

Central / Configuration Example

 17-Nov-25

Central Configuration Example

This chapter explores using Central's configuration model to configure a WLAN for APs and a Layer-2 access switch. It does not provide a complete reference configuration, but is intended to illustrate the power and functionality of element profiles.

▼ Table of contents

- Central Configuration Example
 - Element Profile Configuration Process
 - Apply Element Profiles
 - Configure Global Profiles
 - Configure Access Switch
 - General Switch Configuration
 - Uplink Port Configuration
 - Port Standardization
 - Configure Bridged WLAN

Feedback

Element Profile Configuration Process

All profiles are created using the same general process. The following steps create an **AAA Authentication** profile, and assign it a Device Function and Scope. This example can be used to create additional profiles to establish a fully functioning solution.

Step 1 Click the **Gear** icon in the upper right hand corner of the window to enter configuration mode.

Step 2 Click **Library** in the left-hand navigation pane to display the configuration context path.

Step 3 Click **Manage** in the Security tile to view all profile types this category.

Note: Element Profiles are grouped into category tiles. The **AAA Authentication** profile type is located in the **Security** tile. Clicking **Manage** in a tile category displays all the profiles available in that category. Use the buttons at the bottom of a tile to move through the tile's pages. In this example, the **AAA Authentication** profile type appears on the first page. When the desired profile type is displayed in the tile, click the profile type to select it.

HPE aruba Central (Public Preview)

GLOBAL Configuration Overview
Information about the Library

Library 2

Global

Site Collections 6 collections

Sites 22 sites

Devices 122 devices

Device Groups 15 groups

Profiles Roles & Policies Named Objects Services

Profiles Management
Device Function: All

Category	Type	Profiles
Application Experience	App Recognition and Control	5
	Manage	
Interfaces	AP Uplink	0
	Device Profile	1
	Fault Monitoring	0
	Management Interface	1
Network Services	DHCP Pool	1
	DHCP Relay	0
Routing & Overlays	BFD	1
	Static Routing	4
	Route Maps	1
	BGP	0
Security	AAA Authentication	17
	Authentication Server	9
	Authentication Server Group	12
	Captive Portal Authentication	1
System	AP System	1
	DNS Server	7
	Dump Server	0
	Dynamic DNS	0
Tunnels	GRE Tunnel	0
	GRE Tunnel Group	0
VLANs & Networks	Named VLANs	11
	STP	4
	VLAN	38
	VRRP Global	0
Wireless	Mesh	0
	MPSK	1
	RF	3
	Wireless IDS/IPS	3

Step 4 Click **Manage** on the **AAA Authentication** profile type.

The screenshot shows the 'Profiles Management' page. On the left is a 'Library' sidebar with categories: Global, Site Collections (6 collections), Sites (22 sites), Devices (122 devices), and Device Groups (15 groups). The main header has tabs: Profiles, Roles & Policies, Named Objects, and Services. Below the header, there's a breadcrumb 'Library > Security' and a 'Device Function' dropdown set to 'All'. The main content area displays three profile categories: 'AAA Authentication' (Manage AAA Authentication Profiles, 17 Profiles, with a 'Manage' button), 'Captive Portal Authentication' (Manage Captive Portal Authentication Profiles), and 'Authentication S...' (Manage Authentication Profiles). There is also an 'EST' section for 'Manage EST Profiles'.

Step 5 On the **AAA Authentication** profile page, click **Create Profile**.

The screenshot shows the 'AAA Authentication' profile page. The breadcrumb is 'Library > Security > AAA Authentication'. There is a search bar with the text '17 items' below it. On the right side, there is an orange 'Create Profile' button and a dropdown menu icon.

Step 6 In the **Create Profile** window, assign the following settings and click **Create**.

- **Name:** *New-AAA-Profile*
- **Authentication Protocol:** *802.1X*
- **802.1X Authentication Server Group:** *Global Radius*
- **Accounting Server Group:** *Global Radius*

Create Profile ✕

Name *

New-AAA-Profile

Description

Authentication Protocol *

802.1X ▼

Client Limit

802.1X Authentication Server Group

Global-Radius ▼

Authentication Parameters

☐ Switch Specific Parameters

Authorization Parameters

☐ Switch Specific Parameters

Accounting

☐ Interim RADIUS Accounting

Accounting Server Group

Global-Radius ▼

802.1X Parameters

Max Authentication Failure

☐ Reauthentication

☐ Switch Specific Parameters

Create

Note: Profiles often reference other profiles in their configuration. In this example, the **Global Radius** Authentication Server Group and its member servers must be created before the current profile.

After creating the profile, it is added as a shared profile to the Library, but its configuration is not applied to devices until a **Device Function** and **Scope** are applied.

Apply Element Profiles

Assigning a Device Function applies the profile to devices based on their role in the network, such as campus access points or aggregation switches. Assigning the scope allows administrators to select which devices are assigned the profile based on organizational structure or device groups. These two attributes are evaluated together using Central's **inheritance** logic to apply the profile to devices.

Step 1 Select the desired element profile in the library, hover the cursor over the profile entry, and click the **triple dots (⋮)**.

Profiles

Roles & Policies

Named Objects

Services

Library > Security > AAA Authentication

Create Profile

⌵

17 items

Name	Assigned Device Function	Assigned Scope
ACCESS-DOT1X-MAC	Mobility Gateway	Global
New-AAA-Profile	-	-

Step 2 On the popup menu, click **Assign**.

Profiles

Roles & Policies

Named Objects

Services

Library > Security > AAA Authentication

Create Profile

⌵

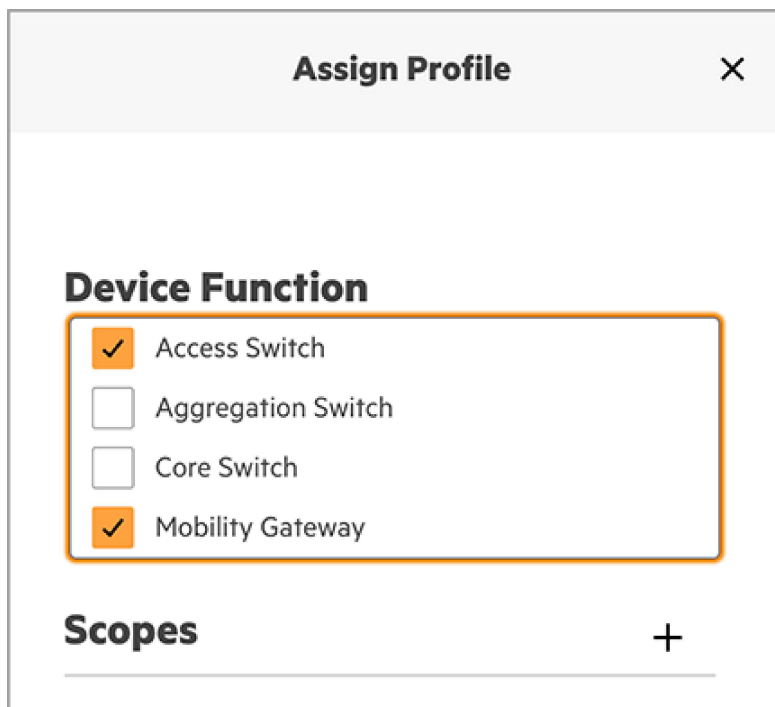
17 items

Name	Assigned Device Function	Assigned Scope
ACCESS-DOT1X-MAC	Mobility Gateway	Global
New-AAA-Profile	-	-
OWL AAA Auth Settings	Access Switch	HERCP-CNX
RSVCP-WLAN-8021x_1757000365281129448_	Mobility Gateway	RSVCP-New-Central-WLAN

Assign

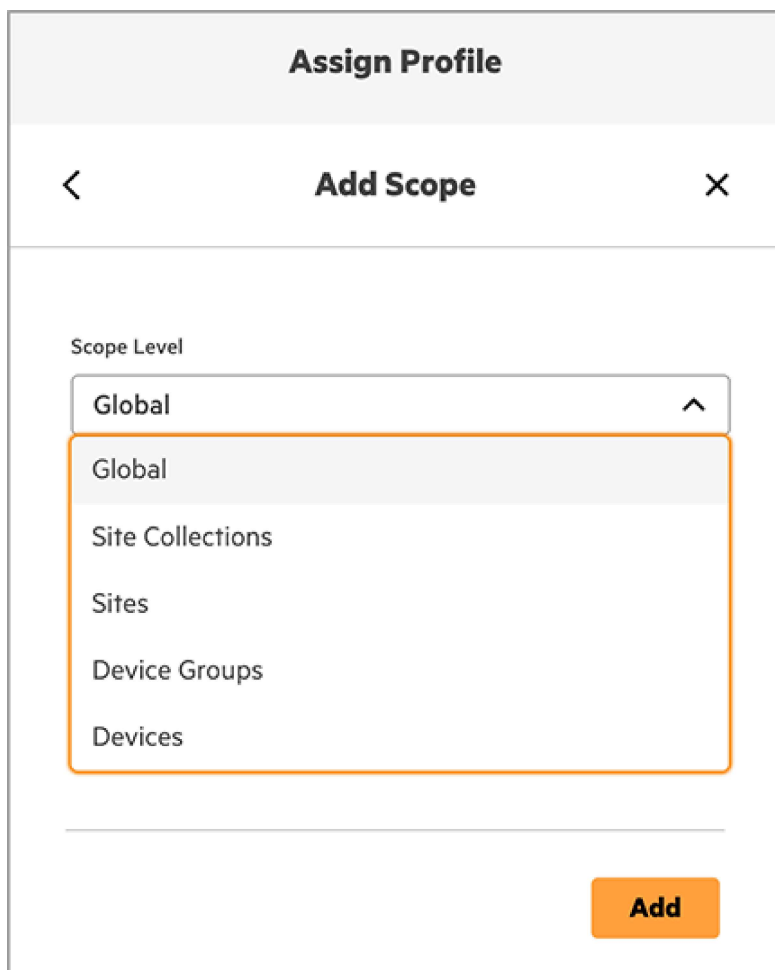
Unassign

Step 3 Select the **Device Function(s)** for the profile, then click the plus sign (+) beside **Scopes**.



The **Assign Profile** dialog box has a close button (X) in the top right. Below the title bar, the **Device Function** section contains a list of four options, each with a checkbox:
- ☒ Access Switch
- ☐ Aggregation Switch
- ☐ Core Switch
- ☒ Mobility Gateway
This list is enclosed in an orange border. Below this section, the **Scopes** section has a plus sign (+) to its right.

Step 4 In the **Add Scope** window, select the **Scope Level**, then click **Add**.



The **Assign Profile** dialog box contains a sub-dialog titled **Add Scope**. The sub-dialog has a back arrow (<) on the left and a close button (X) on the right. Inside the sub-dialog, the **Scope Level** section features a dropdown menu currently showing **Global** with an upward arrow (^) to its right. An orange border highlights the dropdown menu and its expanded list of options:
- Global (highlighted)
- Site Collections
- Sites
- Device Groups
- Devices
At the bottom right of the sub-dialog is an orange **Add** button.

Note: When selecting Site Collections, Sites, Device Groups, or Devices as a scope, an additional assignment of a specific instance within the scope is presented in a context-based dropdown menu. For example, when choosing Site as a scope, another dropdown enables selection of one or more sites.

Step 5 Click **Assign** to assign the Device Function(s) and Scope(s) to the profile.

Assign Profile

Device Function

☒ Access Switch

☐ Aggregation Switch

☐ Core Switch

☒ Mobility Gateway

Scopes

Name

Global

Scope Level

Global

Assign

After completing the assignment, the profile's configuration is pushed to appropriate devices based on the rules of inheritance.

Configure Global Profiles

Element profiles applied to all or most of an organization are typically assigned at the Global scope. A small number of exceptions can be managed by using profile overrides or by assigning additional profiles at different scopes, which use inheritance to replace the Global profiles with customized settings.

It is common to apply the profiles in the following table globally, since they can often be used across an entire organization and on all device functions.

Each profile is populated with an operating-system agnostic set of parameters. When Central applies the configuration to specific devices, it uses the syntax appropriate for each platform.

The profile list is suggested to establish a base set of configurations for network services. This includes configuring AAA Authentication to define how users and devices are authenticated to the network, and Authentication Server and Authentication Server Group profiles to define a centralized authentication source such as ClearPass. Additionally, System profiles such as NTP Server, DNS Server, and System Administration are set to ensure that all devices have synchronized time, can resolve hostnames, and are configured for secure management access.

Element Profile	Device Function	Scope	Note
Security > Authentication Server	All	Global	Each Authentication Server profile defines an individual AAA server, such as a ClearPass server. Multiple Authentication Server profiles are required, one for each AAA server in the network.
Security > Authentication Server Group	All	Global	Each Authentication Server Group profile defines a group of AAA servers, and multiple groups are treated in an additive manner.
Security > AAA Authentication	All	Global	Each AAA Authentication profile defines a method to authenticate network hosts to a AAA server, including 802.1X and MAC-Authentication. Dynamic authorization is enabled to honor AAA server change the authorization (CoA) requests.
System > NTP Server	All	Global	The NTP Server profile defines a set of NTP servers to ensure that all devices have synchronized time. Time synchronization is vital for security, logging, and system management. It is best practice to set at least two NTP servers in a profile. Only a single NTP Server profile is applied to each device using the rules of inheritance.
System > DNS Server	All	Global	The DNS Server profile defines a set of DNS servers so network devices can resolve hostnames. It is best practice to set at least two DNS servers in the profile. Only one DNS Server is applied to each device using the rules of inheritance.
System > System Administration	All	Global	The System Administration profile configures local, RADIUS, and TACACS authentication types used by SSH, web, and console services.

Configure Access Switch

Access switches inherit the profiles defined above because they were assigned to the Global scope and all Device Functions. The element profiles in the subsections below complete the access switch configuration.

General Switch Configuration

The following element profiles establish the general configuration settings for access switches. Key element profiles to include are VLANs for user traffic and for switch management, Spanning Tree Protocol (STP) to prevent loops in the network, VSF for switch stacking, and a Device Profile to ensure that connected access points are automatically provisioned. Additional profiles are noted with a description of their purpose.

Element Profile	Device Function	Scope	Description
System > Switch System	Access Switch	Site	The Switch System profile sets the timezone, enables unsupported transceivers, enables AAA globally on the switch, and enables telemetry for CX switches.
System > Source Interface	Access Switch	Site or device	The Source Interface profile configures an interface to source traffic originated from the switch, such as RADIUS requests, NTP queries, etc.
Security > UBT	Access Switch	Site	The UBT profile enables UBT, creates a UBT zone, and associates a gateway cluster to UBT traffic.
VLANs & Networks > VLAN	Access Switch	Site	An individual VLAN profile is created for the management VLAN and each user VLAN.
VLANs & Networks > VLAN	Access Switch	Device (Local Override)	A local override is created for each VLAN profile that requires an IP address assignment. An access switch typically requires only one override for the management VLAN. The override forks the profile from the site level and creates a new local profile at the device level.
VLANs & Networks > STP	Access Switch	Site	The STP profile enables MSTP by default. Access switches typically use the default STP priority of 8 (the STP priority on aggregation switches is generally set to 4).
Routing & Overlays > Static Routing	Access Switch	Site	The Static Routing profile is used to create a default route for the in-band management network. A single Static Routing profile can contain multiple static routes, but the profiles are applied in an additive manner, so multiple Static Routing profiles can be applied to the same device.
Network Services > DHCP Snooping	Access Switch	Site	This profile enables DHCP snooping and its associated options, including trusted servers.
High Availability > VSF	Access Switch	Device-Group	This VSF profile configures Layer 2 VSF stacking for simplified management and redundant Layer 2 connectivity to the aggregation layer.

Element Profile	Device Function	Scope	Description
Interfaces > Device Profile	Access Switch	Site	A Device Profile defines a set of OUI and system description parameters used to auto-assign access points to the ARUBA-AP role.

Uplink Port Configuration

An element profile at the device level creates a Link Aggregation Group (LAG) as an 802.1Q trunk. This provides link redundancy to the aggregation layer and allows the uplinks to carry all host VLANs. Also, enable LACP for active-mode port bundling and enable DHCP snooping trust.

Element Profile	Device Function	Scope	Description
Interfaces > Switch Interface Configuration	Access Switch	Device	The Switch Interface Configuration profile for an individual switch or switch stack allows creating a LAG with common parameters such as LACP.

Port Standardization

The following profiles enable the administrator to create and apply a standardized configuration for access switch edge ports. A comprehensive Port Profile is created to define common settings for administrative state, speed, PoE, and VLAN assignment. This profile also incorporates essential security measures such as Loop-Protect and BPDU Guard to protect the network from loops. The Port Profile is then applied to physical switch interfaces, ensuring that all access ports have a consistent and secure configuration.

Element Profile	Device Function	Scope	Description
Interfaces > Port Profile	Access Switch	Site	Each Port Profile contains a standardized switch port configuration. Multiple Port Profiles can be defined to accommodate different port functions (e.g., host facing ports or uplink ports).
Interface > Switch Interface Configuration	Access Switch	Device	The Switch Interface Configuration profile at the device level is used to assign port profiles to physical and logical switch ports.

Configure Bridged WLAN

In this example of element profiles, a WLAN in bridged mode is configured. The profiles below combined with the Global profiles above support a WLAN configured for WPA3 personal as an authentication method. A full WPA3 Enterprise implementation requires additional profiles (Authentication Server, Authentication Group, and AAA Authentication profiles).

Note: If Mobility Gateway tunneling is implemented, the scope of the element profiles must change from Global or Site to Device Group to support the current implementation of Gateway Clusters.

The switch port connected to an AP used for bridged WLANs requires a trunk port setting, where the native VLAN is typically set to a management VLAN, and WLAN traffic is bridged to a tagged VLAN.

Element Profile	Device Function	Scope	Description
VLANs & Networks > Named VLANs	Campus Access Point	Site or Global	Each Named VLAN profile contains a list of one or more user VLANs. This profile can then be referenced by WLAN profiles for VLAN assignment of bridged traffic. Each VLAN listed in the profile must have a corresponding VLAN profile created for the switch infrastructure. The VLAN profile for switches is not tied directly to the Named VLANs profile for Campus Access Points.
Interfaces > AP Uplink	Campus Access Point	Global	For a bridged WLAN, the AP Uplink profile defines a trunk port with the native VLAN set to the management VLAN. It is critical to ensure that settings, including allowed VLANs, match the corresponding switch uplink port.
Wireless > WLAN	Campus Access Point	Site or Global	Each WLAN profile assigns an SSID name, bridge mode, WPA3 PSK password, and the Named VLAN for bridging traffic. A Default Role is auto-created for a bridged SSID and can be later modified in Library > Roles and Policies .

[Privacy](#)[Terms of Use](#)[Ad Choices & Cookies](#)[Do Not Sell or Share My Personal Information](#)[Sitemap](#)

© Copyright 2024 Hewlett Packard Enterprise Development LP