securely until VIA is uninstalled or until IKE authentication fails with stored credentials. If this option is disabled, VIA prompts for credentials every time it establishes a connection. If secure tokens such as the RSA tokens are used for authentication, disable this option to prompt the user for a password/token for each connection attempt. By default, this is enabled. |
| Enable supplicant               | This parameter enables the supplicant mode.                                                                                                                                                           |
| Enable FIPS module              | This parameter enables the VIA FIPS module.                                                                                                                                                          |
| Auto-launch supplicant         | This parameter automatically connects to the configured WLAN network.                                                                                                                                  |
| Lockdown all settings           | This parameter locks all the configuration options available on the end-user VIA client. If this option is enabled, a VIA user can only connect, disconnect or send logs. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Diagnostics such as traceroute and ping can still be used, but no settings can be changed. <strong>NOTE:</strong> This option is available in VIA 2.1 and later versions.</td>
</tr>
<tr>
<td>Domain suffix in VIA authentication</td>
<td>This parameter enables domain suffix in VIA authentication.</td>
</tr>
<tr>
<td>Enable Controllers load balance</td>
<td>This parameter enables load balancing of VIA clients by randomly choosing a VPN Concentrator from the list of available VIA VPN Concentrators that can be used for connection. This feature does not take the existing load of the VPN Concentrator into account. <strong>NOTE:</strong> This option is available in VIA 2.1 and later versions.</td>
</tr>
<tr>
<td>Enable domain pre-connect</td>
<td>This parameter enables pre-connection to the domain. By default, this is enabled.</td>
</tr>
<tr>
<td>VIA banner message reappearance timeout(minutes)</td>
<td>This parameter configures the timeout value in minutes for reappearance of VIA login banner message. The default value is 60 minutes.</td>
</tr>
<tr>
<td>VIA client network mask</td>
<td>This network mask is set on the client after the VPN connection is established. The default value is 255.255.255.255.</td>
</tr>
<tr>
<td>Validate server certificate</td>
<td>If enabled, the VIA client validates the server certificate presented by the VPN Concentrator during the IPsec process. Remember that to validate the server certificate, the CA that signed the VPN Concentrator certificate should be a trusted CA in the client certificate store. By default, this is enabled.</td>
</tr>
<tr>
<td>VIA client DNS suffix list</td>
<td>This is the DNS suffix that is set on the client after the VPN connection is established.</td>
</tr>
<tr>
<td>OCSP cert verification enabled</td>
<td>This parameter enables OCSP certificate verification.</td>
</tr>
<tr>
<td>In EAP/IKE, action taken when OCSP cert verification result is unknown</td>
<td>This parameter accepts the certificate when OCSP certificate verification result is unknown for EAP/IKEs.</td>
</tr>
<tr>
<td>VIA domain name profile</td>
<td>This parameter allows you to add VIA domain name profiles.</td>
</tr>
<tr>
<td>Destination traffic to be blocked</td>
<td>This parameter allows you to configure the IP address and netmask of the destination traffic for blocking.</td>
</tr>
<tr>
<td>Block-destination-traffic-selector (on/off)</td>
<td>This parameter enables or disables the blocking of destination traffic.</td>
</tr>
<tr>
<td>VIA max session timeout</td>
<td>This parameter defines the maximum time, in minutes, allowed before the VIA session is disconnected. Default: 1440 min</td>
</tr>
<tr>
<td>VIA logon script</td>
<td>This parameter specifies the name of the logon script that must be executed after VIA establishes a secure connection. The logon script must reside on the client computer.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VIA logoff script</td>
<td>This parameter specifies the name of the logoff script that must be executed after VIA tears down a secure connection. The logoff script must reside on the client computer.</td>
</tr>
<tr>
<td>VIA support e-mail address</td>
<td>This is the support email address to which VIA users send client logs using the VIA client. For information on sending VIA logs using the VIA client, see Chapter 8: Establishing VIA connection.</td>
</tr>
<tr>
<td>Maximum reconnection attempts</td>
<td>This parameter defines the maximum reconnection attempts by the VIA client. If the reconnection attempt is exceeded, the VIA client becomes idle. However, if the connection attempt fails due to an IKE authentication failure error, then the user is prompted to reenter username and password. Default: 3</td>
</tr>
<tr>
<td>VIA external download URL</td>
<td>The VIA installer can be hosted on an external server other than the VPN Concentrator for download by the VIA client during VIA upgrades and by the end users. If the VIA installer is hosted on an external server, this parameter should be configured to redirect the VIA clients to the external URL for the upgrade process. If this parameter is not configured, the VIA clients automatically go to https://&lt;VPN Concentrator IP address or FQDN &gt;/via for upgrades.</td>
</tr>
<tr>
<td>Allow user to disconnect VIA</td>
<td>This feature determines whether the users can disconnect VIA or not. Remember that a user with administrative rights to a laptop can always uninstall VIA or disable the service running on the laptop. For users with restricted access to the laptops, disabling this feature ensures that users cannot disconnect VIA. By default, this is enabled.</td>
</tr>
<tr>
<td>Content security gateway URL</td>
<td>When split-tunnel mode is enabled, traffic to external websites is inspected by the CSS.</td>
</tr>
<tr>
<td>Comma separated list of HTTP ports to be inspected (apart from default port 80)</td>
<td>Traffic to the specified list of ports is verified by the CSS provider.</td>
</tr>
<tr>
<td>Certificate criteria</td>
<td>Certificate criteria expressed in key-value pairs where keys can be certificate attributes, or certificate OIDs. Multiple key-value pairs can be combined with semi-colon.</td>
</tr>
<tr>
<td>Enable content security services</td>
<td>This parameter enables the CSS. The CSS requires the CSS licenses.</td>
</tr>
<tr>
<td>Keep VIA window minimized</td>
<td>When this feature is enabled, the VIA client is minimized to the system tray during the connection phase. This feature is applicable only for VIA clients installed on Microsoft Windows laptops. Default: disabled</td>
</tr>
<tr>
<td>Block traffic until VPN tunnel is up</td>
<td>This parameter allows blocking of traffic until VPN tunnel is up.</td>
</tr>
<tr>
<td>Block traffic rules</td>
<td>This parameter configures the VIA whitelist traffic rules. Specify the IP address, netmask and description for the traffic rules.</td>
</tr>
<tr>
<td>User idle timeout</td>
<td>User idle timeout value. Allowed range is 30-15300 seconds in multiples of 30 seconds.</td>
</tr>
<tr>
<td>VIA client mtu value</td>
<td>MTU value for the VIA client. Allowed range is 576-5120 bytes. The default value is 1452 bytes.</td>
</tr>
</tbody>
</table>
Attaching the VIA Connection Profile to User Role

VIA connection profile that the VIA client has to download should be attached to the user role to be assigned to the user. When a user goes through the authentication phase it is placed on a role which has a certain connection profile associated. Suppose, the users authenticating to the VIA authentication profile are assigned the default-via-role. To assign a specific connection profile to these users, attach the connection profile to the default-via-role.

To attach the VIA connection profile to a user role, complete the following steps:

1. From the app selector, click Gateway Management.
2. Select a group to which the VPN Concentrators are provisioned.
3. Click Security > Roles.
4. Select the role to which you want to associate a VIA connection profile and select the More tab.
5. Expand VPN and select the required VIA connection profile from the VIA connection profile drop-down list.
6. Save the changes.

Uploading VIA Installer to VPN Concentrator

Separate VIA installers are needed for Apple Mac OS X, Apple iOS devices, and Windows 32-bit and 64-bit operating systems. The Apple iOS VIA installer is available in the Apple App store. All other VIA installers are available at the Aruba support site and they should be uploaded to the VPN Concentrator or an external hosting server for download by the users. If the VPN Concentrator is used to host the VIA images, the VPN Concentrator automatically detects the operating system of the device that is connecting to the VIA download page. The VPN Concentrator learns the parameters of the web browser used to connect to the VIA download page to determine the operating system. After the users login to the VIA download page, the VPN Concentrator presents the appropriate VIA installer image. After the initial installation, the VIA clients are capable of automatically upgrading their image (depends on VIA connection profile setting). If the network administrator uploads a new version of VIA installer to the VPN Concentrator or to an external server (indicated by the VIA external download URL parameter of the VIA connection profile), the VIA clients automatically upgrade their image.
After you set up the data center and branch sites and configure devices deployed in the SD-Branch, the **Monitoring & Reports** application allows you to view the branch health and monitor the WAN uplink and gateway performance. This application also provides a dashboard for analyzing application usage by the clients connected in the WAN network. You can also view the branch topology, configure alerts, and create reports.

For more information on details shown on the monitoring dashboard and **Monitoring & Reports** application options, see the following topics:

- [Gateway Details](#)
- [Network Health](#)
- [Site Health](#)
- [Topology](#)
- [Gateway Alerts](#)
- [Gateway Reports](#)

**Gateway Details**

After you onboard and configure the gateways, you can view the branch health, monitor the WAN uplink, and view gateway performance from the **Gateways** page.

From the app selector, click **Monitoring & Reports** and go to **Network Overview > Gateways**. The **Gateways** page displays the following details for the gateways that are deployed in the WAN network.
**Table 35: Gateways Page**

<table>
<thead>
<tr>
<th>Data Pane Content</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Filter Bar**     | **Group Filter**—From the group selection filter bar, select the group or the gateway device that you want to monitor.  
**Temporal Filter**—By default, the graphs on the dashboard are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **3 Hours** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month, and 3 months. |
| **Usage**          | **NOTE:** If you select All Devices from the Group Filter, aggregate data is displayed. If you select a particular group, label, site, or device, data pertaining to your selection is displayed. Displays the following graphs:  
  ■ **Usage**—Displays the incoming and outgoing data traffic in the WAN network.  
  ■ **WAN Compression**—The graph displays the data packet compression statistics for the WAN network. You can view the compressed, uncompressed, and saved bandwidth. By default, traffic between the Branch Gateway and VPN Concentrator is subject to compression.  
  ■ **WAN Tag Provider Distribution**—Displays the number of online and offline uplinks per WAN provider.  
  ■ **WAN Type Provider Distribution**—Displays the number of online and offline uplinks per WAN circuit type.  
  ■ **WAN Transport Health**—Displays the Mean Opinion Score (MOS) score trends for each uplink for the selected time range. The uplink health trend is plotted using health indicators such as Good, Fair, and Poor. |
| **List of Online Gateways** | Displays the list of gateways that is reachable from Central. |
| **List of Offline Gateways** | Displays the list of gateways that is unreachable from Central. |
| **Distribution**    | Displays the following charts:  
  ■ **Model Distribution**—Displays the percentage of gateway hardware platforms in the network.  
  ■ **Firmware Distribution**—Displays the percentage of firmware versions running on gateways that are deployed in the WAN network. |
| **Gateways table**  | Select either List of Online Gateways or List of Offline Gateways to view the details of gateways provisioned in Central.  
  ■ **Name**—Name of the gateway.  
  ■ **MAC Address**—MAC address of the gateway.  
  ■ **IP Address**—IP address of the gateway.  
  ■ **Group**—Group to which the gateway is assigned.  
  ■ **Site Name**—Name of the site in which the gateway is deployed.  
  ■ **Labels**—Name of the label. Clicking the label name opens the per label details.  
  ■ **Serial Number**—Serial number of the gateway.  
  ■ **Model**—Hardware model of the gateway. |

**Gateway Details**

To view the details of a gateway:

1. On the Gateways page, click **List of Online Gateways**. The list of gateways connected in Central are displayed.

2. Click the gateway link for which you want to see the details. A dashboard showing the details of the selected gateway opens.
Table 36: Gateway Details Page

<table>
<thead>
<tr>
<th>Data Pane Content</th>
<th>Description</th>
</tr>
</thead>
</table>
| Actions           | Displays the following options:  
  - **Reboot**—Reboots the gateway.  
  - **Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.  
  **NOTE:** If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy y and Paste functions available under the menu options in the web browser.  
  - **Troubleshoot**—Opens the Troubleshooting page in a new browser window. Allows administrators and users with read-write permissions to run troubleshooting or diagnostics commands on the selected Branch Gateway. For more information, see the Troubleshooting Devices section in the Aruba Central Help Center. |
| Tabs              | The Gateway Details page has the following tabs:  
  - **Summary**  
  - **WAN**  
  - **LAN**  
  - **Tunnel**  
  - **Path Steering**  
  - **Alerts**  
  - **Routes**  
  - **Applications**  
  **NOTE:** If the gateway is provisioned as a VPN Concentrator, the **WAN**, **Path Steering**, and **Applications** tabs are disabled.  
  **NOTE:** In the tab bar, the **WAN** and **LAN** tabs display the number of active ports and the total number of ports, and the **Tunnel** tab displays the number of active tunnels and the total number of tunnels. |

Summary Tab

The Summary dashboard provides gateway device details, WAN availability and performance information, and the list of top applications. The Summary tab displays the following details:

Table 37: Summary Tab

<table>
<thead>
<tr>
<th>Pane</th>
<th>Applicability</th>
</tr>
</thead>
</table>
| **Device Info**  | Branch Gateway  
  - **VPN Concentrator** |
| **WAN Availability** | Branch Gateway |
| **VPN Hub Availability** | Branch Gateway |
| **Aggr. WAN Usage** | Branch Gateway |
| **Aggr. WAN Compression** | Branch Gateway |
| **Application Usage** | Branch Gateway |
| **Application Web Reputation** | Branch Gateway |
Device Info
Displays the gateway device details. From the drop-down list, select **Summary** to view the following details:
- **Name**—Name of the gateway.
- **Management Conn Status**—Status of connection to Central. Status is displayed as a percentage.
- **Redundancy Peer**—Displays the redundant gateway. Click the link to view the redundant gateway details. See the Setting up Redundant Gateways for High Availability section in the *Aruba Central Help Center*.
- **MAC Address**—MAC address of the gateway.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the Branch Gateway consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **Group**—Name of the group to which the gateway belongs.
- **Current F/W version**—Firmware version running on the gateway.
- **IP address**—IP address of the gateway.

From the drop-down list, select **All Details** to view the following additional details:
- **Serial**—Serial number of the gateway.
- **Model**—Hardware model of the gateway.
- **Labels**—Labels attached to the gateway.
- **Config Sync Status**—Status of the configuration sync.
- **Last Reboot Reason**—Reason for the last reboot.
- **Location**—Physical location of the gateway.

**WAN Availability**
Provides a graphical representation of the Branch Gateway’s WAN uplink availability. The graph displays each WAN uplink availability for the selected time range. Availability is determined by default gateway, monitored IP, and data VPN Concentrator reachability.

**VPN Hub Availability**
Provides a graphical representation of the VPN Concentrator’s tunnel availability. Availability is determined by the probe settings configured using the **Health Check** option.

**Aggr. WAN Usage**
Displays the Branch Gateway’s aggregate inbound and outbound traffic usage by WAN interface. Select one of the following options from the drop-down list:
- **All Traffic**
- **Internet vs. VPN**

**Aggr. WAN Compression**
Displays the aggregate WAN compression details across all uplinks. The average bandwidth savings is displayed as a percentage. The compressed and uncompressed bandwidth is displayed as vertical grouped bar graphs. For more information about the process to enable data compression, see the Configuring Uplink Interfaces section in the *Aruba Central Help Center*.

**Application Usage**
If Deep Packet Inspection (in AppRF application) is enabled on the Branch Gateway, the **Application Usage** graph displays top N applications based on total bandwidth usage. Apart from the top N, the rest of the applications are grouped under the **Others** category.
Application Web Reputation

If website URL filtering is enabled on the Branch Gateway, the **Application Web Reputation** graph displays the reputation of the web content according to the reputation score configured.

**WAN Tab**

If the gateway is provisioned as a VPN Concentrator, the **WAN** tab is disabled.

If the gateway is provisioned as a Branch Gateway, the **WAN** tab displays the following details:

- **Port Status**—Displays the WAN port status. Click a WAN port for more details.
- **WAN Interfaces Summary**—The table lists the WAN interfaces and provides the total number of WAN interfaces. Displays the summary of WAN uplinks. The following details are displayed for the port:
  - **Port**—Port number.
  - **Type**—WAN interface type.
  - **VLAN**—VLAN ID.
  - **WAN Status**—WAN port status.
  - **Provider Tag**—Service provider uplink tag.
  - **Provider Type**—Service provider uplink type.
  - **Speed**—Uplink speed.
  - **Duplex**—Duplex type.
  - **Oper. State**—Operational status.
  - **IP**—IP address.
- **WAN Interface Details**—In the **WAN Interfaces Summary** table, click any port number to view the WAN interface details. The following details are displayed for the WAN interface:
  - **Status**—Operational status.
  - **Provider Tag**—Service provider uplink tag.
  - **Provider Type**—Service provider uplink type.
  - **Private IP**—Private IP address.
  - **Public IP**—Public IP address.
  - **Default Gateway**—Default gateway.
  - **Avg. MOS**—Indicates the transport health based on active monitoring probes. The field displays the average MOS score of all VPN probes.
- **Availability**—Provides a graphical representation of the selected WAN interface's availability based on reachability. The graph shows the selected WAN port's ability to reach its default gateway, monitored IP, and VPN Concentrator.
- **Throughput**—Provides a graphical representation of the selected WAN interface's throughput. The graph displays the WAN interface's transmit and receive performance in bps.
- **Usage**—Displays the inbound and outbound traffic usage.
- **WAN Compression**—Displays the WAN compression details. The average bandwidth savings is displayed as a percentage.
- **Performance**—Displays the following details for the uplink:
  - **Latency**—Displays the latency in microseconds.
  - **Jitter**—Displays the jitter in microseconds.
  - **Packet Loss**—Displays the packet loss in percentage terms.
- **MOS Score**—Displays the transport health score. The range is from 1 to 5.
- **Port Details of Gigabit Ethernet**—Displays the Gigabit Ethernet port details.
  From the **Port Statistics** drop-down list, select **Packets** to view the inbound and outbound packets for the following:
  - Unicast
  - Multicast
  - Broadcast
  From the **Port Statistics** drop-down list, select **Errors** to view the following:
  - CRC Errors
  - Error Frames
  - Collisions

**LAN Tab**

The **LAN** tab displays the following details:
- **Port Status**— Displays the LAN port status. Click a LAN port for more details.
- **LAN Interfaces Summary**—The table lists the LAN interfaces and provides the total number of LAN interfaces. Displays the summary of LAN interfaces. The following details are displayed for the port:
  - **Port**—Port number.
  - **Description**—Description of the LAN interface.
  - **Admin State**—Administrative state of the LAN interface.
  - **Oper. State**—Operational state of the LAN interface.
  - **Speed**—Speed.
  - **Duplex**—Duplex type.
  - **VLANs**—Range of VLANs.
  - **MTU**—MTU value.
- **VLAN Interfaces Summary**—The table lists the VLAN interfaces and provides the total number of VLAN interfaces. Displays the summary of LAN interfaces. The following details are displayed:
  - **VLAN ID**—VLAN ID number.
  - **Description**—Description of the VLAN.
  - **Admin State**—Administrative state of VLAN interface.
  - **Oper. State**—Operational state of the VLAN interface.
  - **Addressing Mode**—Type of addressing mode.
  - **IP Address**—IP address.
- **DHCP Pools**—The table lists the DHCP pools and total number of DHCP pools. Displays the summary of DHCP pools. The following details are displayed:
  - **VLAN**—VLAN ID number.
  - **Client Subnet**—IP address of the client subnet.
  - **Free**—Percentage of free IP addresses in the DHCP pool.
- **Active Leases**—The table lists the active leases and the total number of active leases. Displays the summary of active leases. The following details are displayed:
  - **IP Address**—IP address of the client subnet.
  - **MAC Address**—MAC address of the client.
- **Start Date**—Start date and time of the lease.
- **End Date**—End date and time of the lease.
- **Remaining**—Remaining time for the lease to expire.

**Port Details of Gigabit Ethernet**—Displays the Gigabit Ethernet port details. The following details are displayed:
- **Port**—Gigabit Ethernet port number.
- **Native VLAN**—Native VLAN number.
- **POE**—Power over Ethernet (PoE) status of the Gigabit Ethernet port.
- **VLAN Mode**—VLAN mode of the Gigabit Ethernet port.
- **Allowed VLANs**—Allowed VLAN range.
- **MTU**—MTU value.
- **LLDP Neighbor**—LLDP neighbor port details.

From the **Port Statistics** drop-down list, select **Packets** to view the inbound and outbound packets for the following:
- Unicast
- Multicast
- Broadcast

From the **Port Statistics** drop-down list, select **Errors** to view graphs for the following:
- CRC Errors
- Error Frames
- Collisions

**Tunnel Tab**

The **Tunnel** tab displays the following details:

- **Tunnels**—Displays the following details:
  - **Total VPN Tunnels**—Total number of VPN tunnels.
  - **Up VPN Tunnels**—Number of VPN tunnels in UP state.
  - **Down VPN Tunnels**—Number of VPN tunnels in DOWN state.
  - **Total VPN Peers**—Total number of VPN peers.

The following details are displayed in the **Tunnels** table:
- **Tunnel**—Tunnel number.
- **Status**—Status of the tunnel.
- **Source**—Source IP address of the tunnel.
- **Destination**—Destination IP address of the tunnel.
- **Availability**—Availability graph of the tunnel. Displays the percentage of time the tunnel was in UP state.

- **Tunnels Info**—Displays the following details of the tunnel:
  - **Port**—Uplink port details.
  - **VLAN ID**—VLAN ID.
  - **WAN IP**—WAN IP address.
  - **Peer IP**—Peer IP address.
  - **Last Change Reason**—Reason for the last status change of the tunnel.
- **Usage**—Displays the inbound and outbound traffic usage.
- **Throughput**—Displays the inbound and outbound traffic rates for the selected tunnel.
- **Performance**—Displays the following details for the tunnel:
  - **Latency**—Displays the latency in microseconds.
  - **Jitter**—Displays the jitter in microseconds.
  - **Packet Loss**—Displays the packet loss in percentage terms.
  - **MOS Score**—Displays the transport health score. The MOS score range is from 1 to 5.

**Path Steering Tab**

If the gateway is provisioned as a VPN Concentrator, the **Path Steering** tab is disabled.

In the **Path Steering** tab, you can view traffic path steering details for the WAN policies configured on the Branch Gateway. The tab also displays the number of DPS policies that are compliant along with the total number of policies configured on the Branch Gateway. For more information on Dynamic Path Steering and configuration steps, see the *Dynamic Path Steering* section in the *Aruba Central Help Center*.

From the **WAN Policies** drop-down list, select the WAN policy for which you want to view the path steering details.

The **Path Steering** tab displays the following information:

- **Expected Threshold Values**
  - **Bandwidth**—Percentage of bandwidth utilization.
  - **Latency**—Round-trip ping time in milliseconds.
  - **Jitter**—Jitters in packet transmission in milliseconds.
  - **Packet Loss**—Percentage of packet loss allowed for the traffic type.
- **Path Preference**—Displays the path preference in the primary, secondary, and standby order.
- **Policy Compliance**—Policy compliance details.
- **Total Sessions**—Provides a graphical representation of uplink sessions. The overall sessions and the primary, secondary, and standby sessions are displayed.

**Alerts Tab**

The **Alerts** tab displays the following information:

- **Open Alerts**—Displays a list of open alerts. Select the alert and click **Acknowledge** or select multiple alerts and click **Acknowledge All** to acknowledge alerts.
- **Acknowledged Alerts**—Displays a list of acknowledged alerts.

The following details are displayed for open and acknowledged alerts:

- **Source**
- **Description**
- **Cause**
- **Severity**
- **Action**
- **Timestamp**

For more information about gateway alerts, see the *Gateway Alerts* section in the *Aruba Central Help Center*. 
Routes Tab
The Routes tab displays the following route details for the gateway:

- **Route Summary**
  - **Total**—Total number of routes.
  - **Default**—Number of default routes.
  - **Static**—Number of static routes.
  - **Overlay**—Number of overlay routes.
  - **Connected**—Number of connected routes.
  - **Dynamic**—Number of dynamic routes.

- **Routes**
  - **Route**—Destination IP address of the route.
  - **Next Hop**—IP address of the next router on the route.
  - **Protocol**—Routing protocol. Possible values are Connected, Static, RAP-NG, Aggregated RAP-NG, OSPF, RIP, Default, or Aggregated Static.
  - **Metric**—Distance for static routes. For a given route destination, there can be multiple nexthops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
  - **Flags**—Route flags. Possible value is either Not Redistributed or CFG-SET.
  - **Type**—Displays the route type. Possible values are Directly Connected, Tunnel Interface, Management Interface, or Branch Gateway Peer Uplink.
  - **Search Bar**—Allows you to filter the content in the Routes table.

Applications Tab
Displays charts showing client traffic trends to application, application categories, website categories, and websites of a specific security reputation score. To view the traffic classification based on application, application category, and website category, you must enable Deep Packet Inspection on the Branch Gateways.

For more information, see the Analyzing Application Usage and Traffic Patterns section in the Aruba Central Help Center.

The Applications tab displays pie charts for the following:

- **Application Categories**—Displays top N application categories based on total bandwidth usage. Apart from the top N, the rest of the application categories are grouped under the Others category.

- **Applications**—Displays top N applications based on total bandwidth usage. Apart from the top N, the rest of the applications are grouped under the Others category.

- **Web Categories**—Displays top N web categories based on total bandwidth usage. Apart from the top N, the rest of the web categories are grouped under the Others category.

- **Web Reputation**—Displays the reputation of the web content according to the reputation score configured.

Analyzing Application Usage
The AppRF graphs on the Gateways page option provides a detailed information on application usage by the clients connected to APs in the network.
**Enabling Application Visibility**

To enable AppRF, complete the following steps:

1. From the app selector, click **Gateway Management**.
2. From the group selector, select a group or a device.
3. Click **Security > Applications**.
4. Click **Application Visibility**.
5. Select the **Deep Packet Inspection (AppRF)** check box.
6. For website URL filtering, select the **Web Content Classification (WebCC)** check box.

**AppRF Graphs**

You can view the client traffic to **Applications, Application Categories, Website Categories, and Web Reputation** graphs for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in the last three hours.

The **AppRF** pane displays the following data graphs on the client traffic flowing to application (Apps), application categories (App Categories), web categories, and website reputation.

**App Categories Chart**

The **App Categories** chart displays details on the client traffic towards the application categories. When the cursor is placed on the chart, the app category and percentage of client traffic flowing to that app category is displayed. The legend below the chart displays the list of application categories to which the client traffic flow is detected. On clicking an app category from legend, the chart hides that app category and displays data for the remaining app categories.

**Apps Chart**

The **Apps** chart displays details on the client traffic flow to specific applications. When the cursor is placed on the chart, the application and percentage of traffic to that application is displayed. The legend below the chart displays the list of applications to which the client traffic flow is detected. On selecting an app from the legend, the chart hides that app and displays data for the remaining apps.

**Web Categories Chart**

The **Web Categories** chart displays details of the client traffic to web categories. When the cursor is placed on the chart, the web category and percentage of traffic to the web category is displayed. The legend below the chart displays the list of website categories to which the client traffic flow is detected. On selecting a web category from the legend, the chart hides that web category from the chart and displays data for the remaining web categories.

**Web Reputation Charts**

The Web Reputation chart displays details of the client traffic flow to the URLs that are assigned a web reputation score. When the cursor is placed on the chart, the web reputation type and percentage of traffic to the web reputation is displayed. On selecting a web reputation type from the legend, the chart hides the web reputation type and displays data for the remaining web reputation types.

**Network Health**

The **Network Health** menu option in the **Monitoring & Reports** application provides detailed information of the network health status and usage for the sites configured in your setup.
Data Source

The Network Health page displays network and site health data for the overall network and gateways. From the Data Source drop-down list, select Gateway to view network and site health data for gateways.

Table 38: Gateway Page

<table>
<thead>
<tr>
<th>Header</th>
<th>Totals</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Displays the total number of sites. Name of the site. Use the column filter bar to search for a particular site. Click the site name to open the Site Health page. For more information, see the Site Health section in the Aruba Central Help Center.</td>
<td></td>
</tr>
</tbody>
</table>
| Site Type    | Displays the total number of sites for each site type. Displays whether the device is deployed as a hub or spoke.  
  - To filter gateways provisioned as a hub, click Hub.  
  - To filter gateways provisioned as a spoke, click Spoke. |
| Device Status| Displays the total count of devices in the UP and DOWN states.  
  - To filter devices in UP state, click Up.  
  - To filter devices in DOWN state, click Down. |
| Connectivity | Displays the total number of links and the average bandwidth consumed. Displays the following information:  
  - Status—Displays the overall connectivity status. Hover your mouse over the column to view the circuit status, tunnel status, overlay status, and underlay status separately. One of the following statuses is displayed:  
    - Up  
    - Partial  
    - Down  
  - Bandwidth—Displays bandwidth details.  
    - Configured—Displays the bandwidth that is configured on the Branch Gateway.  
    - Estimated—Displays the estimated bandwidth availability for the uplinks. The Bandwidth Estimation feature must be enabled to display this data. For more information, see Bandwidth Estimation on page 51.  
    - Consumed—Displays the bandwidth consumed by the clients. |
| Performance  | Displays the average value for site availability and policy compliance. Displays the following metrics:  
  - Site Availability—Displays the site availability. The range is from 0 to 100 percent. To filter site availability, click the column filter bar and enter values in the Min and Max text boxes. Hover your mouse over the column to view site availability on a per provider basis.  
  - Policy Compliance—Displays the policy compliance. The range is from 0 to 100 percent. To filter policy compliance, click the column filter bar and enter values in the Min and Max text boxes. Hover your mouse over the column to view policy compliance on a per policy basis. |

Page Views

The Network Health page offers the following views:

- Grid—Primarily provides numerical representation of the data. The Site Type and Connectivity Status columns provide textual values.
- Status—Uses the following indicators to present information on status of the network health:  
  - Small black bullet icon—Indicates no issues.  
  - Big red bullet icon—Indicates potential issues.
- **MAP**—The map provides a pictorial view of the network across various sites. The sites are color coded; red indicates potential issues and gray indicates that there are no issues. To change the zoom level, click the zoom icons.
  - From the **Pin Radius** drop-down list, select one of the following options: No Grouping, 5 miles, 10 miles, 15 miles, 20 miles, or 50 miles.
  - From the **Data Column For Map** drop-down list, select one of the following options: Device Status, Connectivity Status, Site Availability, or Policy Compliance.

### Site Health

The **Site Health** page displays details for the wired, wireless, and gateway devices deployed on the site. The **Site Health** page view can be set to the **Summary** or the **Gateways** view.

To open the **Site Health** page:

1. From the app selector, go to Monitoring & Reports > Network Health.
2. From the **Network Health** page, click the site name to view details of a specific site. The **Site Health** page is displayed.

### Gateways

The **Site Health** > **Gateway** page displays the following information:

#### Table 39: Site Health Gateways Page

<table>
<thead>
<tr>
<th>Content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Site Name</strong></td>
<td>Name of the site. From the drop-down list, select a site.</td>
</tr>
<tr>
<td><strong>Data View</strong></td>
<td>Data source. From the drop-down list, select either Summary or Gateway. For example, if the data view is set to Gateway, the page displays data for the gateways deployed on the site.</td>
</tr>
<tr>
<td><strong>Time Range</strong></td>
<td>Time range selection drop-down for viewing site health. You can set the time range to 3 hours, 1 day, 1 week, 1 month, or 3 months.</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>The following details are available:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong>—Name of the site.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Location</strong>—Location of the site.</td>
</tr>
<tr>
<td></td>
<td>- <strong>APs</strong>—Number of APs deployed on the site.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Switches</strong>—Number of switches deployed on the site.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Gateways</strong>—Number of gateways deployed on the site.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Topology Icon</strong>—Link to topology view. The topology page displays the network topology of the site.</td>
</tr>
<tr>
<td><strong>Site Availability graph</strong></td>
<td>Site availability metrics per provider represented in a chart. The graph displays detailed metrics for the number of sites in the down status, percentage of site availability, and the number of unknown sites.</td>
</tr>
<tr>
<td><strong>Policy Compliance graph</strong></td>
<td>Policy compliance metrics for the site. The path steering data is used to calculate this metric.</td>
</tr>
<tr>
<td><strong>Bandwidth graph</strong></td>
<td>Bandwidth utilization of the selected site. From the drop-down list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- All Traffic</td>
</tr>
<tr>
<td></td>
<td>- Internet vs. VPN</td>
</tr>
</tbody>
</table>
Table 39: Site Health Gateways Page

<table>
<thead>
<tr>
<th>Content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Provider graph</td>
<td>Bandwidth utilization of the selected uplink. From the drop-down list, select the uplink.</td>
</tr>
<tr>
<td>Transport Health graph</td>
<td>Displays the transport health of the site based on active monitoring probes. Site transport health is an average of MOS score across all probes.</td>
</tr>
</tbody>
</table>

**NOTE:** If you hover over any graph, a pop-up window opens and displays the data specific to that graph. Click on the graph to lock the time range. After you lock the selection, the same time range is selected across all the graphs in the Site Health page.

**NOTE:** If you click on any graph, a see devices button in enabled below all the graphs. Click see details to view the list of devices. From the Add Metric drop-down list, select one or more of the following: Site Availability, Policy Compliance, Bandwidth, Internet vs. VPN, or Transport Health.

Topology

The Topology map in Central provides a graphical representation of the network layout, details of the devices deployed in a branch site, and the health of the WAN uplinks and tunnels. The minimum required ArubaOS version for Topology is ArubaOS version 8.1.0.0-1.0.1.1.

On Switches, LLDP is enabled by default. On Branch Gateways, if the port type is LAN, LLDP is enabled by default and you can view the topology map.

For more information, see the following sections in the Aruba Central Help Center:

- Configuring Ports for LAN Interfaces
- Configuring Other Parameters for Port

Before You Begin

The topology map filters devices based on sites. To view the topology map, ensure that you have assigned the devices to sites. For more information, see the Assigning Devices to Sites in the Aruba Central Help Center.

Viewing Topology Map

To access the topology map:

1. From the app selector, click Monitoring & Reports.
2. Click Topology.
3. From the filter bar, select a site.

Navigating the Topology Map

The topology map provides a pictorial view of the devices deployed in the branch site, uplink health, and tunnel status. A task pane on the right provides a summary of the devices, VLAN interfaces, uplink, and tunnel details. The red and green indicators show the current status and health of the WAN uplinks and tunnels.

- To view the name, type, and hardware model of the device, hover your mouse on the device.
- To view more details about the device such as VLAN interfaces, click the device icon on the map.
- To view details of the uplink interfaces, click the lines on the map.
- To change the zoom level, click the zoom icons.
Task Pane

The task pane consists of the following tabs:

- **Details**—Provides a detailed summary of the devices, uplink interfaces, and tunnels. It also highlights the status of the device and uplinks.

- **Filter**—Allows you to apply a filter criteria for displaying devices on the map. The following options are available:
  - Branch Gateway
  - Switch
  - IAP

For example, if you set the filter to Branch Gateways, only the Branch Gateway details are displayed. Similarly, you can set the filter to show or hide the devices that are linked on uplink ports.

The **Details** tab displays the following information:

**Table 40: Contents of the Details Tab**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device details</strong></td>
<td></td>
</tr>
<tr>
<td>Branch Gateway</td>
<td>Displays the following details:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong>—Hostname of the Branch Gateway.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Serial</strong>—Serial number of the Branch Gateway.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IP</strong>—IP address of the Branch Gateway.</td>
</tr>
<tr>
<td></td>
<td>- <strong>MAC</strong>—MAC address of the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>—Type of device deployment. For Branch Gateways, the type shows up as <strong>BOC</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Model</strong>—Hardware model of the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong>—Operational status of the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Health</strong>—Operational health of the device.</td>
</tr>
<tr>
<td>Switch</td>
<td>Displays the following details:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong>—Hostname of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Serial</strong>—Serial number of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IP</strong>—IP address of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>MAC</strong>—MAC address of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>—Type of the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Model</strong>—Hardware model of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong>—Operational status of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Health</strong>—Operational health of the switch.</td>
</tr>
<tr>
<td>Instant AP</td>
<td>Displays the following details:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong>—Hostname of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Serial</strong>—Serial number of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IP</strong>—IP address of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>MAC</strong>—MAC address of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong>—Type of the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Model</strong>—Hardware model of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong>—Up and down arrows indicating the operational status of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Health</strong>—Operational health of the Instant AP.</td>
</tr>
</tbody>
</table>

**Tunnel, Uplink, and Edge details**

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Displays the following information about tunnels configured on the Branch Gateway:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>VLAN</strong>—VLAN ID of the tunnel.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Established Time</strong>—Timestamp showing when the tunnel was established.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Uplink</td>
<td>Displays the following information about uplinks configured on the Branch Gateway:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Link ID</strong>—Link ID of the uplink.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Uplink Type</strong>—Type of the uplink.</td>
</tr>
<tr>
<td></td>
<td>- <strong>VLAN</strong>—VLAN ID of the uplink.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Link Status</strong>—Uplink status.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Description</strong>—Description of the uplink.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tunnel Description</strong>—Description of the tunnel.</td>
</tr>
<tr>
<td></td>
<td>- <strong>WAN Status</strong>—WAN status.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Public IP</strong>—Public IP address.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Device MAC</strong>—MAC address of the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Serial</strong>—Serial number of the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Port Number</strong>—Port number of the device.</td>
</tr>
<tr>
<td>Edge—Switch to IAP</td>
<td>Displays the following information about the switch to Instant AP link:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Interface numbers</strong>—Switch and Instant AP interface numbers.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Interface</strong>—Interface number of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Serial</strong>—Serial number of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Device Name</strong>—Device name of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Port Number</strong>—Port number of the switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Interface</strong>—Interface number of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Serial</strong>—Serial number of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Device Name</strong>—Device name of the Instant AP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Port number</strong>—Port number of the Instant AP.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Edge—BOC to Switch          | Displays the following information about the Branch Gateway to switch link:  
  - **Interface numbers**—Branch Gateway and switch interface numbers.  
  - **Interface**—Interface number of the Branch Gateway.  
    - **Serial**—Serial number of the Branch Gateway.  
    - **Device Name**—Device name of the Branch Gateway.  
    - **Port Number**—Port number of the Branch Gateway.  
  - **Interface**—Interface number of the switch.  
    - **Serial**—Serial number of the switch.  
    - **Device Name**—Device name of the switch.  
    - **Port Number**—Port number of the switch.  
  NOTE: If an alternate link is configured for redundancy, link details are displayed for the alternate Branch Gateway to switch link as well. |
| Edge—BOC to IAP             | Displays the following information about the Branch Gateway to Instant AP link:  
  - **Interface numbers**—Branch Gateway and Instant AP interface numbers.  
  - **Interface**—Interface number of the Branch Gateway.  
    - **Serial**—Serial number of the Branch Gateway.  
    - **Device Name**—Device name of the Branch Gateway.  
    - **Port Number**—Port number of the Branch Gateway.  
  - **Interface**—Interface number of the Instant AP.  
    - **Serial**—Serial number of the Instant AP.  
    - **Device Name**—Device name of the Instant AP.  
    - **Port number**—Port number of the Instant AP. |

**Gateway Alerts**

The Alerts pane displays all types of alerts generated for events pertaining to device provisioning, configuration, and user management.

**Viewing the Alerts Summary and Acknowledging Alerts**

To view a summary of alerts and acknowledge alerts, complete the following steps:

1. From the app selector, click Monitoring & Reports.
2. Click Alerts. The Alerts page shows a summary of alerts and the Configure Alerts and Acknowledge All buttons.

**Table 41: Alerts pane**

<table>
<thead>
<tr>
<th>Data Pane Content</th>
<th>Description</th>
</tr>
</thead>
</table>
| Open              | Displays the number of alerts in the following categories:  
  - Critical  
  - Major  
  - Minor  
  - Warning  
  - **Search box**—Allows you to search for alerts using keywords.  
  - **Acknowledge**—The Acknowledge button appears when you hover your mouse over any alert. Click Acknowledge to acknowledge that specific alert.  
  - **Acknowledge All**—Allows you to acknowledge all alerts at once.  
| Acknowledged      | Displays a list of acknowledged alerts. Use the search box to search for an alert.                                                                                                                                                                                                                                                      |
Configuring Alerts
To configure alerts, complete the following steps:

1. From the app selector, go to Monitoring & Reports > Alerts.
2. On the Alerts page, click Configure Alerts.
3. In the Configure Alerts page, click All.
4. In the All tab, select an alert and click + to enable the alert with default settings. In any alert category, click ...More to expand the list of alerts. For a complete list of gateway alerts that you can configure, see Types of Gateway Alerts on page 139.

To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:

   a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning.

For a few alerts, you can configure threshold value for one or more alert severities. To set the threshold value, select the alert and in the exceeds text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

   b. **Duration**—Enter the duration in minutes.

   c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:

      - **Group**—Select a group to limit the alert to a specific group.
      - **Label**—Select a label to limit the alert to a specific label.
      - **Device**—Select a device to limit the alert to a specific device.

   d. Select the Email check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.

   e. Click **Save**.

   f. **Add Rule**—(Optional) For a few alerts, the Add Rule option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the page.

Types of Gateway Alerts
The following is a list of gateway alerts that you can configure:

- **SLA DPS Compliance Violations**—Generates an alert when the WAN policy does not meet the compliance criteria.

- **New Gateway Connected**—Generates an alert when a new Branch Gateway is connected.

- **Gateway Disconnected**—Generates an alert when a Branch Gateway is disconnected. In the Duration field, enter the duration after which the alert must be generated.

- **Gateway CPU Utilization**—Generates an alert when the Branch Gateway CPU utilization exceeds the threshold value. In the Duration field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.

- **Gateway Memory Utilization**—Generates an alert when the Branch Gateway memory utilization exceeds the threshold value. In the Duration field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.

- **Gateway Emergency Mode**—Generates an alert when the Branch Gateway emergency mode changes.

- **OSPF Session Error**—Generates an alert when the OSPF session fails to establish.

- **WAN Health-Check Failure**—Generates an alert when WAN health check fails.
- **WAN VPN-Peer Unreachable**—Generates an alert when the WAN VPN peer is unreachable.
- **VPN Peer Failover**—Generates an alert when the VPN peer fails over.
- **WAN Uplink Status Change**—Generates an alert when the WAN uplink status changes.
- **WAN Uplink Autonegotiation State Change**—Generates an alert when the WAN uplink autonegotiation status changes.
- **WAN Uplink Input Errors**—Generates an alert when the WAN uplink input errors exceed the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink Output Errors**—Generates an alert when the WAN uplink output errors exceed the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink PHY Errors**—Generates an alert when the WAN uplink PHY errors exceed the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **DHCP Pool Consumption**—Generates an alert when the DHCP pool consumption exceeds the threshold value. In the **Subnet** field, enter the subnet address to filter the alert based on subnet.
- **IPSec Establishment Failure**—Generates an alert when the IPsec tunnel fails to establish.
- **IPSec SA Down**—Generates an alert when the IPsec SA is down.
- **All IPsec SAs Down**—Generates an alert when all the IPsec SAs are down.
- **CFG-SET Advertisement Failure**—Generates an alert when the CFG-SET advertisement fails.
- **Uplink Flapping**—Generates an alert when the uplink state changes frequently. In the **Duration** field, enter the duration after which the alert must be generated. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Tunnel Flapping**—Generates an alert when the tunnel state changes frequently. In the **Duration** field, enter the duration after which the alert must be generated. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Uplink Speed Flapping**—Generates an alert when the uplink speed changes. In the **Duration** field, enter the duration after which the alert must be generated. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **EST Enrollment Failure**—Generates an alert when the Virtual Gateway fails to enroll with the EST server.

**Viewing Enabled Alerts**

To view the alerts that you have enabled:

1. From the app selector, go to **Monitoring & Reports > Alerts**.
2. On the **Alerts** page, click **Configure Alerts**.
3. In the **Configure Alerts** page, click the **Enabled** tab.
   The **Enabled** tab lists the alerts that you have enabled.

**Gateway Reports**

The **Reports** pane allows you to create various reports. You can configure the reports to be run on demand or periodically. You must have read/write privileges or you must be an admin user to be able to create reports. The **Reports** page has the following sections:

- **Configure Reports**—Displays the reports configured using the **Create Report** option.
- **Generated Reports**—Displays the reports generated.
This section includes the following topics:

- Types of Gateway Reports on page 141
- Creating a Report on page 142
- Generated Reports on page 143
- Viewing Generated Reports on page 144
- Gateway Reports on page 140

Types of Gateway Reports

The following table lists the different types of gateway reports that you can generate in Central:

Table 42: Types of Gateway Reports

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN Inventory</strong></td>
<td>Displays a list of Branch Gateways onboarded. The report is segregated by ArubaOS software version and contains the following details:</td>
</tr>
<tr>
<td></td>
<td>- Site Name</td>
</tr>
<tr>
<td></td>
<td>- Serial Number</td>
</tr>
<tr>
<td></td>
<td>- Host name</td>
</tr>
<tr>
<td></td>
<td>- MAC</td>
</tr>
<tr>
<td></td>
<td>- IP Address</td>
</tr>
<tr>
<td></td>
<td>- Model</td>
</tr>
<tr>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td>- Street Address</td>
</tr>
<tr>
<td><strong>WAN Policy Compliance</strong></td>
<td>Displays the worst performing or best performing links according to the SLA compliance violations. The report contains the following details:</td>
</tr>
<tr>
<td></td>
<td>- Link ID</td>
</tr>
<tr>
<td></td>
<td>- Provider Tag</td>
</tr>
<tr>
<td></td>
<td>- Link Type</td>
</tr>
<tr>
<td></td>
<td>- Branch Gateway Serial Number</td>
</tr>
<tr>
<td></td>
<td>- Host name</td>
</tr>
<tr>
<td></td>
<td>- MAC</td>
</tr>
<tr>
<td></td>
<td>- Site Name</td>
</tr>
<tr>
<td></td>
<td>- Top N intervals when the link was non-compliant.</td>
</tr>
<tr>
<td></td>
<td>- Compliance %</td>
</tr>
<tr>
<td><strong>WAN Transport Health</strong></td>
<td>Displays the top N links with probed values. The report contains the following details:</td>
</tr>
<tr>
<td></td>
<td>- Title</td>
</tr>
<tr>
<td></td>
<td>- Probe Destination IP</td>
</tr>
<tr>
<td></td>
<td>- Branch Gateway</td>
</tr>
<tr>
<td></td>
<td>- Site</td>
</tr>
<tr>
<td></td>
<td>- Serial Number</td>
</tr>
<tr>
<td></td>
<td>- Host name</td>
</tr>
<tr>
<td></td>
<td>- MAC</td>
</tr>
<tr>
<td></td>
<td>- Uplink</td>
</tr>
<tr>
<td></td>
<td>- Name</td>
</tr>
<tr>
<td></td>
<td>- Uplink</td>
</tr>
<tr>
<td></td>
<td>- Value</td>
</tr>
<tr>
<td></td>
<td>- Either Loss (%) or Latency (ms)</td>
</tr>
<tr>
<td><strong>WAN Availability</strong></td>
<td>Displays WAN overlay and underlay availability information. The <strong>Underlay</strong> report contains the following details:</td>
</tr>
<tr>
<td></td>
<td>- Branch Gateway</td>
</tr>
<tr>
<td></td>
<td>- Site</td>
</tr>
<tr>
<td>Report Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|             | ● Serial Number  
|             | ● Host name  
|             | ● MAC  
|             | ● Uplink  
|             | ● Name  
|             | ● Type  
|             | ● VLAN  
|             | ● %Uptime  
|             | ● Uptime  
|             | ● Downtime  

The **Overlay** report contains the following details:

- Branch Gateway  
  ● Site  
  ● Serial Number  
  ● Host name  
  ● MAC  
- Uplink  
  ● VLAN  
- Tunnel  
  ● Name  
  ● SIP  
  ● DIP  
- ● %Uptime  
- ● Uptime  
- ● Downtime

### WAN Utilization

Displays WAN bandwidth utilization information for Underlay, Overlay, and Uplinks.

The report contains the following details:

- Branch Gateway  
  ● Site  
  ● Serial Number  
  ● Host name  
  ● MAC  
- Uplink  
  ● Name  
  ● Type  
  ● VLAN  
- Usage  
  ● Average Bandwidth (Mbps)  
  ● SLA Bandwidth (Mbps)  
  ● %Utilization

### Creating a Report

To create a report, complete the following steps:

1. From the app selector, click **Monitoring & Reports** and select **Reports**. The **Reports** page is displayed.
2. From the **Report Type** drop-down list, select the type of the report to generate. You can generate one of the following reports for gateways:
   - **WAN Inventory**
   - **WAN Policy Compliance**
     - From the **Report Order** drop-down list, select either **Best Performing** or **Worst Performing**. By default, the report is created for worst performing links.
     - In the **Top N** field, enter the number of top N links. The range is from 1 to 25.
- **WAN Transport Health**
  - From the **Transport Type** drop-down list, select **Overlay** or **Underlay**.
  - From the **Report Order** drop-down list, select either **Best Performing** or **Worst Performing**. By default, the report is created for worst performing links.
  - In the **Top N** field, enter the number of top N links. The range is from 1 to 25.

- **WAN Availability**
  - From the **Transport Type** drop-down list, select **Overlay** or **Underlay**.
  - From the **Report Order** drop-down list, select either **Best Performing** or **Worst Performing**. By default, the report is created for worst performing links.
  - In the **Top N** field, enter the number of top N links. The range is from 1 to 25.

- **WAN Utilization**
  - From the **Transport Type** drop-down list, select **Overlay** or **Underlay**.
  - From the **Report Order** drop-down list, select either **Best Performing** or **Worst Performing**. By default, the report is created for worst performing links.
  - In the **Top N** field, enter the number of top N links. The range is from 1 to 25.

3. In the **Title** text box, enter the name of the report.

4. For **WAN Policy Compliance**, **WAN Transport Health**, **WAN Availability**, and **WAN Utilization** reports, you can select the period for which you want to create the report. From the **Period** drop-down list, select one of the following:
   - Last day
   - Last week
   - Last month
   - Custom range

5. Select **Now** from **Schedule** to generate the report immediately. To run reports at a later time, select **Later** and specify the date and time.

6. From the **Run Report** drop-down list, select how often you want to generate the report by choosing **One Time**, **Daily Interval**, **Weekly Interval**, or **Monthly Interval**.

7. To email the generated report, specify the email address of the recipient in **Email Report**.

8. Click **Create**.

### Generated Reports

In the **Generated Reports** section of the **Reports** page, a table listing the parameters used for generating a report is displayed.

**Table 43: Reports Pane**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Displays the title name of the report generated.</td>
</tr>
<tr>
<td><strong>Date Run</strong></td>
<td>Displays the date on which the report was generated.</td>
</tr>
<tr>
<td><strong>Saved By</strong></td>
<td>Indicates the user login name using which the report was generated.</td>
</tr>
<tr>
<td><strong>Device Group</strong></td>
<td>Indicates the device group or groups for which the report was generated.</td>
</tr>
</tbody>
</table>
### Viewing Generated Reports

To view a generated report, complete the following steps:

1. From the app selector, click Monitoring & Reports and select Reports.
2. From the Report Type drop-down list in the Generated Reports section of the Reports page, select the report type. The following types of gateway reports are available:
   - WAN Inventory
   - WAN Policy Compliance
   - WAN Transport Health
   - WAN Availability
   - WAN Utilization
3. To send the report through email, click the email icon, enter the email address, and then click Send email.

### Editing a Report

To edit a configured report, complete the following steps:

1. In the Reports page, go to the Configure Reports table.
2. Select the report that you want to edit and click the edit icon.
3. Edit the field(s) as necessary and click Update.

### Deleting Report(s)

To delete report(s), in the Reports page, go to the Configure Reports table.

- To delete a configured report, complete the following steps:
  1. Select the report that you want to delete and click the delete icon.
  2. In the Confirm Action pop-up window, click Yes.
- To delete multiple configured reports, complete the following steps:
  1. Press and hold the Ctrl key and select the reports that you want to delete and click Batch Remove Reports.
  2. In the Confirm Action pop-up window, click Yes.

In the Reports page, go to the Generated Reports table.

- To delete a generated report, complete the following steps:
  1. Select the report that you want to delete and click the delete icon.
  2. In the Confirm Action pop-up window, click Yes.
To delete multiple generated reports, complete the following steps:

- Press and hold the Ctrl key and select the reports that you want to delete and click **Batch Remove Reports**.
- In the **Confirm Action** pop-up window, click **Yes**.

**Exporting a Report**

To export a generated report, complete the following steps:

1. In the **Reports** page, go to the **Generated Reports** table.
2. Select the report that you want to export and click the export icon.
The **Maintenance** application allows you to upgrade firmware and troubleshoot devices. See the following topics for more information:
- Managing Software Upgrades on page 146
- Troubleshooting Devices on page 146

## Managing Software Upgrades
For information on how to upgrade software images on SD-WAN Gateways, see the *Managing Software Upgrades* topic in *Aruba Central Help Center*.

## Troubleshooting Devices
The **Troubleshooting** menu in the **Maintenance** module allows your network administrators to run troubleshooting or diagnostics commands on the devices managed from Central. When a troubleshooting operation is initiated, Central establishes a session with the devices, retrieves the output of the commands, and displays the output in the UI.

Central supports running troubleshooting operations on one or several devices. You can select up to 10 devices for a troubleshooting operation. If the user access is restricted to certain groups within a network, Central allows running troubleshooting commands only for the devices provisioned in the allowed groups.

For more information on troubleshooting, see *Troubleshooting Devices* in the *Aruba Central Help Center*.

### Configuring SD-WAN Gateways for Syslog Message Collection
This section outlines the steps required to configure logging on an SD-WAN Gateway.

For each category or subcategory of message, you can set the logging level or severity level of the messages to be logged.

The following table summarizes these categories:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>Network messages</td>
</tr>
<tr>
<td>all</td>
<td>All network messages</td>
</tr>
<tr>
<td>packet-dump</td>
<td>Protocol packet dump messages</td>
</tr>
<tr>
<td>mobility</td>
<td>Mobility messages</td>
</tr>
<tr>
<td>dhcp</td>
<td>DHCP messages</td>
</tr>
<tr>
<td>system</td>
<td>System messages</td>
</tr>
<tr>
<td>all</td>
<td>All system messages</td>
</tr>
</tbody>
</table>
For each category or subcategory, you can configure a logging level. The following table describes the logging levels in order of severity, from most to least severe.

**Table 45: Logging Levels**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>captive portal user messages</td>
</tr>
<tr>
<td>alert</td>
<td>VPN messages</td>
</tr>
<tr>
<td>critical</td>
<td>802.1x messages</td>
</tr>
<tr>
<td>errors</td>
<td>RADIUS user messages</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>warning</td>
<td>warning messages</td>
</tr>
<tr>
<td>notice</td>
<td>Significant events of a non-critical and normal nature.</td>
</tr>
<tr>
<td>informational</td>
<td>Messages of general interest to system users.</td>
</tr>
<tr>
<td>debug</td>
<td>Messages containing information useful for debugging.</td>
</tr>
</tbody>
</table>

The default logging level for all categories is Warning. You can also configure IP address of a syslog server to which the Branch Gateway can direct these logs.

**Configuring Logging Levels**

1. From the app selector, click **Gateway Management**.
2. From the group selection filter bar, select the SD-WAN Gateway that you want to configure.
3. Click **System > Logging**.
4. Click + in the **Syslog Servers** section to add a logging server.
5. Add the logging server to the list of logging servers. Update the followings fields:
   - IP address
   - Category
   - Logging facility
   - Logging level
   - Format: Select the logging format from the **Format** drop-down list. The ArcSight CEF is a log management standard that uses a standardized logging format so that data can easily be collected and aggregated for analysis by an enterprise management system.

   Ensure that the syslog server is enabled and configured on this host.

6. Click **Save Settings**.

To select the types of messages you want to log, select **Logging Levels**.

1. Select the category or subcategory to be logged.
2. To select the severity level for the category or subcategory, select the level from the **Logging Level** drop-down list.
3. Click **Save Settings**.

**API Gateway**

Central supports an Application Programming Interface (APIs) to allow the administrator users to create and manage APIs. It supports the following types of APIs:

- A polling-based API—The Representational State Transfer (REST)-based APIs support HTTP GET operations by providing a specific URL for each query. The output for these operations are returned in the JSON format.
- Push or Event APIs—The Push API gives web applications the ability to receive messages pushed to them from a server.

The API Gateway feature in Central offers the following benefits:
- Provides an API management gateway to create, publish, manage the life cycle of APIs
- Provides a gateway that can run on public and private cloud as containers
- Displays the API usage pattern
- Provides a developer portal to develop applications using the APIs

The administrators of a web API gateway can create a API gateway cluster to route the API traffic to Aruba cloud services. Central offers the following consoles for API management:

- Administrator Console—The console for managing APIs and consumers.
- Publisher Console—The console for creating and publishing an API.

For more information on API Gateway, supported APIs, and the OAuth token generation procedure, see the API Gateway topic in Aruba Central Help Center.