Solution overview

HPE Aruba Networking Central NAC

Introduction

Network Access Control (NAC) serves as a pivotal element of network defense, empowering IT teams to enforce secure access to networks. By authenticating and authorizing users and devices before granting them access to the network, NAC enables organizations to implement the zero trust security at the network level. With modern security threats, rising cost of network breaches, and accelerated adoption of Internet of Things (IoT) and bring your own device (BYOD), the use cases for NAC have evolved over time.

A recent study conducted by Ponemon Institute highlights that more than half of organizations (54%) in 2024 use NAC solutions, an increase from 32% in 2023.[1] The same study highlights that high performing security organizations—those considered highly effective in keeping up with threats and closing security gaps place a higher value on NAC solutions and the integration of NAC functionality than others.

NAC has traditionally been delivered through an on-prem solution; however, the accelerated migration of enterprises to cloud, coupled with the stability and trust in SaaS model, and the demand for simple-to-use solutions, have created a growing need for a cloud-delivered NAC solution. This solution must offer the same reliability as traditional on-premises NAC while providing the added benefits of simplicity and scalability.

HPE Aruba Networking, known for its highly-rated on-premises NAC solution ClearPass, has leveraged its expertise to create HPE Aruba Networking Central NAC, a cloud-based NAC solution with robust security capabilities.

What is NAC?

Learn more about HPE Aruba Networking ClearPass Policy Manager

[1] "The 2025 Global Study on Closing the IT Security Gap," Ponemon Institute Research Report, 2025.

What is HPE Aruba Networking Central NAC?

HPE Aruba Networking Central NAC is a robust, cloud-delivered NAC solution that offers advanced authentication, authorization, and seamless guest access. The solution caters to customers of all sizes and needs, offering turnkey and simplified solutions to implement zero trust security for small and mid-sized organizations, and supporting advanced NAC functionalities for larger enterprises.

HPE Aruba Networking Central NAC is **built-in** from group-up in the HPE Aruba Networking Central, terminating the need for **bolted-on** security solutions and enabling HPE Aruba Networking Central NAC to leverage the AI capabilities of HPE Aruba Networking Central for client visibility and profiling. As a cloud-native platform, HPE Aruba Networking Central NAC offers quantifiable business benefits, including:

— **Ease of use:** A highly intuitive interface supporting at-a-glance analytics and straightforward policy management, reducing time to value and lowering the learning curve for new IT employees.

— **Robust security:** Developed by the team behind HPE Aruba Networking ClearPass, bringing proven security capabilities to the cloud.

— **Cloud scalability:** Organizations can effortlessly scale NAC controls to support a growing and geographically distributed workplace and workforce, without infrastructure bottlenecks.

— **Reduced operational expense:** Cloud delivery minimizes hardware needs and reduces ongoing management overhead, driving down operational expenditures.

Secure by design approach: Central NAC is built from group up to protect customers' data, it only uses the data it needs and keeps it locked to customers' tenant. This helps maintain privacy, security, and compliance with regulations like GDPR.

HPE Aruba Networking Central NAC is pivotal to delivering HPE's vision of secure AI-native networking that enables all enterprises, irrespective of size, to deploy the core NAC security without any additional cost. Central customers can leverage core NAC features (also referred as Central NAC (core)) like authentication, authorization, visitor access, and captive portal customization at no additional cost. For customers seeking to implement advanced or pro NAC functionalities (also referred as Central NAC (pro)) like BYOC, support for multiple IdPs, 3rd party NAD support, and more contextual driven policies implementation, need to buy additional NAC subscription.

i): HPE Aruba Networking Central NAC (core): Available to all HPE Aruba Networking Central customers without any additional cost: Provides seamless, secure way to onboard and authenticate end users and nonuser devices (cameras, printers, IoTs, and so on) to wired and wireless networks using integration with cloud identity stores such as Google Workspace™, Microsoft Entra ID, and Okta Workforce. Supports EAP-TLS, MAC Authentication, Captive Portal Authentication, and MPSK (Admin and user managed). Offers a robust visitor access control and a highly customizable captive portal design engine.

ii): HPE Aruba Networking Central NAC (pro): NAC subscription license is required to activate pro features: Provides advanced NAC functionalities such as additional policy definition controls for authentication and authorization, bring your own certificates (BYOC), third-party NAD support, and use of multiple Identity Provider (IdP), along with all the HPE Aruba Networking Central NAC (core) features mentioned earlier. Note that: HPE Aruba Networking Central NAC (pro) license is counted as per concurrent connected client.

Equipped with an intuitive interface, integrated Cloud Guest engine, and seamless Air Pass support, HPE Aruba Networking Central NAC makes it easy to onboard new clients, as well as to monitor and troubleshoot issues that prevent users from connecting to the network. End users are authenticated and provided authorizations for appropriate network access through fine-grained policies as configured by the administrator in HPE Aruba Networking Central.

How does HPE Aruba Networking Central NAC work?

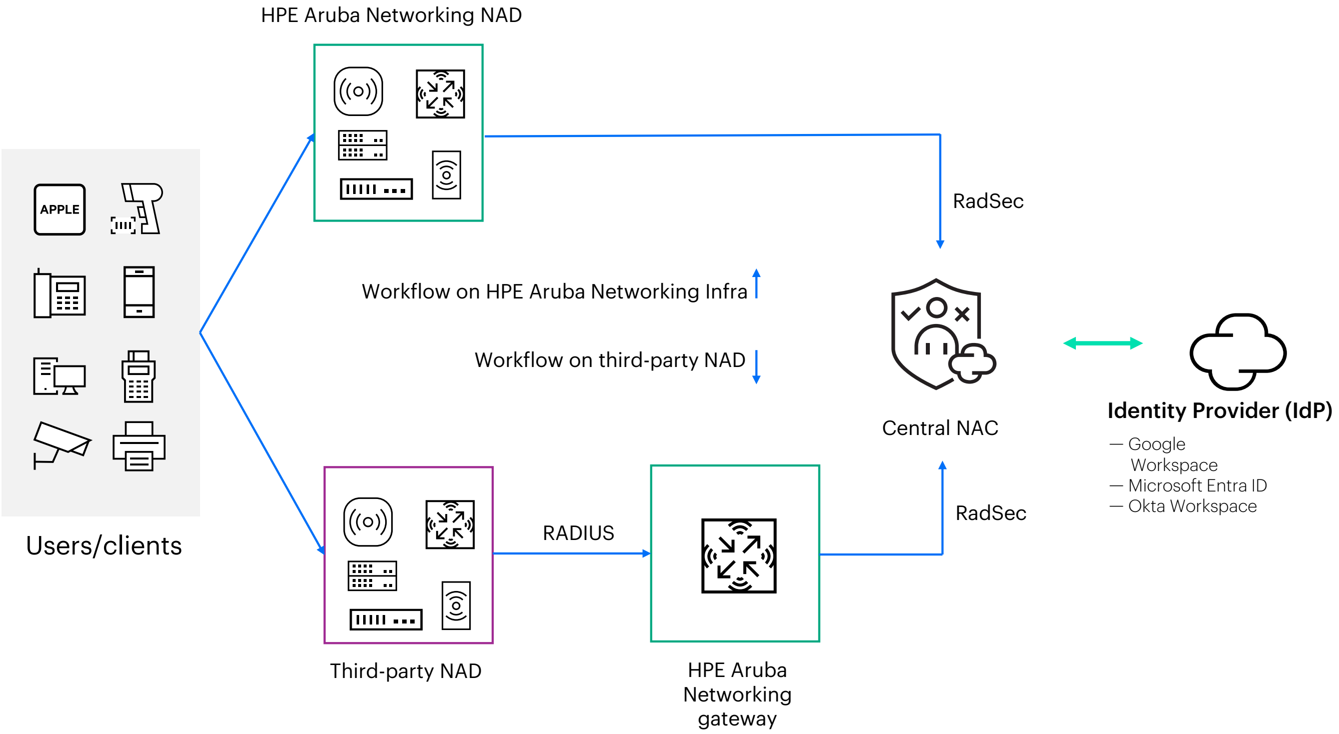


Figure 1. HPE Aruba Networking Central NAC workflow

HPE Aruba Networking Central NAC unifies security policies across campus, branch, and data centers—in a multivendor environment. As shown in Figure 1, devices connect through managed switches or access points, establishing secure RadSec tunnels to the HPE Aruba Networking Central NAC RADIUS server using factory-installed certificates. In a multivendor environment, a third-party NAD device communicates with HPE Aruba Networking gateway using RADUIS, and the gateway then establishes RadSec tunnels to communicate with HPE Aruba Networking Central NAC. User identities are verified through integrations with cloud Identity Providers (IdP) such as Google Workspace, Microsoft Entra ID, and Okta, allowing administrators to assign roles and enforce policies consistently. For IoT devices, MAC-based access control is supported.

Note: HPE Aruba Networking Central NAC requires HPE Aruba Networking CX Operating System or HPE Aruba Networking Wireless Operating System to work. For third-party NAD support, HPE Aruba Networking Central NAC requires HPE Aruba Networking
gateway version 10.7.2 or later.

HPE Aruba Networking Central NAC provides an intuitive NAC engine to configure

i): Authentication profiles

ii): Authorization policies

iii): Identity management

iv): Visitor access

v): Messaging

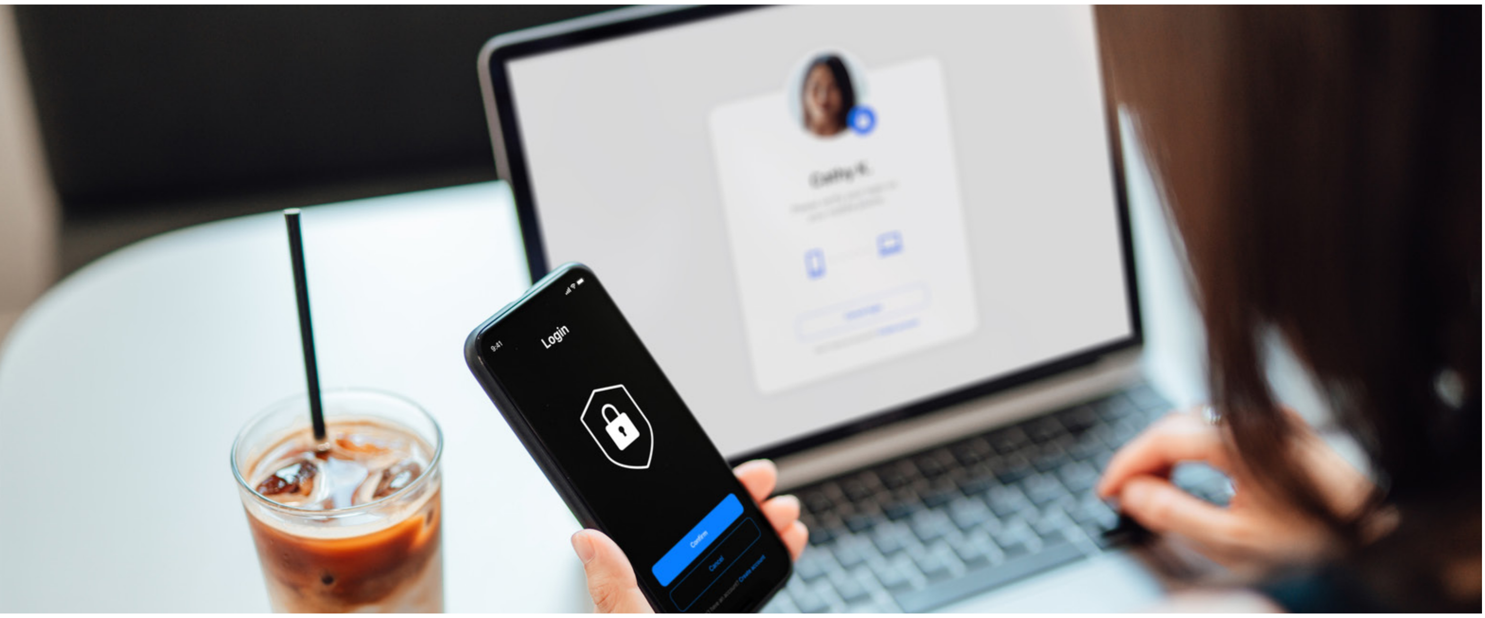
vi): Portal customization

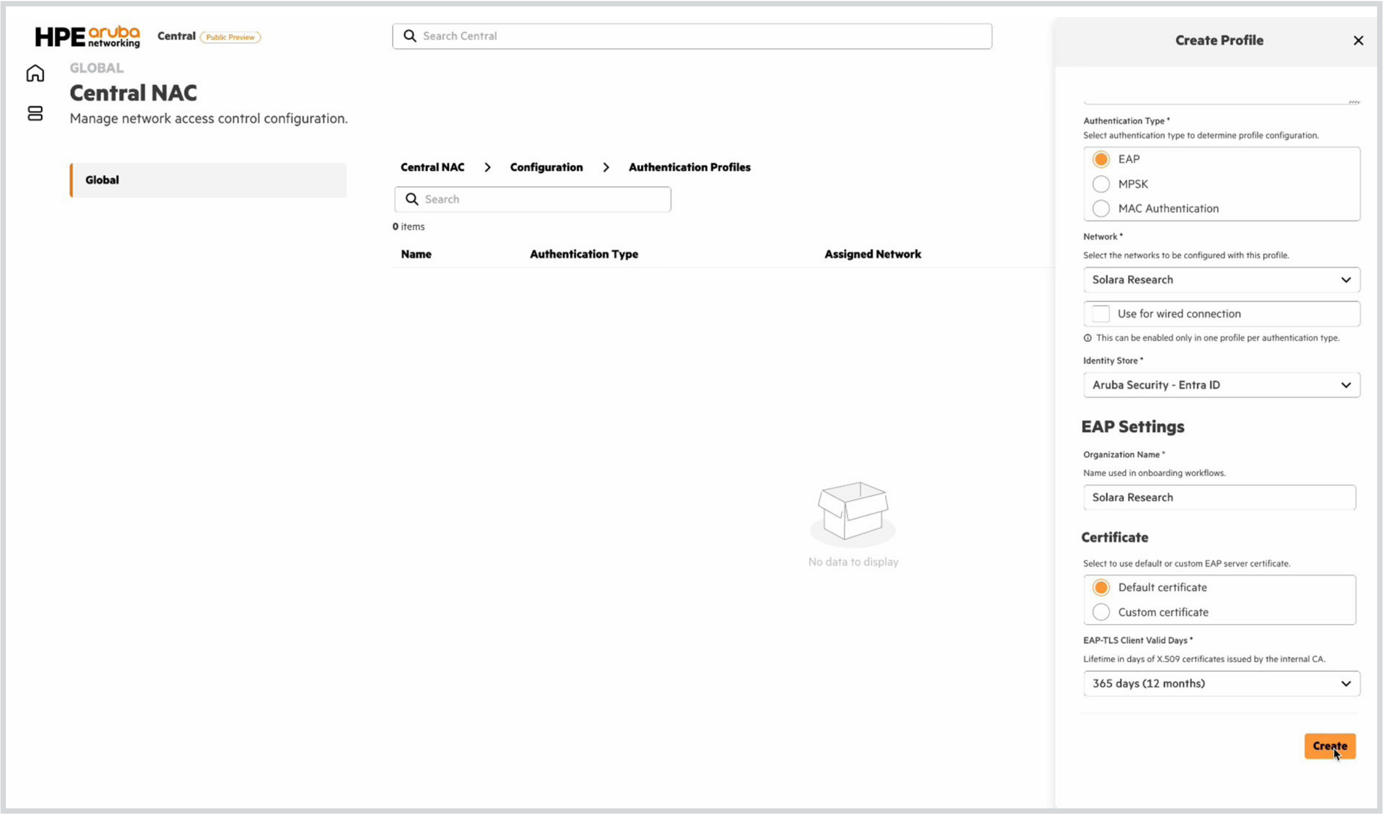
Learn how HPE Aruba Networking Central NAC works: Watch the zero trust with cloud-native network access control video

Note: WLAN needs to be created before configuring authentication profiles

i): Authentication profiles: Authentication profiles tie together the network, identity source, and authentication method. HPE Aruba Networking Central NAC enforces strong authentication, helping ensure that only authorized users or devices can access the network. This typically involves certificates or unique pre-shared keys to verify the identity of users and devices. The solution supports advanced authentication methods, such as EAP-TLS, MAC Auth, MPSK (admin and user managed), and captive portal. Within EAP-TLS, HPE Aruba Networking Central NAC (pro) supports custom certificate or BYOC authentication, allowing the IT teams to configure their own certificate for authentication.

Each tenant has access to a dedicated certificate authority (CA), but some customers may prefer to use their own certificates for user identity in NAC. With HPE Aruba Networking Central NAC (pro), administrators can choose which certificates to apply on each network—using certificates from Hewlett Packard Enterprise on one network and their own on another, or exclusively using their own across all networks. Unlike many other solutions, HPE offers the flexibility to validate certificates in real time using OCSP, reducing the need for manual updates or relying solely on expiration dates to confirm validity.





GLOBAL

Central NAC

Manage network access control configuration.

0 items

Name	Authentication Type	Assigned Network

No data to display

Create Profile ✕

Authentication Type *

Select authentication type to determine profile configuration.

● EAP
○ MPSK
○ MAC Authentication

Network *

Select the networks to be configured with this profile.

Solara Research

□ Use for wired connection

ⓘ This can be enabled only in one profile per authentication type.

Identity Store *

Aruba Security - Entra ID

EAP Settings

Organization Name *

Name used in onboarding workflows.

Solara Research

Certificate

Select to use default or custom EAP server certificate.

● Default certificate
○ Custom certificate

EAP-TLS Client Valid Days *

Lifetime in days of X.509 certificates issued by the internal CA.

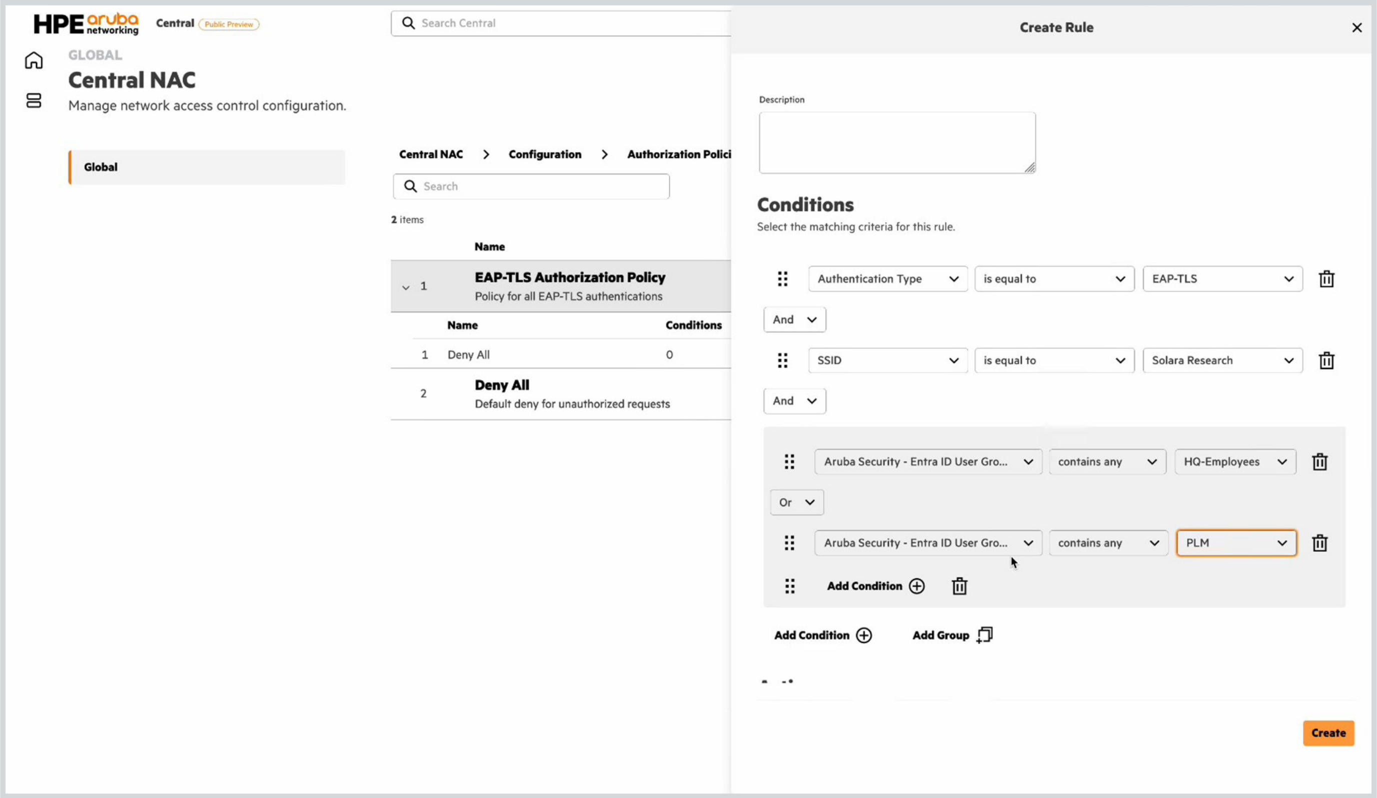
365 days (12 months)

Figure 2. HPE Aruba Networking Central NAC authentication profiles fields

ii): Authorization policies: Once authentication is successful, HPE Aruba Networking Central NAC uses granular authorization policies to determine the level of access granted. These policies are based on various factors, such as the user's group membership in identity store, location, authentication method, device category, compliance, and other context around the device. Please refer to Table 1 and Table 2 for complete list of parameters supported by Central NAC (core) and Central NAC (pro).

Authorization policies have preconditions that determine which policy would be used. When a policy is first created, it would only have the **deny all** rule within it—in line with zero trust principle. Additional rules would have to be configured that specify the role/vlan/session timeout to be returned after a successful authentication.

HPE Aruba Networking Central NAC triggers a reauthentication whenever there is a change in the context of the user or device, prompting a re-evaluation of the access policies. This approach helps ensure that zero trust is enforced dynamically by continuously verifying the user and device context. User context is available in the form of IdP group membership, and device context in the form of client tags and category from HPE Aruba Networking Central Client Insights.


HPE aruba networking Central Public Preview
Search Central
GLOBAL
Central NAC
Manage network access control configuration.
Global
Central NAC > Configuration > Authorization Polici
Search
2 items
Create Rule
Description
Add Condition
Add Group
Create

	Name
1	**EAP-TLS Authorization Policy** Policy for all EAP-TLS authentications
2	**Deny All** Default deny for unauthorized requests

	Name	Conditions
1	Deny All	0

Conditions

Select the matching criteria for this rule.

Authentication Type | is equal to | EAP-TLS

And

SSID | is equal to | Solara Research

And

Aruba Security - Entra ID User Gro... | contains any | HQ-Employees

Or

Aruba Security - Entra ID User Gro... | contains any | PLM

Figure 3. HPE Aruba Networking Central NAC authorization policies fields

iii): Identity management: Identity management integration is a core capability in HPE Aruba Networking Central NAC. By connecting with leading IdPs, the solution seamlessly authenticates users and devices regardless of their location.

HPE Aruba Networking Central NAC supports the following cloud-based identity providers for user identity:

— Microsoft Entra ID

— Google Workspace

— Okta Workforce Identity Cloud

The identity stores in HPE Aruba Networking Central NAC are used for: Authentication and authorization, onboarding devices and generating user based MPSK.

Identity stores can be created in just a few steps by configuring the following parameters:

— Name—Enter a name of the identity store

— Description—Enter description

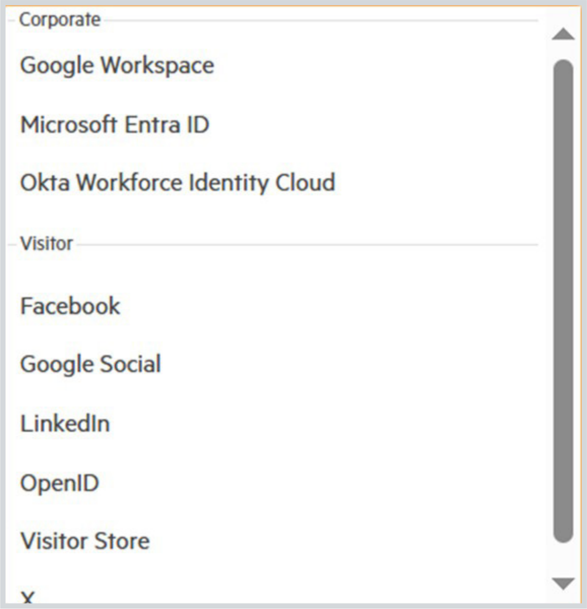
— Provider—Select a corporate identity service provider from the following options, or choose a visitor identity provider

- Microsoft Entra ID
- Okta Workforce Identity Cloud
- Google Workspace

If you select any other visitor identity store like Facebook, Google, LinkedIn, etc., enter details for the following required fields:

— Client ID—Enter your Application (client) ID

— Client Secret—Enter your secret value



Corporate

Google Workspace

Microsoft Entra ID

Okta Workforce Identity Cloud

Visitor

Facebook

Google Social

LinkedIn

OpenID

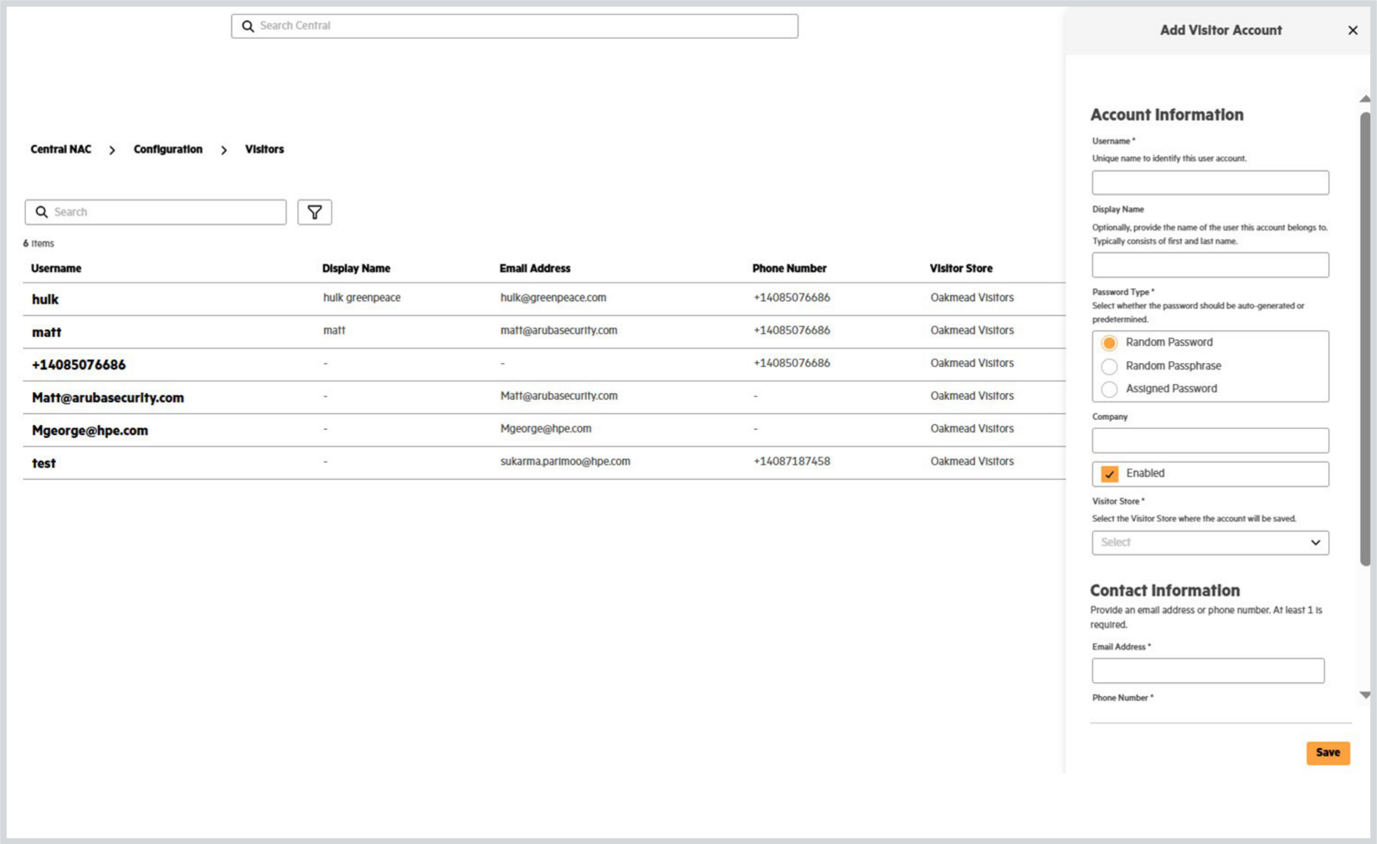
Visitor Store

X

Figure 4. HPE Aruba Networking Central NAC identity management fields

HPE Aruba Networking Central NAC uses REST APIs to fetch group membership from IdPs. It also uses webhook notifications from IdPs to track changes to user accounts, such as account being deleted, account being disabled, or change in group membership. When an account is either deleted or disabled, HPE Aruba Networking Central NAC revokes any client certificates issued to the user and deletes all the MPSK keys associated with the user. If the user has devices connected to the network, HPE Aruba Networking Central NAC disconnects the devices from the network as well.

iv): Visitor access: Visitor tile in HPE Aruba Networking Central NAC allows administrators to manage visitor access to the network and perform various actions on the visitor accounts. Administrators can choose from multiple visitor authentication methods, including pre-created user accounts, self-registration through email or SMS, and social media login options such as LinkedIn, Google™, X, or Facebook. For scenarios where authentication is not required, a click-to-accept option is also available.



Search Central

Central NAC > Configuration > Visitors

Search

6 items

Username	Display Name	Email Address	Phone Number	Visitor Store
hulk	hulk greenpeace	hulk@greenpeace.com	+14085076686	Oakmead Visitors
matt	matt	matt@arubasecurity.com	+14085076686	Oakmead Visitors
+14085076686	-	-	+14085076686	Oakmead Visitors
Matt@arubasecurity.com	-	Matt@arubasecurity.com	-	Oakmead Visitors
Mgeorge@hpe.com	-	Mgeorge@hpe.com	-	Oakmead Visitors
test	-	sukarma.parimoo@hpe.com	+14087187458	Oakmead Visitors

Add Visitor Account ×

Account Information

Username *

Unique name to identify this user account.

Display Name

Optionally, provide the name of the user this account belongs to. Typically consists of first and last name.

Password Type *

Select whether the password should be auto-generated or predetermined.

● Random Password

○ Random Passphrase

○ Assigned Password

Company

☑ Enabled

Visitor Store *

Select the Visitor Store where the account will be saved.

Select

Contact Information

Provide an email address or phone number. At least 1 is required.

Email Address *

Phone Number *

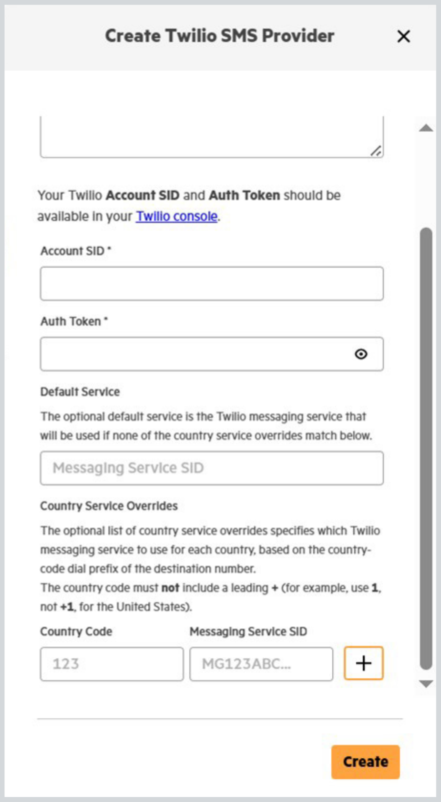
Figure 5. HPE Aruba Networking Central NAC visitor access fields

Admin can perform a range of actions on visitor accounts

- Modify the status of a visitor account to enabled or disabled.
- If a visitor account has expired, admins will not be able to perform any actions; they will be required to edit the visitor account and change the expiration date first.
- Modify the password for a visitor account.
- Delete a visitor account. Any active network sessions associated with the user will also be disconnected.

Admin can also generate visitor report based on a range of filters and download or send that report to a mail address from within the screen.

v): Messaging: Messaging tile in HPE Aruba Networking Central NAC allows administrators to configure a messaging provider and support guest SMS service (for registration).



Create Twilio SMS Provider ✕

Your Twilio **Account SID** and **Auth Token** should be available in your Twilio console.

Account SID *

Auth Token *

Default Service

The optional default service is the Twilio messaging service that will be used if none of the country service overrides match below.

Messaging Service SID

Country Service Overrides

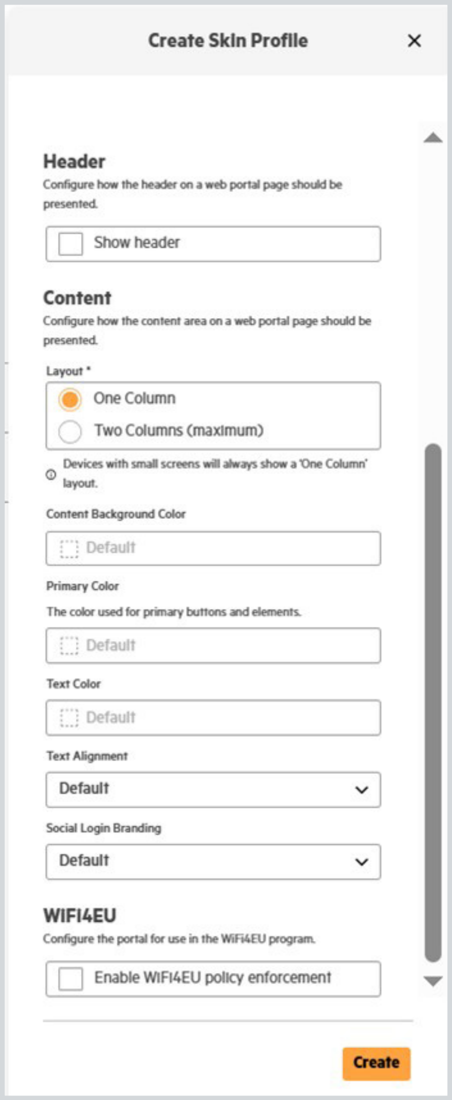
The optional list of country service overrides specifies which Twilio messaging service to use for each country, based on the country-code dial prefix of the destination number.
The country code must **not** include a leading **+** (for example, use **1**, not **+1**, for the United States).

Country Code	Messaging Service SID	
123	MG123ABC...	+

Create

Figure 6. HPE Aruba Networking Central NAC messaging fields

vi): Portal customization: Portal customization engine in HPE Aruba Networking Central NAC allows administrators to tailor the look, feel, and functionality of the captive portal (splash page) presented to guest users when they access a guest Wi-Fi network. This tile consists of sub-tiles: Portal profiles, Skin profiles, Override profiles, and Images. These enable administrators to customize the look and feel and offer the splash page in 19 different languages.



Create Skin Profile ✕

Header

Configure how the header on a web portal page should be presented.

□ Show header

Content

Configure how the content area on a web portal page should be presented.

Layout *

● One Column
○ Two Columns (maximum)

ⓘ Devices with small screens will always show a 'One Column' layout.

Content Background Color: Default

Primary Color

The color used for primary buttons and elements.

Default

Text Color: Default

Text Alignment: Default

Social Login Branding: Default

WIFI4EU

Configure the portal for use in the WiFi4EU program.

□ Enable WIFI4EU policy enforcement

Create

Figure 7. HPE Aruba Networking Central NAC portal customization fields

HPE Aruba Networking Central NAC use cases

Securing IoT devices

HPE Aruba Networking Central NAC leverages MAC authentication to securely connect IoT and headless devices on the network, making sure that these devices have minimal access (Just enough to carry out their dedicated task). HPE Aruba Networking Central NAC policies leverage device profile information and client tags from HPE Aruba Networking Central Client Insights module to create very granular rules that assign appropriate role or VLAN to the devices. For example, a security camera would be assigned a role that only allows the specific ports required for the camera to function and nothing more.

MAC authentication in HPE Aruba Networking Central NAC can be configured in the following two modes:

1. Allow all MAC addresses
2. Allow only the MAC addresses present in the MAC address identity store

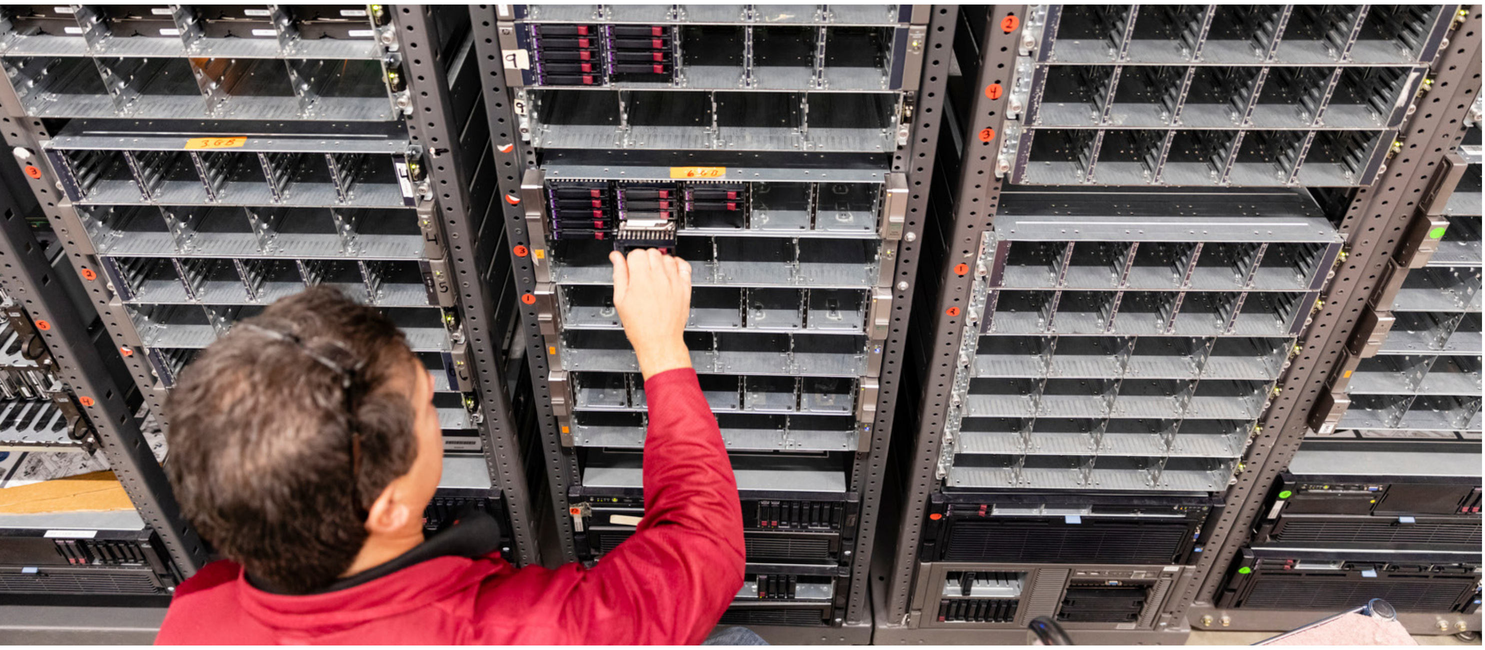
1. Allow all MAC addresses: This feature can be used to allow all devices to connect to the network initially so that HPE Aruba Networking Central NAC can learn MAC Addresses of the devices in the network. When a network is enabled with Allow All MAC Authentication, the MAC address of all the devices connecting to it is added to the MAC address identity store in HPE Aruba Networking Central NAC. Devices that do not match the configured rules can be given very restricted access or even be denied access to the network.

2. MAC address store-based authentication: This feature can be used to allow specific MAC addresses added to the MAC address identity store to connect to the network. Devices whose MAC addresses are not present in the store would be denied access.

All the incoming headless devices are also profiled by HPE Aruba Networking Central Client Insights, granting visibility into the type and behavior of devices in the network. These details are used to create rules for assigning different roles to different types of devices based on their category and behavior in the network.

Multi Pre-Shared Key for seamless connection

Multi Pre-Shared Key (MPSK) allows devices to connect securely using Wi-Fi credentials that are unique to a user or device or a group of devices. With each user or device having a unique MPSK, security is enhanced by limiting exposure if the PSK is compromised. Devices sharing similar functions can be grouped together and can share a single MPSK, thus simplifying management. MPSK improves the security profile of WPA2-PSK without compromising on the ease of use. Therefore, offering a secure and easy way to connect devices where a full 802.1X deployment is not feasible.



Some common use cases with MPSK are:

- IoT and other headless devices that are not capable of doing 802.1X authentication can connect with a unique MPSK per device.
- Guest Wi-Fi for event networks that are short lived. QR codes can be printed and posted at the event venue for attendees to connect easily to the network.
- Easy way for students in dorm rooms to connect all their personal devices using an MPSK that is unique per student.
- Simple and straight forward way for seniors to connect their devices in multi-dwelling units.
- Alternative to captive portal workflows for guest users with MPSKs being rotated periodically.
- It provides an easy connectivity option at small sites where deploying 802.1X is not feasible.

HPE Aruba Networking Central NAC supports two modes for MPSK:

1. User-managed MPSK
2. Admin-managed MPSK

1. User-managed MPSK

This feature allows users to generate and manage their own unique MPSK through a self-service portal. Per-user Wi-Fi credentials reduce the risk associated with single shared passwords. It also allows devices to be identified on the network by the user who owns them.

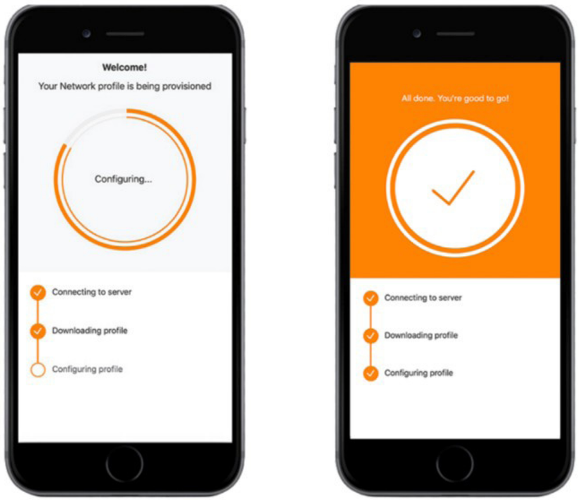
2. Admin-managed MPSK

Here, the admin generates MPSK that can be used with devices that are owned and managed by the organization. In these cases, there is no single user associated with the device. Here, the network admin can create an MPSK that can be used with a single device or a group of devices.

Secure client onboarding

Client devices can be configured using HPE Aruba Networking Onboard, a client app that installs an Enterprise Passpoint profile on the client device. The HPE Aruba Networking Onboard app installs EAP-TLS certificates on user devices. With BYOC, these certificates can be issued from organization's own PKI infrastructure instead of using HPE default CA. With this profile, anytime the user walks into range of the network, the client device will automatically connect with the appropriate network access rules as configured by the admin through HPE Aruba Networking Central.

HPE Aruba Networking Onboard provides automatic renewals, requiring no additional onboarding steps and upkeep from the end user while allowing the admin to change and update policies at any time. It is supported on macOS, Windows, iOS, Android™, Ubuntu, and ChromeOS operation systems.



Welcome!

Your Network profile is being provisioned

Configuring...

Connecting to server

Downloading profile

Configuring profile

All done. You're good to go!

Connecting to server

Downloading profile

Configuring profile

Figure 8. HPE Aruba Networking Onboard installing Enterprise Passpoint profile

Network security in a multivendor environment

The new HPE Aruba Networking Central NAC is designed to unify and simplify NAC across diverse infrastructures by extending robust security policy support for third-party network access devices (NADs). This capability helps ensure that a consistent security policy is enforced across campus, branch, and data center environments—regardless of the underlying network vendor.

By helping ensure a consistent policy enforcement across a multivendor network environment, HPE Aruba Networking Central NAC terminates the need to replicate security policies to suit different infrastructures. By providing role, ACL, or VLAN, HPE Aruba Networking Central NAC talks to underlying infrastructure and translates the authentication and authorization protocols configured by security team into device-compatible format.

This approach not only streamlines security management but also significantly reduces operational overhead and costs. Organizations can maintain a heterogeneous network environment without compromising on visibility, control, or compliance—making HPE Aruba Networking Central NAC a future-ready solution for scalable, vendor-agnostic access control.

In a multivendor environment, third-party NADs initiate RADIUS requests that are first received by HPE Aruba Networking OS-10 Gateways, which function as RADIUS proxies. These gateways securely forward the authentication and authorization requests to HPE Aruba Networking Central NAC using RadSec, a protocol that helps ensure encrypted and reliable communication. Upon receiving the requests, HPE Aruba Networking Central NAC evaluates them and returns policy decisions (VLAN values) that are specifically tailored to the capabilities and configurations of the originating NAD, enabling precise and context-aware access control across diverse network environments. By automatically identifying the type of NAD in use, HPE Aruba Networking Central NAC helps ensure that when dynamic authorization is needed—such as a Change of Authorization (CoA) or Disconnect messages—the correct message is sent to the appropriate NAD. This targeted response strengthens the overall zero trust network architecture by enforcing precise and secure access control.

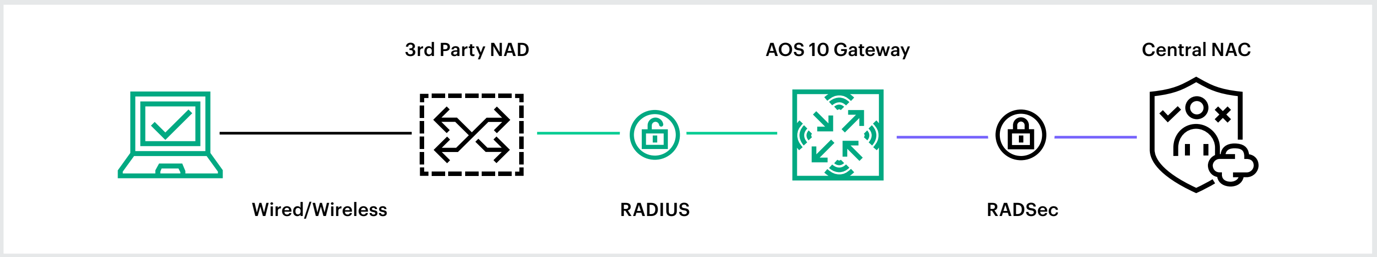


Figure 9. HPE Aruba Networking Central NAC third-party NAD support flow

HPE Aruba Networking Central NAC licensing

As discussed earlier, HPE Aruba Networking Central NAC comes with Central at no additional cost—for implementing core NAC functionalities. Customers seeking to implement advanced NAC functionalities need to buy additional NAC subscription. Table 1 below breaks down the NAC core feature set

Table 1. Feature List in HPE Aruba Networking Central NAC (core)

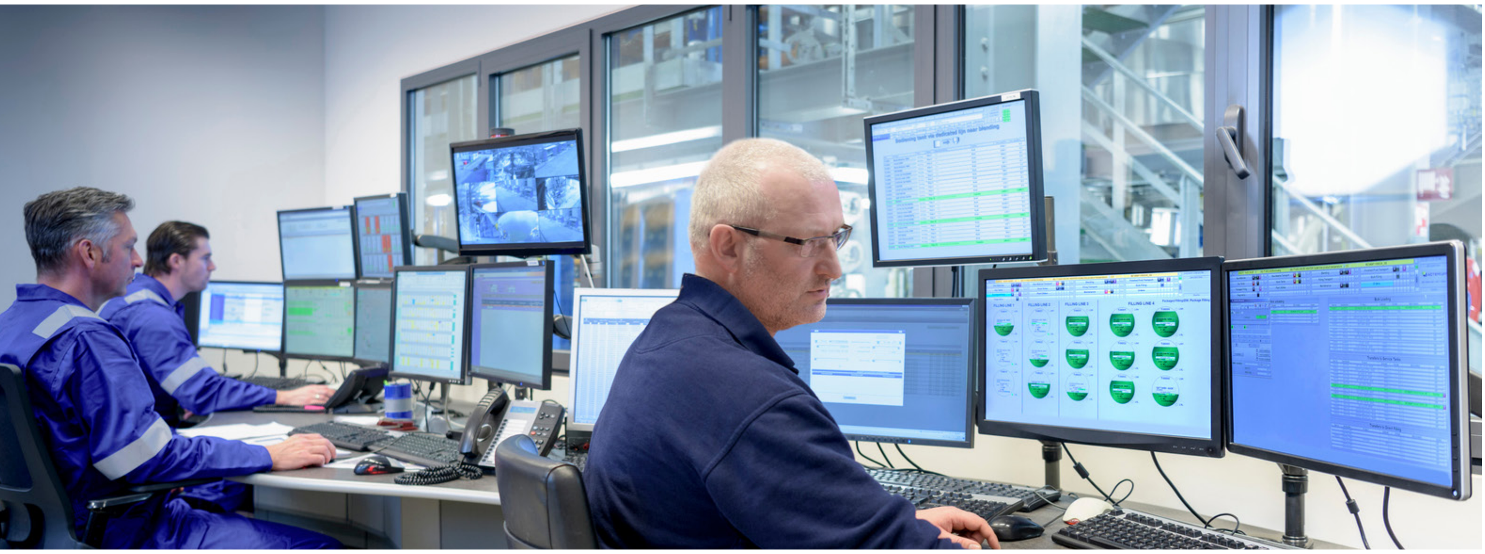
Feature list	Highlight
Identity source	Create only one corporate identity provider for enterprise use (Okta, Entra ID, or Google Workspace)
Authentication profiles	**EAP** — Select only one corporate identity provider **MPSK** — Select only one corporate identity provider — 5000 MPSK supported **MAB** — Similar to premium license
Authorization policies	— Create policies through predefined templates with prepopulated preconditions that cannot be edited • User policy • Client policy — Use only a subset of attributes while creating rules and enforcement profiles within a policy • Rule attributes can contain only client tags, client category, and user groups • Enforcement profile can contain only HPE Aruba Networking user role, **Allow** and **Deny** actions, and **Session Timeout**

NAC subscription license

The NAC subscription license unlocks the pro NAC features along with all the core NAC feature set as mentioned in Table 1

Table 2. Feature list in HPE Aruba Networking Central NAC (pro)

Feature list	Highlight
Identity source	Create multiple corporate IdPs for enterprise use (Okta, Entra ID, or Google Workspace) of the same or different IdP types
Authentication profiles	**EAP** — Supports BYOC — Select multiple identity providers — Supports unlimited MPSK
Authorization policies	— Ability to create customized authorization policies using the full list of conditions — Select multiple identity providers — Use all attributes in the document while creating rules and enforcement profiles within a policy



Benefit of HPE Aruba Networking Central NAC

HPE Aruba Networking Central NAC offers significant business benefits, starting with cost savings as it terminates the need to purchase and maintain hardware, thereby reducing capital and operational expenses. The solution leverages cloud scalability and high uptime redundancy to provide uninterrupted security services. Developed by the HPE Aruba Networking ClearPass team, HPE Aruba Networking Central NAC inherits a legacy of reliability and trust by customers worldwide. It delivers a comprehensive solution for end-to-end enforcement through HPE Aruba Networking Central, which includes HPE Aruba Networking Central Client Insights and HPE Aruba Networking Central Policy Manager, allowing businesses to unify policies across campus, branch, and data center environments.

HPE Aruba Networking Central NAC is available without any additional cost to Central customers for implementing core NAC functionalities, and a straight-forward NAC subscription license for implementing advanced or pro NAC functionalities. This combination of cost efficiency, scalability, trust, comprehensive enforcement, and ease of use makes HPE Aruba Networking Central NAC an invaluable asset for modern enterprises.

HPE Aruba Networking Central NAC—Built-in and not bolted-on security

HPE Aruba Networking Central NAC is a critical component of HPE Aruba Networking zero trust strategy. Weaved into HPE Aruba Networking Central, the solution works with other HPE Aruba Networking Central features and offers a robust and scalable network security, reducing the need for any additional network security product and any patchwork required to integrate that into the environment.

HPE Aruba Networking Central NAC collaborates seamlessly with **HPE Aruba Networking Central Client Insights** and **HPE Aruba Networking Policy Manager** to deliver a robust zero trust security. HPE Aruba Networking Central Client Insights functions as an AI-powered profiling engine that meticulously analyzes device behavior and assigns tags based on the observed patterns. These tags are then leveraged by HPE Aruba Networking Central NAC to assign appropriate roles to the devices. This role assignment is crucial as it determines the level of access and permissions granted to each device within the network. By utilizing these roles, HPE Aruba Networking Central Policy Manager orchestrates security policies in alignment with HPE Aruba Networking infrastructure, helping ensure a strong end-to-end zero trust enforcement.

This comprehensive approach extends beyond just a single location. The roles and policies defined by HPE Aruba Networking Central NAC can be applied across campus, branch, and data centers, making the role and policies a centralized network security control for the entire enterprise. This centralized control helps ensure consistent security measures are in place, regardless of where the devices are located, thereby enhancing the overall security posture of the organization. By integrating AI-driven insights with robust policy enforcement, this system provides a dynamic and adaptive security framework that is essential for modern enterprises.

Learn more at

HPE.com/us/en/Aruba-Central.html

Visit HPE.com

Chat now

a50013820ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com