Zero-Touch Provisioning for ArubaOS-Switch
Version 16.08
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Zero Touch Provisioning via Aruba Airwave</td>
<td>3</td>
</tr>
<tr>
<td>DHCP server configuration</td>
<td>3</td>
</tr>
<tr>
<td>Workflow</td>
<td>4</td>
</tr>
<tr>
<td>Templates</td>
<td>7</td>
</tr>
<tr>
<td>Secure ZTP with an Aruba Controller</td>
<td>8</td>
</tr>
<tr>
<td>DHCP Server Configuration</td>
<td>9</td>
</tr>
<tr>
<td>Aruba Controller Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Sample Debug Outputs</td>
<td>14</td>
</tr>
<tr>
<td>Example Log Messages</td>
<td>14</td>
</tr>
<tr>
<td>Example ZTP Debug Output</td>
<td>15</td>
</tr>
<tr>
<td>Provisioning with Aruba Central</td>
<td>17</td>
</tr>
<tr>
<td>Group Creation and Device Assignment</td>
<td>17</td>
</tr>
<tr>
<td>UI-based Group and Device Configuration</td>
<td>17</td>
</tr>
<tr>
<td>Template-based Group Configuration</td>
<td>18</td>
</tr>
<tr>
<td>Provisioning sequence with Activate and Central</td>
<td>19</td>
</tr>
<tr>
<td>Zero Touch Provisioning with DHCP and TFTP.</td>
<td>20</td>
</tr>
<tr>
<td>Create vendor class on DHCP server</td>
<td>20</td>
</tr>
<tr>
<td>Set Predefined Options</td>
<td>21</td>
</tr>
<tr>
<td>Supported Platforms</td>
<td>23</td>
</tr>
</tbody>
</table>
OVERVIEW

The ArubaOS-Switch software platform provides three primary methods to automatically provision Aruba switches with predefined configuration and software images — TFTP automatic download, AirWave, and Central. This document provides setup instructions, best practices, and troubleshooting guidelines for utilizing zero-touch provisioning on ArubaOS-Switch.

Zero touch provisioning (ZTP) is a switch feature that allows the devices to be provisioned and configured automatically, eliminating most of the manual labor involved with adding them to a network. ZTP allows the hardware to be installed directly into the environment and for that act to be the last hands-on moment. When it’s powered on, the switch sends out a request through DHCP (Dynamic Host Configuration Protocol) or TFTP (Trivial File Transfer Protocol) to get the location of its centrally stored image and configuration, which it downloads and runs.

The objectives of this document are to demonstrate Aruba’s various Zero Touch Provisioning (ZTP) solutions that enables the auto-configuration of Aruba switches (from a factory default configuration) without requiring any administrator’s intervention at the switch. The switches can use DHCP server options to provide the relevant info for successful provisioning via a TFTP server or Aruba’s AirWave management platform. A third option, Aruba Central, a cloud-based management platform, allows switches to reach out to the Aruba Central servers when in a factory default state, subsequently managed by Central.

ZERO TOUCH PROVISIONING VIA ARUBA AIRWAVE

The main goal of Zero Touch Provisioning (ZTP) is that when a switch, in its initial configuration, boots up, it will perform a DHCP request on its default VLAN (VLAN-1) and then uses DHCP response to discover Airwave. The switch then contacts AirWave and gets its configuration.

The Airwave details received from the DHCP options are stored in the switch configuration. This assures that the configuration is retained even after the switch is rebooted.

DHCP server configuration

The switch will receive AirWave information via DHCP options 43 and 60. Option 43 can provide AirWave details in two ways:

1. Provide Airwave details in Sub option 146 - For Traditional DHCP ZTP Deployments
2. Provide Airwave details directly in option 43 in Conjunction with option 60 (with Value "ArubaInstantAP") - For deployments where Aruba APs are involved

The presence of option 60 with the value "ArubaInstantAP" helps the Aruba switch to decide how to read Option 43. If Option 60 is not provided, or sent with a different value, the switch will try to look for sub option146 with Airwave details. If AirWave details are not found, the switch will try to reach out to Aruba Activate. Option 60 is included in the initial DHCP discover message that a DHCP client broadcasts in search of an IP address. Option 60 is used by DHCP clients in order to identify itself to the DHCP server.

In the following example, the DHCP server needs to be configured to provide the correct information back to new Aruba switches.

First, the DHCP Option 60 string needs to be defined in the scope options of the DHCP server, for this example, Windows Server 2016 is being used.
Then, DHCP option 43, needs to be configured, which points to the Airwave server in the following format:

\insula{Group}:\لندا{Topfolder},\لندا{AMP IP},\لندا{shared secret}

LAN switches: Branch1, 192.168.1.15, aruba123

**Workflow**

The provisioning workflow is as follows:
1. The switch boots up with a factory default configuration.
2. The switch sends out a DHCP discovery from the primary VLAN interface.
3. The switch will expect DHCP option 60 with the configured string value “ArubaInstantAP” along with DHCP option 43 to parse Airwave details.
4. After the Airwave details are verified and configured, the switch initiates the HTTPS connection to the Airwave server.
5. After a successful registration, Airwave can then monitor, configure, and troubleshoot the switches.
6. If the DHCP options are not configured for Airwave, the switch is left in its default state for manual configuration.

In AirWave, select AMP Setup > General > Automatic Authorization, automatically authorized switch mode should be set to “Managed Read/Write” and switch whitelisting should be set to “All”. This is the default setting for Airwave.

Once the switch connects to the network, it should receive a DHCP address if proper connectivity to the DHCP server is configured. Executing the command “show ip” should validate whether the switch has received an IP address or not.

```
switch# show ip

Internet (IP) Service

IP Routing : Disabled

Default Gateway : 192.168.58.254
Default TTL : 64
Arp Age : 20
Domain Suffix :
DNS server :

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP Config</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Proxy ARP</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT_VLAN</td>
<td>DHCP/Bootp 192.168.58.120</td>
<td>255.255.255.0</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```
By performing a packet capture and examining the DHCP options sent to the switch, the previous DHCP option configuration can be observed.

After the switch registers with AirWave, the switch-initiated TLS connection can then be viewed.

It should be noted that if the ZTP device is the first discovered device in the newly created group and folder, then it will show under the new devices list which we need to move into the desired group/folder.

From the second ZTP device onwards for the same group and folder as the first device, it will automatically move into the corresponding group and folder.
Templates

Once the switch is registered with AirWave and moved to a group, a template needs to be created. This can be done in two ways: a template can be manually created or fetched from the switch after it is manually configured with a “Golden configuration”.

To navigate to templates, select the “Groups” menu on the left, then select the desired group from the list and then click “Templates”.

Once in the template window, select the “pencil icon” to edit the template as shown in the figure below.

From here, the desired switch can be selected from the “Search devices” field and the template fetched from the switch.
The other method is to manually enter the template into the template window. Variables can be used for settings that may change across a suite of switches. For more information on templates, please see the Aruba AirWave Switch Configuration Guide - [https://support.hpe.com/hpsc/doc/public/display?docId=a00062310en_us/](https://support.hpe.com/hpsc/doc/public/display?docId=a00062310en_us/)

An additional way to add variables into the template is to use a Bulk CSV file. This allows a CSV file containing pertinent switch information to be imported into AirWave, using variables to assign the values from the CSV spreadsheet. This is helpful when provisioning stacks or switches that could contain many different variables. For more information on adding devices via a CSV file, refer to the AirWave Switch Config Guide - [https://support.hpe.com/hpsc/doc/public/display?docId=a00062310en_us/](https://support.hpe.com/hpsc/doc/public/display?docId=a00062310en_us/)

Secure ZTP with an Aruba Controller

This solution provides a secure communication (IPSec) method between Aruba Switches and the Aruba controller (acting as a VPN concentrator) for network management traffic to Airwave.
Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

The IPsec is an open standard as a part of the IPv4 suite. IPsec uses the following protocols to perform various functions:

- **Authentication Headers (AH)** provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- **Encapsulating Security Payloads (ESP)** provides confidentiality, connectionless integrity, data-origin authentication, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.
- **Security Associations (SA)** provides the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange, with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2).

The process works as follows:

- An IPSEC tunnel for Airwave is auto-configured. The switch decides to create IPSEC tunnel only when an Aruba controller IP is present in the device before establishing the connection to Airwave.
- If the controller IP is not provided and only Airwave details are provided, the switch will try to establish a direct HTTPS connection to Airwave.
- If Airwave details are missing from DHCP, the ZTP process will try to connect to Activate to receive Airwave details
- If the controller IP is present, the ArubaOS-Switch auto configures and initiates an IPSEC tunnel interface. Once the tunnel is established, the Aruba controller provides an inner IP which the switch will then use as source IP to send any Airwave bound traffic. The switch then creates a static route to Airwave with the IPsec tunnel interface as the gateway.

Note: It is vital that Airwave can reach the inner switch IP address via the IPSec tunnel for the solution to work.

This method uses the DHCP server to provide the IP address of the controller, it is recommended to have a valid NTP server so that the time can be synchronized between the switch and controller.

**DHCP Server Configuration**

Historically, option 138 was used for CAPWAP, in this case, it will be used to pass the controller IP address to the new switch. To be able to add DHCP option 138, the DHCP server scope options will need to be edited, in the following examples, Windows Server 2016 is used. Option 138 is used in conjunction with Options 43 and 60.

From the DHCP scope, right click on IPv4 and “set Predefined Options”. Click on “Add” and enter the relevant controller information as shown below.
After clicking "OK", enter the controller’s IP address and select "OK".

**Aruba Controller Configuration**

Before configuring the controller, the MAC address of the switch to be provisioned needs to be captured. This can be done by executing the command “show system” at the switch:
switch# show system

Status and Counters - General System Information

System Name : Switch
System Contact :
System Location :

MAC Age Time (sec) : 300

Time Zone : 0
Daylight Time Rule : None

Software revision : YC.16.08.0002
ROM Version : YC.16.01.0002

Up Time : 21 hours
CPU Util (%) : 0

IP Mgmt - Pkts Rx : 613,583
Pkts Tx : 618,296

Memory - Total : 360,047,104
Free : 257,178,964

CPU Util (%) : 0

Lowest : 4829
Missed : 0

The MAC address above will then be added to the controller’s whitelist after disabling control-plane-security on the controller.

(Controller) [mynode] (config) #no control-plane-security
controller-plane-security
    no cpsec-enable

(Controller) #whitelist-db rap add mac-address 98:f2:b3:c0:a5:00 ap-group default
(Controller) #local-userdb add username 98:f2:b3:c0:a5:00 password 98:f2:b3:c0:a5:00
(Controller) #configure t
ip local pool "ARUBA-IPSEC" 10.88.88.10 10.88.88.50

ip access-list session aruba-acl any any tcp 22 permit
any any tcp 443 permit

user-role ap-role
access-list session aruba-acl

Since user role ap-role is already defined, the “aruba-acl” gets added as the last ACL.

Note: For production deployments, ClearPass should be used as the central point for all the whitelist entries.

When a factory defaulted switch is connected to the network, it will get its IP from the DHCP server and then try to establish an IPSEC tunnel with the controller.
From the DHCP Offer packet, the DHCP options can be seen, note Option 138 contains the Controller IP address.

To validate the IPSec tunnel is up, here are some useful commands:

```
switch# show amp-server
```

**AMP Server Configuration details**

- AMP Server IP: 10.5.8.18
- AMP Server Group: 2540
- AMP Server Folder: Top
AMP Server Secret        : admin
AMP Server Config Status : Configured

switch# show aruba-vpn type amp

Aruba VPN details

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba VPN Type</td>
<td>amp</td>
</tr>
<tr>
<td>Aruba VPN Peer IP</td>
<td>192.168.58.36</td>
</tr>
<tr>
<td>Aruba VPN Backup Peer IP</td>
<td></td>
</tr>
<tr>
<td>Aruba VPN Config Status</td>
<td>Configured</td>
</tr>
<tr>
<td>Aruba VPN tos</td>
<td>Value from IPv4 header</td>
</tr>
<tr>
<td>Aruba VPN ttl</td>
<td>64</td>
</tr>
</tbody>
</table>

switch# show interfaces tunnel brief

Status - Tunnel Information Brief

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>: tunnel-129</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>IPsec IPv4</td>
</tr>
<tr>
<td>Source Address</td>
<td>192.168.58.120</td>
</tr>
<tr>
<td>Destination Address</td>
<td>192.168.58.36</td>
</tr>
<tr>
<td>Configured Tunnel Status : Enabled</td>
<td></td>
</tr>
<tr>
<td>Current Tunnel State : Up</td>
<td></td>
</tr>
</tbody>
</table>

switch# show interfaces tunnel aruba-vpn

Tunnel Configuration :

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>: tunnel-129</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Name</td>
<td>aruba-vpn-tunnel</td>
</tr>
<tr>
<td>Tunnel Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Source Address</td>
<td>192.168.58.120</td>
</tr>
<tr>
<td>Destination Address</td>
<td>192.168.58.36</td>
</tr>
<tr>
<td>Mode</td>
<td>IPsec IPv4</td>
</tr>
<tr>
<td>TOS</td>
<td>Value from IPv4 header</td>
</tr>
<tr>
<td>TTL</td>
<td>64</td>
</tr>
<tr>
<td>IPv6</td>
<td>Disabled</td>
</tr>
<tr>
<td>MTU</td>
<td>1280</td>
</tr>
</tbody>
</table>

Current Tunnel Status :

| Tunnel State | : Up |
| Destination Address Route | 192.168.58.0/24 |
| Next Hop IP | 192.168.58.36 |
| Next Hop Interface | vlan-1 |
| Next Hop IP Link Status | Up |
Source Address : Configured on vlan-1
IP Datagrams Received : 0
IP Datagrams Transmitted : 0

Useful Controller Commands:

{Controller} ^[mynode] #show local-userdb

User Summary
----------------------
Name       Password  Role  E-Mail  Enabled  Expiry  Status  Sponsor-Name  Remote-IP  Grantor-Name
---------  --------  ----  ------  -------  ------  ------  ---------------  -------  ---------------
98:f2:b3:c0:a5:00  ********  guest  Yes  Active  0.0.0.0  admin

User Entries: 1

{Controller} ^[mynode] #show crypto ipsec sa

IPSEC SA (V2) Active Session Information
----------------------------------------
Initiator IP  Responder IP  SPI(IN/OUT)  Flags  Start Time
------------------  ----------  -----------  -----  -----------
192.168.58.120  192.168.58.36  c9d60c00/1ead187d  T2  Apr 18 15:22:23
192.168.58.195
Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
1 = uplink load-balance
Total IPSEC SAs: 1

{Controller} ^[mynode] #show crypto isakmp sa

ISAKMP SA Active Session Information
-------------------------------------
Initiator IP  Responder IP  Flags  Start Time  Private IP
---------------  ----------  -----  -----------  -------
192.168.58.120  192.168.58.36  r-v2-c  Apr 18 15:23:43  192.168.58.196
Flags: i = Initiator; r = Responder
m = Main Mode; a = Aggressive Mode; v2 = IKEv2
p = Pre-shared key; c = Certificate/RSA Signature; e = ECDSA Signature
x = XAuth Enabled; y = Mode-Config Enabled; B = EAP Enabled
3 = 3rd party AP; C = Campus AP; R = RAP; Ru = Custom Certificate RAP; I = IAP
V = VIA; S = VIA over TCP; 1 = uplink load-balance
Total ISAKMP SAs: 1

Sample Debug Outputs

Example Log Messages
I 01/01/90 00:12:44 00076 ports: port 1 is now on-line
I 01/01/90 00:12:44 000828 lldp: PVID mismatch on port 1 (VID 1) with peer device port 7 (VID 30) (1)
I 01/01/90 00:12:56 000833 dhcp: updating IP address and subnet mask
I 01/01/90 00:12:56 05177 ip: Setting IP address 10.10.30.1 as default gateway.
I 01/10/90 00:12:56 00025 ip: DEFAULT_VLAN: ip address 10.10.30.100/24 configured on vlan 1
I 01/10/91 00:24:09 00025 ip: DEFAUL_VLAN: ip address 10.10.3.10/24 configured on vlan 1
I 01/10/91 00:24:09 03783 dhcp: DHCP server did not offer all the DNS parameters on Primary VLAN
I 01/25/18 00:24:09 00413 snmp: Updated time by 885687073 seconds from server at 192.168.1.250. Previous time
was Mon Jan 1 00:12:56 1990. Current time is Thu Jan 25 00:24:09 2018.
I 01/25/18 00:24:09 03125 mgr: Startup configuration changed by SNMP. New seq. number 2
I 01/25/18 00:24:13 05101 amp-server: AMP server details configured.
I 01/25/18 00:24:09 05101 amp-server: AMP server configuration is disabled due to first configuration.
I 01/25/18 00:24:07 05306 ZTP mairwaveCtrl: L3 IPv4 Tunnel Interface: Tunnel ID 129 (4874) created.
I 01/25/18 00:24:07 05101 amp-server: AMP server registration started through Primary VLAN.
I 01/25/18 00:24:13 04611 job: Job Scheduler enabled.
I 01/25/18 00:24:19 05304 ZtpIpsec: IKE session initialization with peers 10.10.30.100 and 192.168.1.253 was successful.
I 01/25/18 00:24:19 05306 ZtpIpsec: IKE Security Association (SA) negotiation with peers 10.10.30.100 and 192.168.1.253 was successful.
D 01/25/18 00:24:19 05319 ZtpIpsec: IKE_SA Created
D 01/25/18 00:24:19 05325 ZtpIpsec_SA Created
I 01/25/18 00:24:19 05102 amp-server: AMP server registration started through Primary VLAN.
I 01/25/18 00:24:19 05310 ZtpIpsec: IPv4 route to Airwave Controller 10.99.99.15 via IPsec tunnel interface: Tunnel ID 129.
I 01/25/18 00:24:19 05308 ZtpIpsec: IPSec VPN Tunnel ID 129 successfully established with peers 10.10.30.100 and 192.168.1.253.

Example ZTP Debug Output
switch# debug ztp
switch# debug destination session
0000:00:01:00:64 ZTP mairwaveCtrl:Received message 0x2200060
0000:00:01:06.21 ZTP mDHCPcLint:Received option - OPTION_CAPWAP_AC_V4
0000:00:01:11.29 ZTP mDHCPcLint:Access Controller IP address = 10.88.88.10 configured on tunnel 129
0000:00:01:14.21 ZTP mDHCPcLint:Received option - OPTION_CAPWAP_AC_V4
0000:00:01:14.69 ZTP mDHCPcLint:Access Controller IP address = 10.88.88.10 configured on IPsec tunnel interface: Tunnel ID 129.
0000:00:01:14.86 ZTP mDHCPcLint:Device registration to AMP server successful.
0000:00:01:16.19 ZTP mDHCPcLint:Device registration to AMP server successful.
0000:00:01:17.09 ZTP mDHCPcLint:Device registration to AMP server successful.
0000:00:01:17.60 ZTP mDHCPcLint:Device registration to AMP server successful.
0000:00:01:16.73 ZTP mairwaveCtrl:Added X-Shared-Secret: aruba123
0000:00:01:16.80 ZTP mairwaveCtrl:Added X-Device-State: Factory
0000:00:02:29.23 ZTP mairwaveCtrl:Switch registration failed - Error string: Couldn't connect to server
0000:00:02:29.30 ZTP mairwaveCtrl:Registration with AMP server failed. Scheduling retry in 60 seconds
0000:00:02:29.38 ZTP mairwaveCtrl:Received message 0x91000B
0000:00:02:29.56 ZTP mairwaveCtrl:IPSEC ZTP: In Health-Check timer
0000:00:02:29.63 ZTP mairwaveCtrl:IPSEC ZTP: Switch sends HB
0000:00:02:29.70 ZTP mairwaveCtrl:Received message 0x91000B
0000:00:02:29.80 ZTP mairwaveCtrl:Received message 0x910002
0000:00:02:29.91 ZTP mairwaveCtrl:Default, Primary or Management VLAN is configured with DHCP
0000:00:02:30.05 ZTP mairwaveCtrl:AMP server registration started through Primary VLAN.
0000:00:02:30.15 ZTP mairwaveCtrl:Check-in to Airwave through IPsec
0000:00:02:30.23 ZTP mairwaveCtrl:Sending request to https://10.99.99.15/switch_https
0000:00:02:30.33 ZTP mairwaveCtrl:Added X-Type: Device-Reg
0000:00:02:30.43 ZTP mairwaveCtrl:Added X-Device-State: Factory
0000:00:02:30.53 ZTP mairwaveCtrl:Added X-Device-Info: CN6BHKZ1RQ, B0:5A:DA:98:9A:00, 2930F-8G-PoE+-2SFP+ Switch
0000:00:02:30.63 ZTP mairwaveCtrl:Added X-Group: LAN switches
0000:00:02:30.73 ZTP mairwaveCtrl:Added X-Folder: Branch1
0000:00:02:30.83 ZTP mairwaveCtrl:Added X-Shared-Secret: aruba123
0000:00:02:30.93 ZTP mairwaveCtrl:Switch registered Successfully - HTTP/1.1 200 OK Server: nginx Date
0000:00:02:31.03 ZTP mairwaveCtrl:Registration with AMP server successful. Scheduling periodic checking for 3600 seconds.
PROVISIONING WITH ARUBA CENTRAL

Group Creation and Device Assignment

In order to provision devices using Aruba Central, they must first be assigned to a configuration group. There are two types of configuration groups: the default group type utilizes UI-based settings and offers a subset of ArubaOS-Switch features, while template groups provide full access to the switch feature set via configuration templates, which can be adapted to apply to various device types and use variables to apply different values to a group of devices from the same base template.

To create a configuration group in the Central UI, open Global Settings, then select Manage Groups. Click or tap the New Group button in the bottom left corner, under the group list.

In the Create New Group dialog, give the new group a name. If the new group will use UI-based settings, enter a group password as prompted. If this will be a new template group, check the USE AS A TEMPLATE GROUP box. Select Add Group to create the new group.

You can also create a new UI-based configuration group by importing the existing configuration from a device in the list. Select the switch you wish to use as the configuration source, then click or tap Import Configuration to New Group. Enter a group name and assign a password, then select Import Configuration.

Once the group has been created, select one or more devices from the list on the right (hold Control on Windows or Command on macOS to select multiple devices at once) and drag them to the target group in the list to the left to assign them to that group. You will be presented with the dialog pictured to the right; select Yes to confirm the move, or No to cancel.

UI-based Group and Device Configuration

Use the CURRENT APP navigation menu to open Wired Management. Switches can be managed by group or by individual device; use the filter menu at the top of the page to select either the group you created or an individual switch. Note that, when configuring at the group level, the switch port configuration page displays 52 ports as a group may contain 8-port, 24-port, or 48-port switches (some with 2 or 4 dedicated uplink ports each, for a total of 10, 28, or 52 ports, respectively).

When any setting on a page has been changed, you will need to commit those changes using the Save Settings button in the bottom-right corner before leaving the page. If you attempt to leave the page without saving, a warning prompt will be displayed; choose Continue to remain on the current page (keeping changes intact), or Discard to revert your changes and navigate to the new page.
Basic switch settings can be changed by highlighting a switch in the list, and clicking the pencil-shaped edit button in the rightmost column.

Settings that can be changed here are the hostname and IP address assignment (DHCP or static).

Navigate through each configuration section to configure interfaces, VLANs, ACLs, and other settings. Once the group-level configuration is complete, provision devices in that group by powering them up and connecting them to a network that provides internet connectivity, either directly or via a proxy server (configurable via DHCP option).

**Template-based Group Configuration**

After creating a template-based configuration group and adding at least one device to it, navigate to CURRENT APP ➔ Wired Management. From the filter bar at the top of the page, select the group you just created from the list under GROUPS; it will have the letters TG just to the left of the group name.

To create a new template, open the Templates page and click the + link near the bottom left of the template list.
Give the template a unique name, and for **Device**, select **Aruba Switch**. The Model and Version fields can either be left at **ALL** or set to a specific switch series and major software release (16.03 through 16.08). If a specific switch model or software version are selected, the template will be applied only to switches in the group that match those criteria.

To import a baseline configuration to build the template from, select a device from the list presented, then click or tap **Import Template**.

The resulting template can be modified to suit the desired configuration for the group, using variables (either Central-defined or custom) for device-specific values. For more information on template and variable management, refer to the **Central documentation**.

Once you have finished editing the template and are ready to apply it to switches in the group, select **Save** in the bottom-right corner of the template editor.

If any applicable switches in the group are currently online and being managed by Central, the new or updated template should be pushed to them within 1-2 minutes.

**Provisioning sequence with Activate and Central**

Once the switch boots from a factory default state and acquires a DHCP address with DNS server information, the following events will occur in order:

- The switch will attempt to resolve the Activate server URL to an IP address, and if successful, will attempt to reach the Activate service for initial provisioning. (If a proxy server is configured via DHCP, the switch will use the proxy server to establish connections to Activate and Central.)
- Once connected to Activate, the switch will attempt to synchronize its clock using NTP, then HTTP Time Protocol with the Activate time server (even if time is already synchronized from a local time server configured via DHCP; in this case, the local time synchronization should prevail).
- Activate then pushes a Trust Anchor certificate to the switch to secure communications.
- Activate will determine which management platform the switch needs to register with (Central or AirWave). If the switch has been added to Central, added to a license subscription, and assigned to a group, the URL for the provisioned Central instance will be pushed to the switch.
- The switch connects to the configured Central instance and loads the Central SSL certificate.
- Central begins polling and pushes the applicable configuration (UI-based or template) to the switch.

To view the status of Activate provisioning, use the following command:

```
switch# show activate provision
```

**Configuration and Status - Activate Provision Service**

```
Activate Provision Service : Enabled
Activate Server Address   : device.arubanetworks.com
```
Activation Key : XXXXXXXX
Time Sync Status : Time sync from HTTP Time Protocol
Activate DNS Lookup : Success
Proxy Server DNS Lookup : Success
Activate Connection Status : Success
Error Reason : Time sync has failed from NTP pool

For the status of the Central connection, use this command:

switch# show aruba-central

Configuration and Status - Aruba Central

Server URL : https://portal.central.arubanetworks.com/ws
Connected : Yes
Mode : Monitor
Last Disconnect Time : Thu Apr 18 14:43:19 2019
Server DNS Lookup : Success
Proxy Server DNS Lookup : Success
Error Reason : NA

ZERO TOUCH PROVISIONING WITH DHCP AND TFTP

This method utilizes DHCP vendor classes and options to point the switch at a TFTP server to acquire firmware images and configuration files. This requires switches using this method to be provisioned on a network from which the TFTP server is reachable, and the server must host software images and configuration files compatible with each model of switch to be provisioned.

Create vendor class on DHCP server

First, obtain the vendor class string from each switch model to be provisioned. This can be done using the following command:

switch# show dhcp client vendor-specific

Vendor Class Id = Aruba JL258A 2930F-8G-PoE+-2SFP+ Switch
Processing of Vendor Specific Configuration is enabled

The section in bold must be copied in its entirety and used to create a vendor class on the DHCP server; for the examples that follow, the Windows Server 2016 DHCP Server was used. For other DHCP server implementations, refer to the appropriate platform documentation.

From the DHCP management window, expand the tree in the left-hand navigation pane, right-click the IPv4 list item, and select Define Vendor Classes...
In the window that opens, select **Add**..., then give the new vendor class a unique name and description (either or both may include the part number and/or model name for quick reference).

In the **ASCII** field, type in the full vendor class string obtained from the switch (copying and pasting may not function in this field). Once this is done, select **OK** to save the new class, and **Close** to return to the main DHCP management window.

**Set Predefined Options**

Right-click the **IPv4** item again, and select **Set Predefined Options**...

In the **Predefined Options and Values** window, select the newly-created vendor class from the **Option class** dropdown list, and then click or tap **Add**...

Name the new option “Configuration File”; set the **Data type** to **String**, assign the **Code** a value of **144**, and give the option an appropriate description (see example pictured). Click **OK** to save.

Repeat this process, naming the second new option “Firmware File”; set **Data type** to **String** and **Code** to **145**, and add a description. Click **OK**, then click **OK** again to dismiss the **Predefined Options and Values** window.

In the main DHCP management window, browse to an IPv4 scope and expand it in the list. Right-click the **Scope Options** list item and select **Configure Options**...
Select the **Advanced** tab. Under the **DHCP Standard Options** vendor class, locate option **066 Boot Server Host Name** and check the box. In the **String value** field, enter the IP address of the TFTP server hosting the configuration and/or firmware files.

Now, select the vendor class created earlier from the dropdown list. You should see the two just created predefined options in the list. Check the box next to one or both of them, and set their string values to the configuration and firmware filenames, as stored on the TFTP server. Click **OK** to apply the selected options to the DHCP scope.

In the DHCP Scope Options view, you should now see the three new options and their configured values.

When a switch is connected to the network and acquires a DHCP IP address in this scope, it will attempt to connect to the TFTP server specified by option 66 and first download the firmware image in suboption 145, if configured. If the download is successful, the firmware image will be verified and copied to the primary flash. Regardless of the result, the switch will then attempt to download the configuration file from suboption 144; if successful, the configuration will be validated for compatibility. If the configuration is determined to be valid for the switch model and firmware version, it will replace the default startup configuration and the switch will reboot. This process may take up to 2-3 minutes from initial boot.

To prevent the switch from repeating the ZTP process on subsequent reboot cycles, it is recommended that the configuration file on the TFTP server contain the following commands:

- `no dhcp config-file-update`
- `no dhcp image-file-update`

This will result in the switch ignoring DHCP suboptions 144 and 145 when acquiring a DHCP IP address on the configured scope.
SUPPORTED PLATFORMS

Zero-Touch Provisioning is supported on the following Aruba switch families:

- Aruba 2530 Switch Series
- Aruba 2540 Switch Series
- Aruba 2930F Switch Series
- Aruba 2930M Switch Series
- Aruba 3810M Switch Series
- Aruba 5400R Switch Series