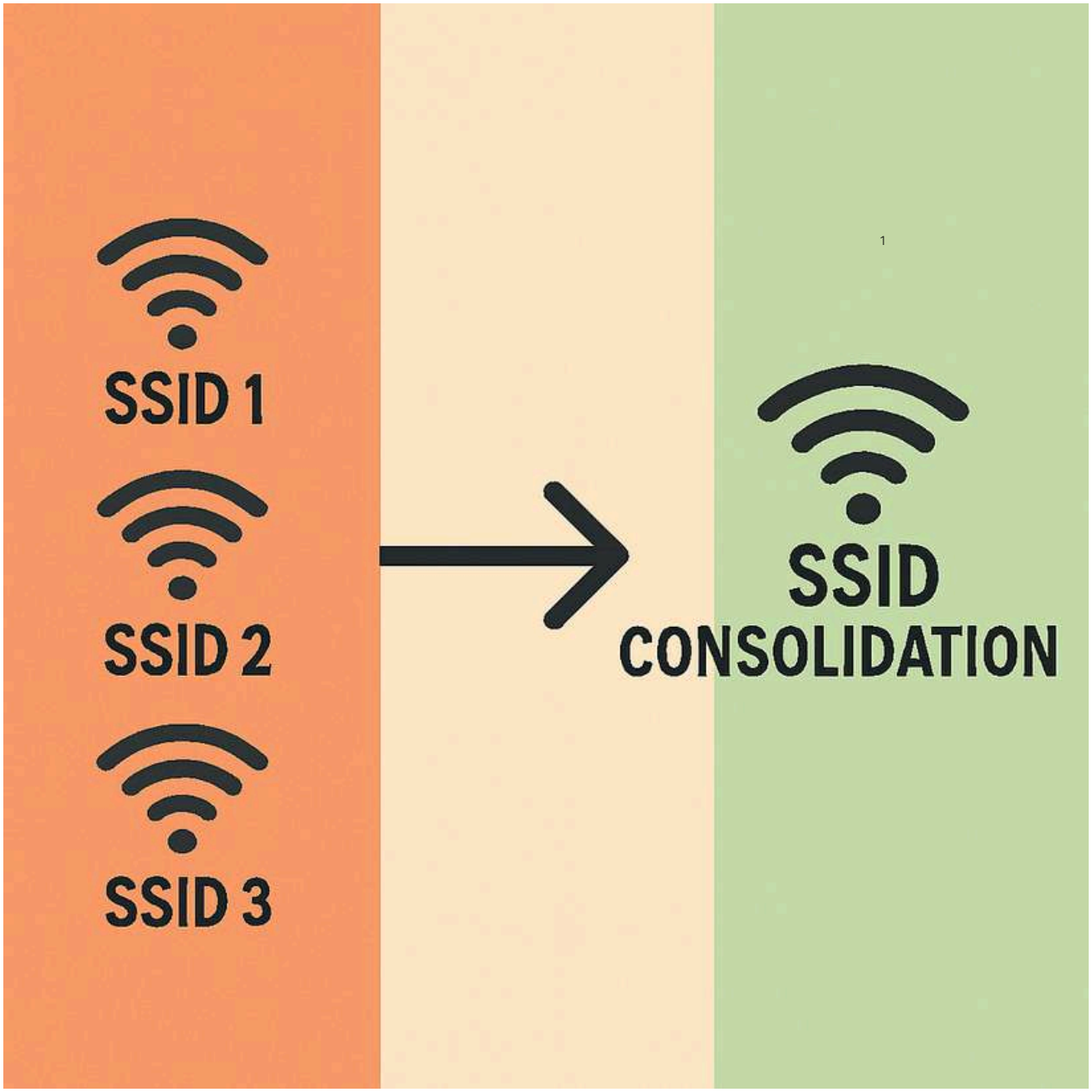
SSID Sprawl to Simplicity: Leveraging NAC for Secure and Scalable Network Access



by Jibran Aziz

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

With Apple introducing Wi-Fi (802.11b) on their iBook devices in 1999, mass adoption of Wi-Fi began. Next few years saw more and more Wi-Fi capable devices rolling out in the market and new Wi-Fi standards ratified. Fast forward ten years, i.e. 2009, Wi-Fi had become the primary medium of network connectivity for corporate and personal devices and was able to support much higher data rates (up to 600 Mbps with 802.11n as compared to up to 11 Mbps with 802.11b). As Wi-Fi took over wired connectivity as a primary medium for LAN connectivity, the number of devices and bandwidth hunger to cater different applications' requirements also kept on increasing, resulting in higher spectrum utilization for the 2.4 and 5Ghz frequency bands (expect to see similar trend on 6Ghz as more Wi-Fi 6E and Wi-Fi 7 capable devices being rolled out). Because Wi-Fi operates in unlicensed spectrum, it is accessible to all users, which makes it essential to carefully design and plan deployments to keep the spectrum as free from interference as possible.

Typical Corporate Environment

Corporate environments are complex and typically have multiple use cases for the WLAN networks to cater different business requirements. A typical corporate office will expect their wireless network to cover following use-cases:

- Provide secure connectivity for the corporate employees
- Allows contractors to connect to the wireless network and have internet and restricted corporate network access
- Allows guest users to connect to the wireless network
- Provides an option for users to bring their own devices (BYOD) and connect them to the network
- Pre-shared key secured SSID to connect things like printers and VoIP phones
- Allows headless and IoT devices to connect to the network
- Few other use cases that will vary from organization to organization

This essentially means a poorly designed Wi-Fi network would have a separate SSID that would be covering each of the use cases. Looking at the example above, there would be 5-6 separate SSIDs configured, if the Wi-Fi network design is not properly thought for and designed.

Why Does It Matter

The efficient design for Service Set Identifiers (SSIDs) play a pivotal role in delivering optimal network performance, security and user experience. Every SSID being broadcasted by an access point generates periodic management frames (such as beacon frames) that consume airtime. These frames are necessary for announcing the presence of the SSID but do not carry useful data for the user. In environments with many SSIDs, especially in high-density deployments, these frames multiply across each AP and every channel, leading to increased contention, congestion, and lower throughput. For instance, broadcasting five SSIDs (as per the requirements above) instead of one can consume up to five times more overhead airtime per access point, resulting in a noticeable performance degradation across the wireless network. While using one SSID to cater all use cases may not be possible, the aim should be to keep the number of SSIDs as minimum as practical.

How a NAC can help in SSIDs Consolidation

Network Access Control (NAC) can play an important role in SSIDs consolidation by enabling dynamic and policy-based network access, reducing the need for multiple SSIDs for different user groups, devices and access levels. Be leveraging a NAC, enterprises can achieve:

- Centralized Authentication and Authorization
- Dynamic VLAN/User role assignment
- Ongoing Posture assessment and compliance of end points
- Reduced operations overhead

While most of the enterprise NACs available (Aruba ClearPass, Cisco ISE, FortiNAC, Forescout NAC, etc) can be used to demonstrate effectiveness of NAC to consolidate SSIDs, I am using Aruba ClearPass for this document. The diagram below shows the topology used for testing and documentation:

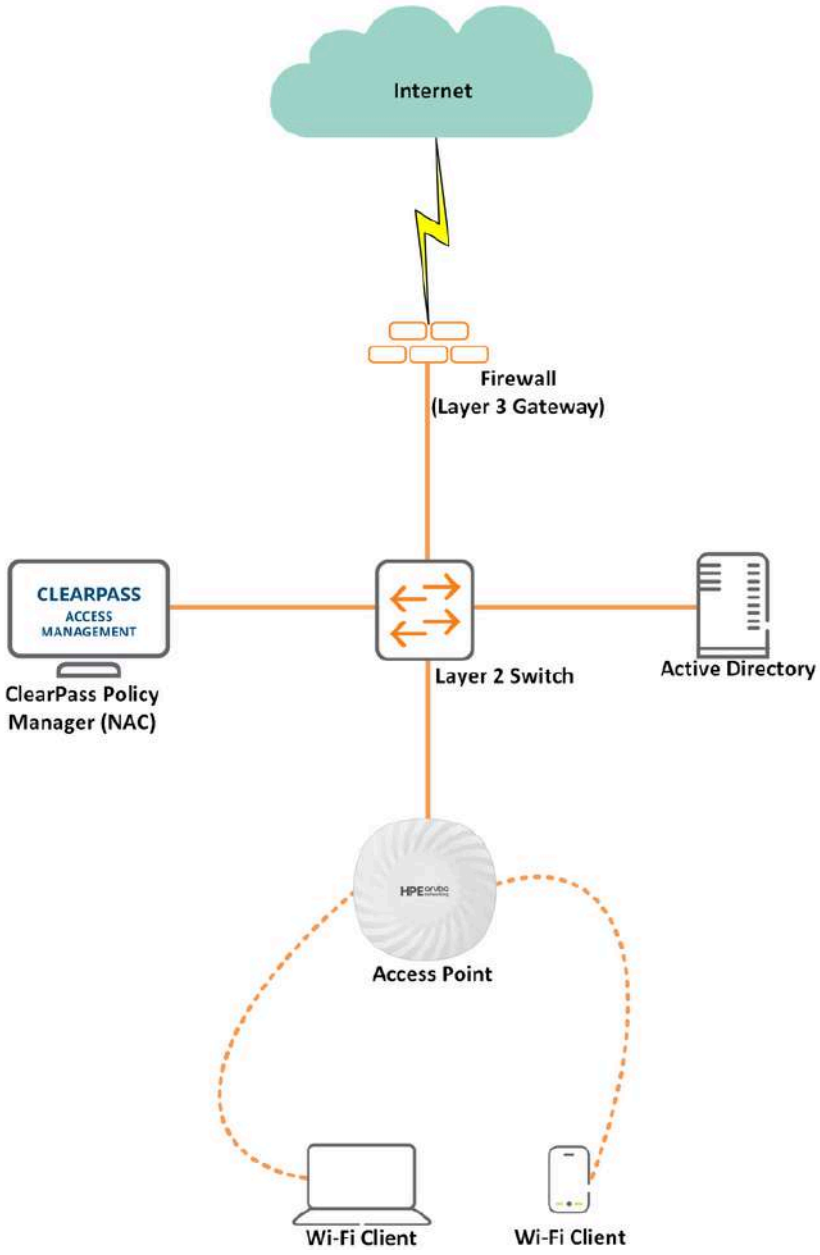


Figure 1- Lab Topology

Referring back to the typical enterprise use-cases, if a dedicated SSID is used to cater each of the use-cases, a total of 6 SSIDs will be required. As previously mentioned, that can have a huge impact of airtime utilization and network performance:

SSID	DESCRIPTION
SSID 1	Ensure secure network access for corporate employees
SSID 2	Enable contractors to connect to the wireless network with internet access and limited access to corporate resources
SSID 3	Support guest user connectivity to the wireless network.
SSID 4	Facilitate Bring Your Own Device (BYOD) capili-lities, allowing users to securely connect personal
SSID 5	Offer a pre-shared key (PSK) secured SSID for connecting non-user devices sucha printers.
SSID 6	Permit headless and IoT devices to access the network securely

Figure 2 - SSIDs Requirement for a Typical Enterprise

First step to consolidate the SSIDs is to plan how are we going to cover multiple use-cases with one SSID. Without a magic wand, we cannot cover all use-cases with a single SSID, but we can fulfil multiple use-cases with one SSID to ultimately reduce the number of SSIDs required to cater all use-cases.

SSID	DESCRIPTION
SSID 1	To connect corporate users, BYOD users and contractors
SSID 2	To allow guest users connect to the Wi-Fi network and allow BYOD users to onboard their devices
SSID 3	To connect non-user devices and IoT devices while keeping segregation between different device types

Figure 3 - Proposed SSIDs Consolidation

SSID Names

To make the SSIDs distinguishable, following SSID names have been used:

SSID	SSID Name	Access Requirements
SSID 1	CWNE-Dot1X	Corporate Resources and Internet
SSID 2	CWNE-Guest	Internet only
SSID 3	CWNE-MPSK	Selected Corporate Resources and Internet

Table 1 - SSID Names

SSID 1 - CWNE-Dot1X

CWNE-Dot1X SSID has been configured to connect following users to the Wi-Fi network:

- Corporate users – having corporate devices that have user certificates issued from the organization CA and have WLAN profile/settings pushed via GPO/Endpoint Manager
- BYOD users – brining their personal devices and connect to the network. The users connecting for the first time to the network do not have any certificate or WLAN profile configured and needs to "onboard" their personal devices before they can connect to the network
- Contractors – third party users and contractors that will have local credentials created in ClearPass and will use username/password instead of machine/user certificate for authentication

The SSID has been configured to perform 802.1X authentication before allowing network access. The three main components of 802.1X authentication are:

- Supplicant (Wi-Fi clients that are being authenticated, test laptop and mobile devices in this lab topology)
- Authenticator (acting as a gatekeeper between supplicant and authentication server, i.e. Access Point this this lab topology)

- Authentication Server (performs the actual authentication checks and decides whether user or a device should be allowed network access. It is ClearPass Policy Manager in this case)

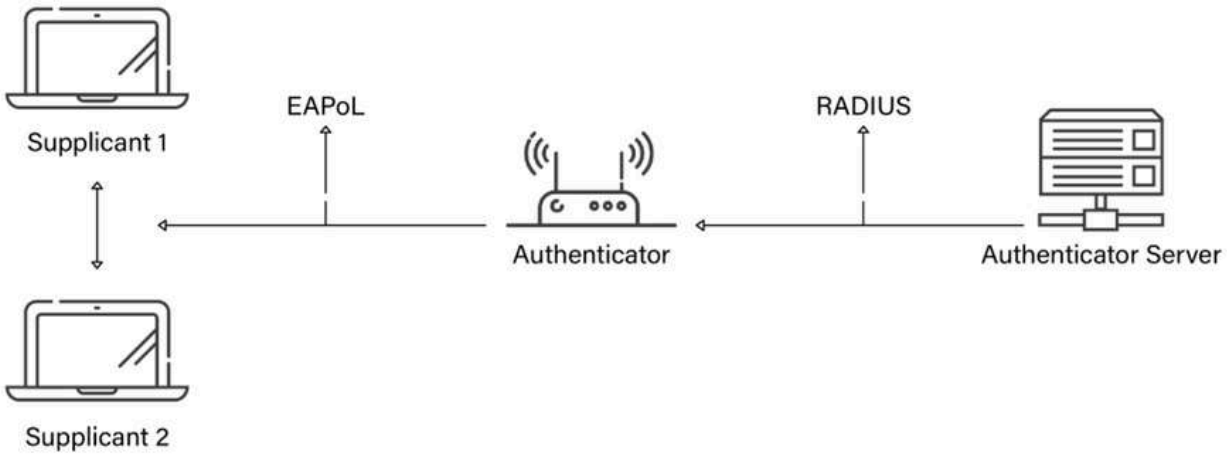
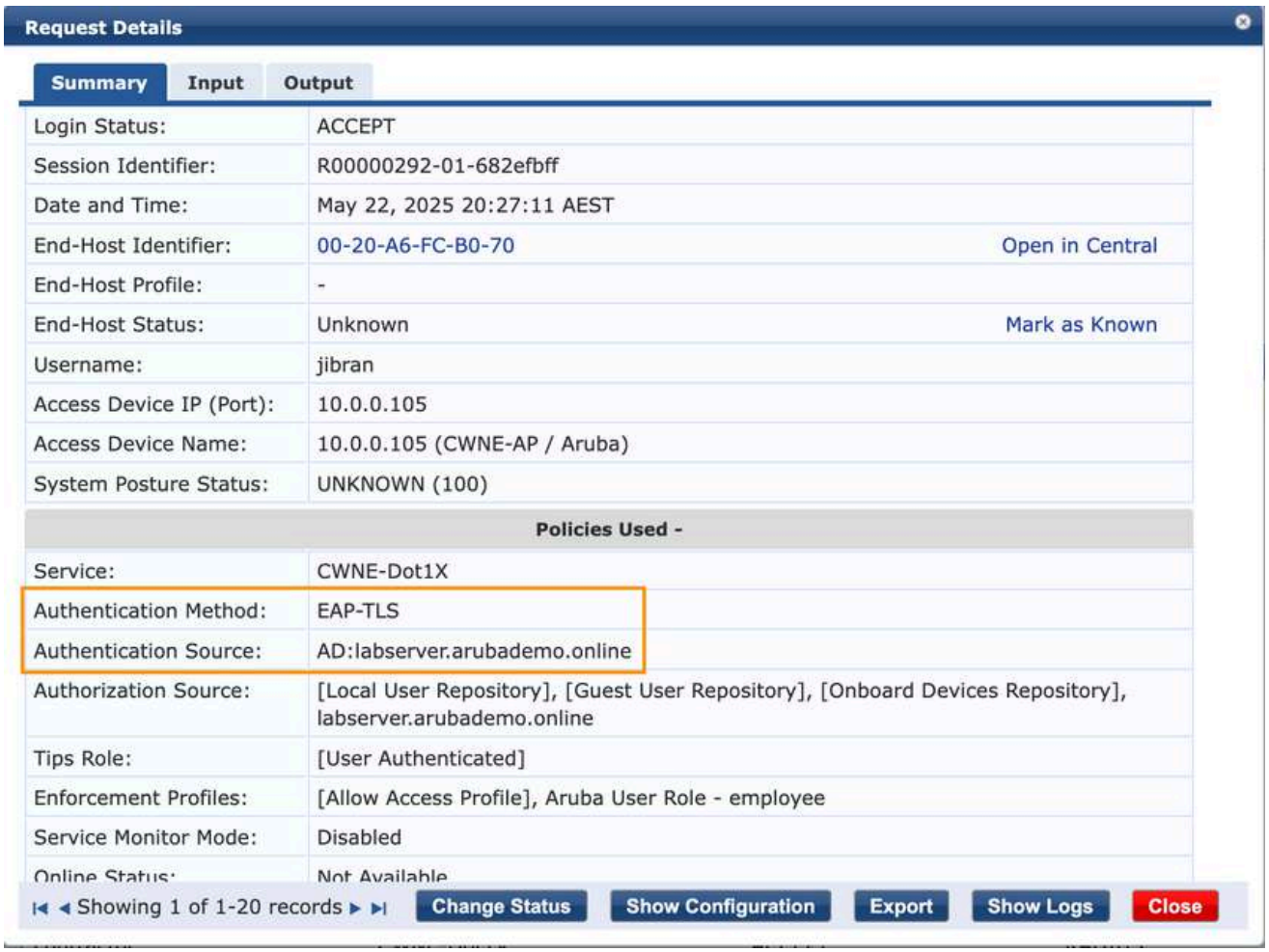


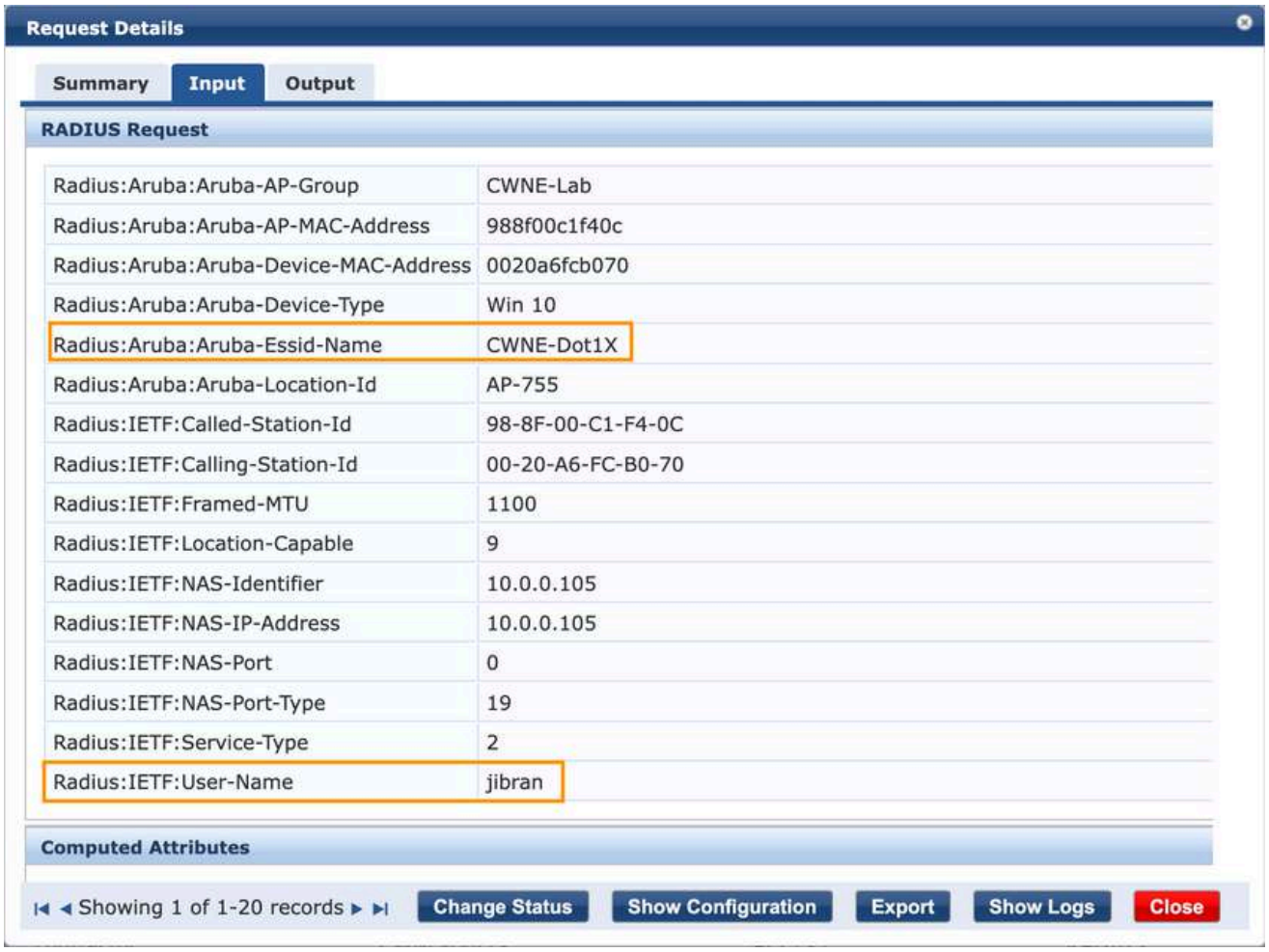
Figure 4 – 802.1X Authentication Roles

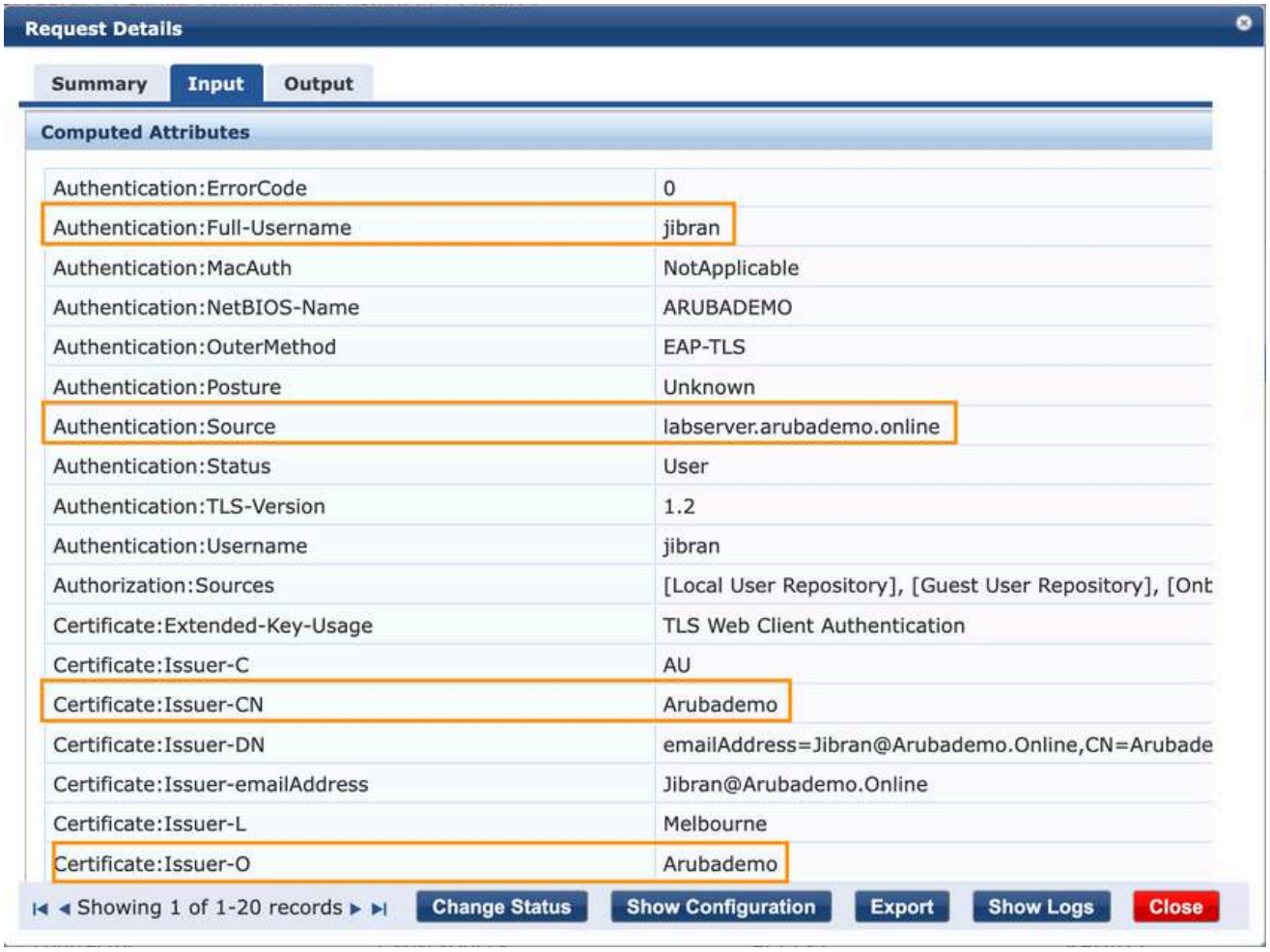
A service has been configured in ClearPass to distinguish between corporate and BYOD (both using EAP-TLS but corporate users will be the certificate issue from the corporate PKI while the BYOD users will have certificate issued from ClearPass Onboard Certificate authority) users based on the certificate parameters they will use to authenticate. Contractors, on the other hand will use username/password for authentication (EAP-PEAP) and will have different enforcement profile assigned as per follow snippet from the ClearPass service configuration:

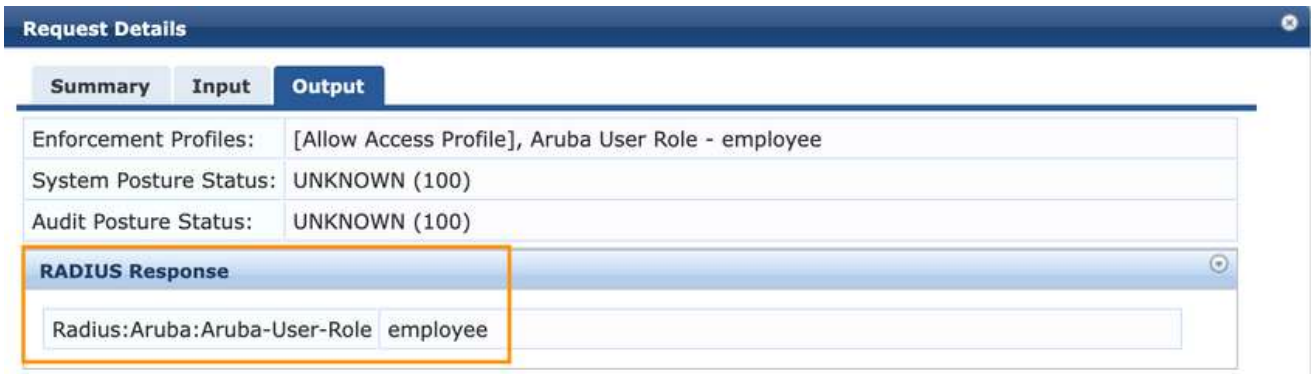
Employee connecting to CWNE-Dot1X SSID

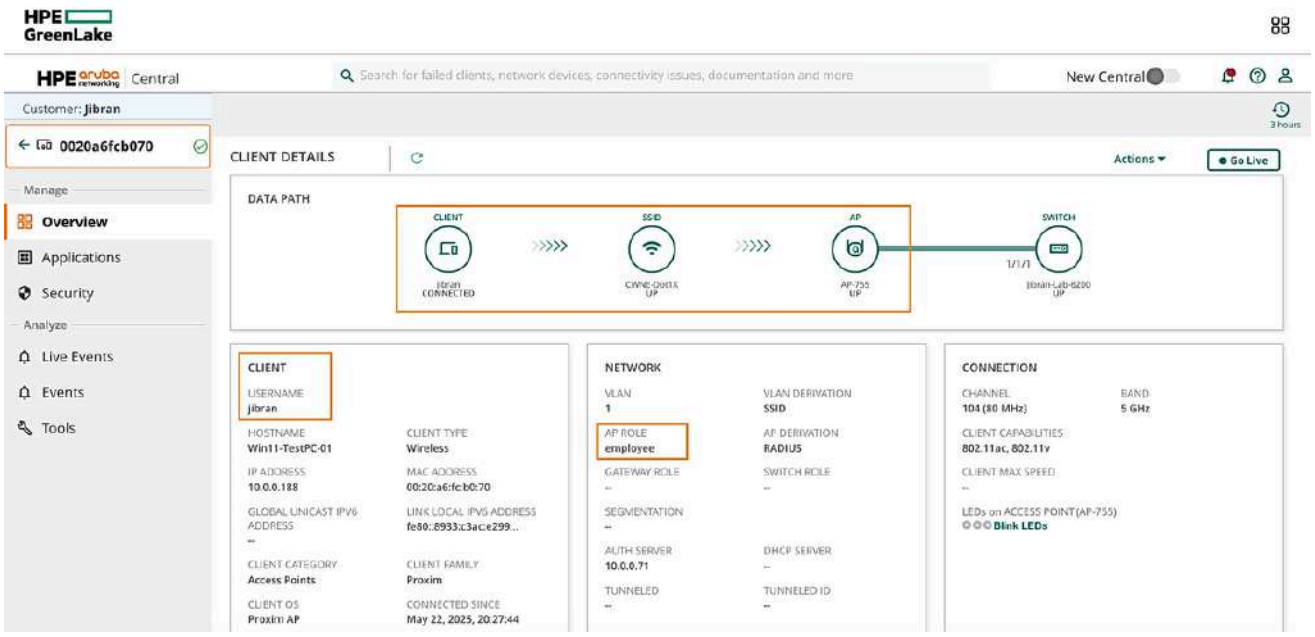
Following series of screenshots (from ClearPass and Aruba Central) captures details of a corporate client connecting to CWNE-Dot1X SSID and how ClearPass policy authenticates the user against on-prem AD and assigns the appropriate user role based on the parameters “computed” from user’s RADIUS request. In this example, user has been assigned user role “employee”:




Request Details
Summary
Input
Output
RADIUS Request
Radius:Aruba:Aruba-AP-Group
CWNE-Lab
Radius:Aruba:Aruba-AP-MAC-Address
988f00c1f40c
Radius:Aruba:Aruba-Device-MAC-Address
0020a6fcb070
Radius:Aruba:Aruba-Device-Type
Win 10
Radius:Aruba:Aruba-Essid-Name
CWNE-Dot1X
Radius:Aruba:Aruba-Location-Id
AP-755
Radius:IETF:Called-Station-Id
98-8F-00-C1-F4-0C
Radius:IETF:Calling-Station-Id
00-20-A6-FC-B0-70
Radius:IETF:Framed-MTU
1100
Radius:IETF:Location-Capable
9
Radius:IETF:NAS-Identifier
10.0.0.105
Radius:IETF:NAS-IP-Address
10.0.0.105
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Radius:IETF:Service-Type
2
Radius:IETF:User-Name
jibran
Computed Attributes
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

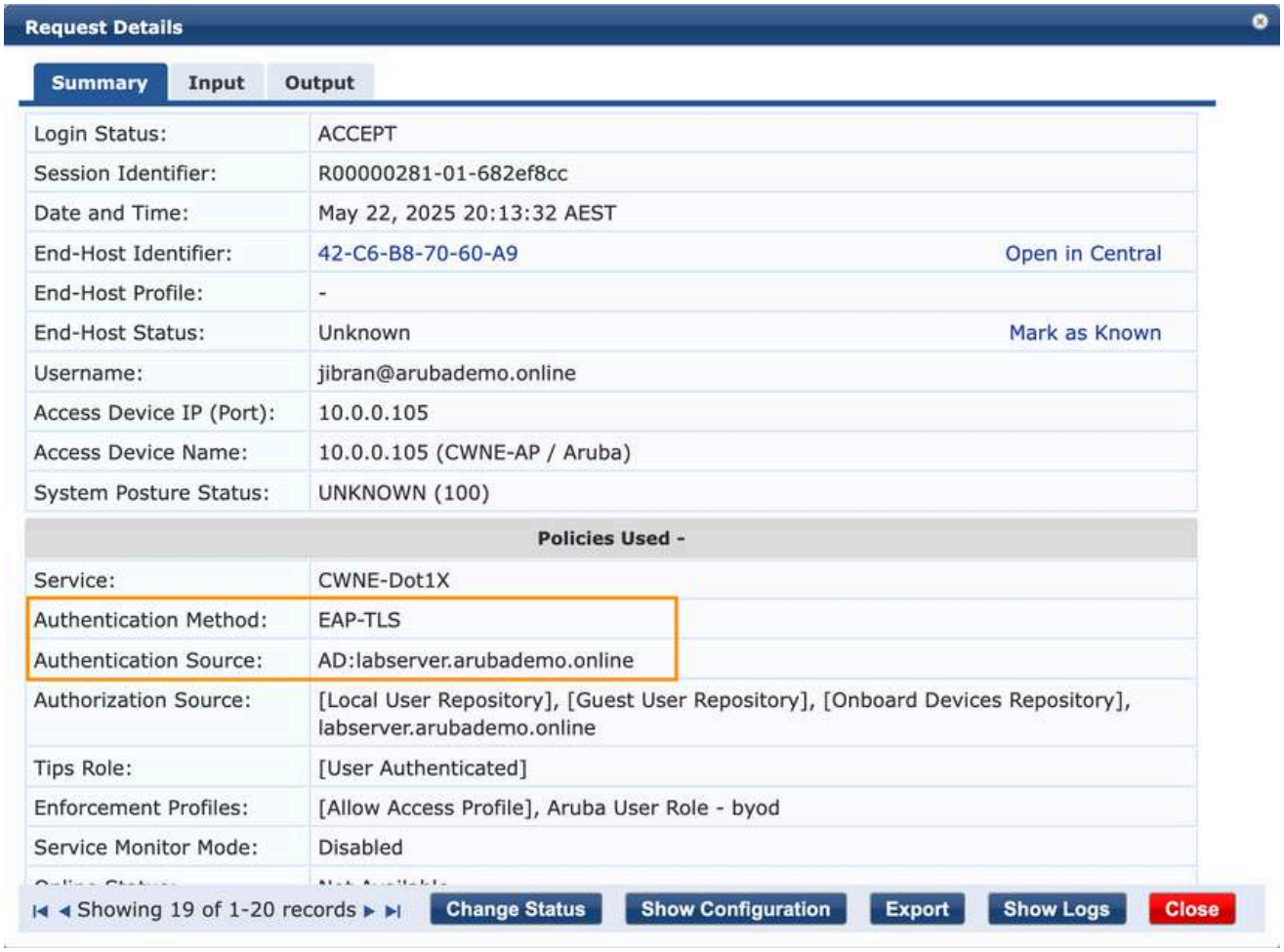

Request Details
Summary
Input
Output
Computed Attributes
Authentication:ErrorCode
0
Authentication:Full-Username
jibran
Authentication:MacAuth
NotApplicable
Authentication:NetBIOS-Name
ARUBADEMO
Authentication:OuterMethod
EAP-TLS
Authentication:Posture
Unknown
Authentication:Source
labserver.arubademo.online
Authentication:Status
User
Authentication:TLS-Version
1.2
Authentication:Username
jibran
Authorization:Sources
[Local User Repository], [Guest User Repository], [Ont
Certificate:Extended-Key-Usage
TLS Web Client Authentication
Certificate:Issuer-C
AU
Certificate:Issuer-CN
Arubademo
Certificate:Issuer-DN
emailAddress=Jibran@Arubademo.Online,CN=Arubade
Certificate:Issuer-emailAddress
Jibran@Arubademo.Online
Certificate:Issuer-L
Melbourne
Certificate:Issuer-O
Arubademo
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

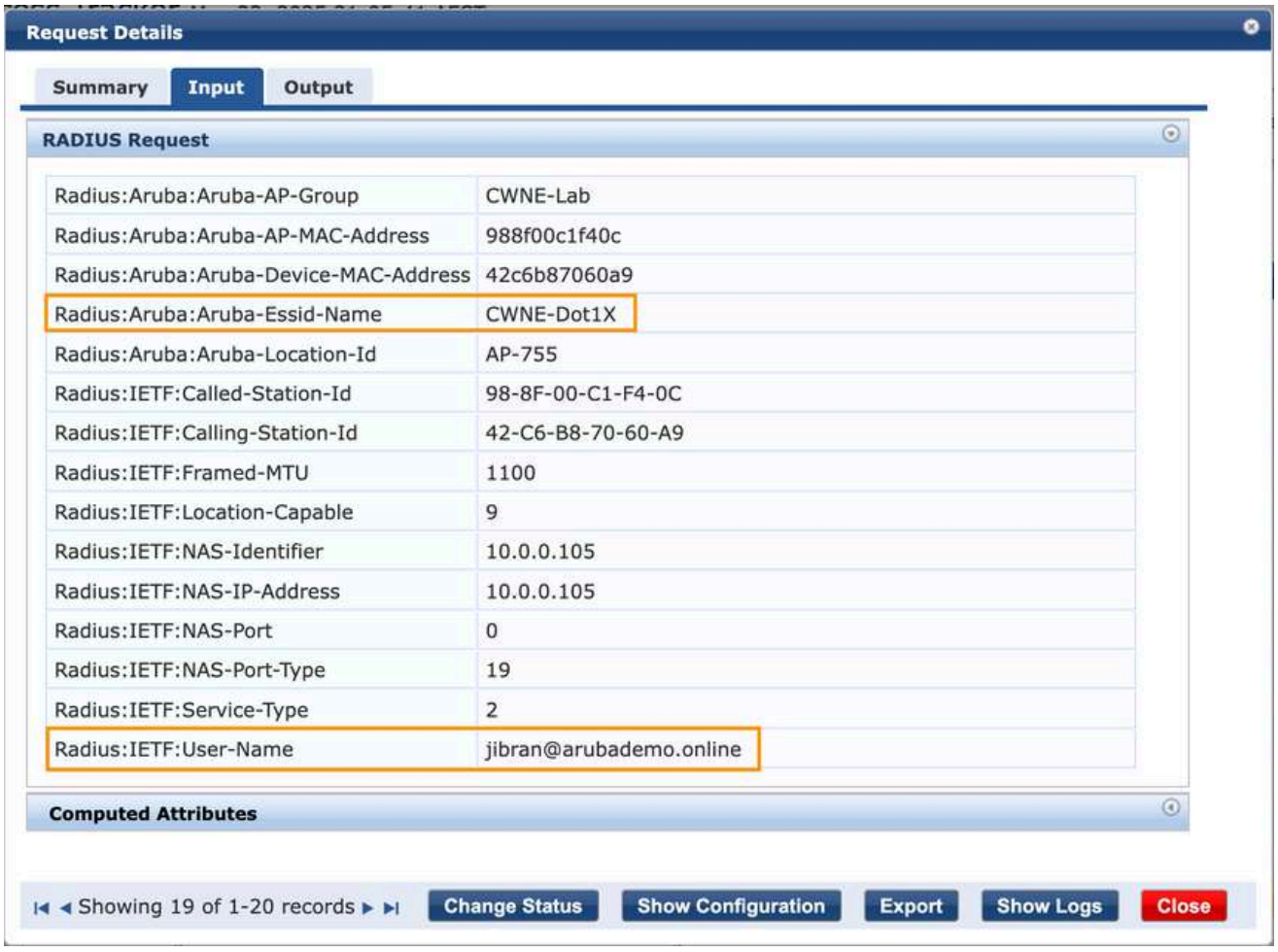

Request Details
Summary
Input
Output
Enforcement Profiles:
[Allow Access Profile], Aruba User Role - employee
System Posture Status:
UNKNOWN (100)
Audit Posture Status:
UNKNOWN (100)
RADIUS Response
Radius:Aruba:Aruba-User-Role
employee

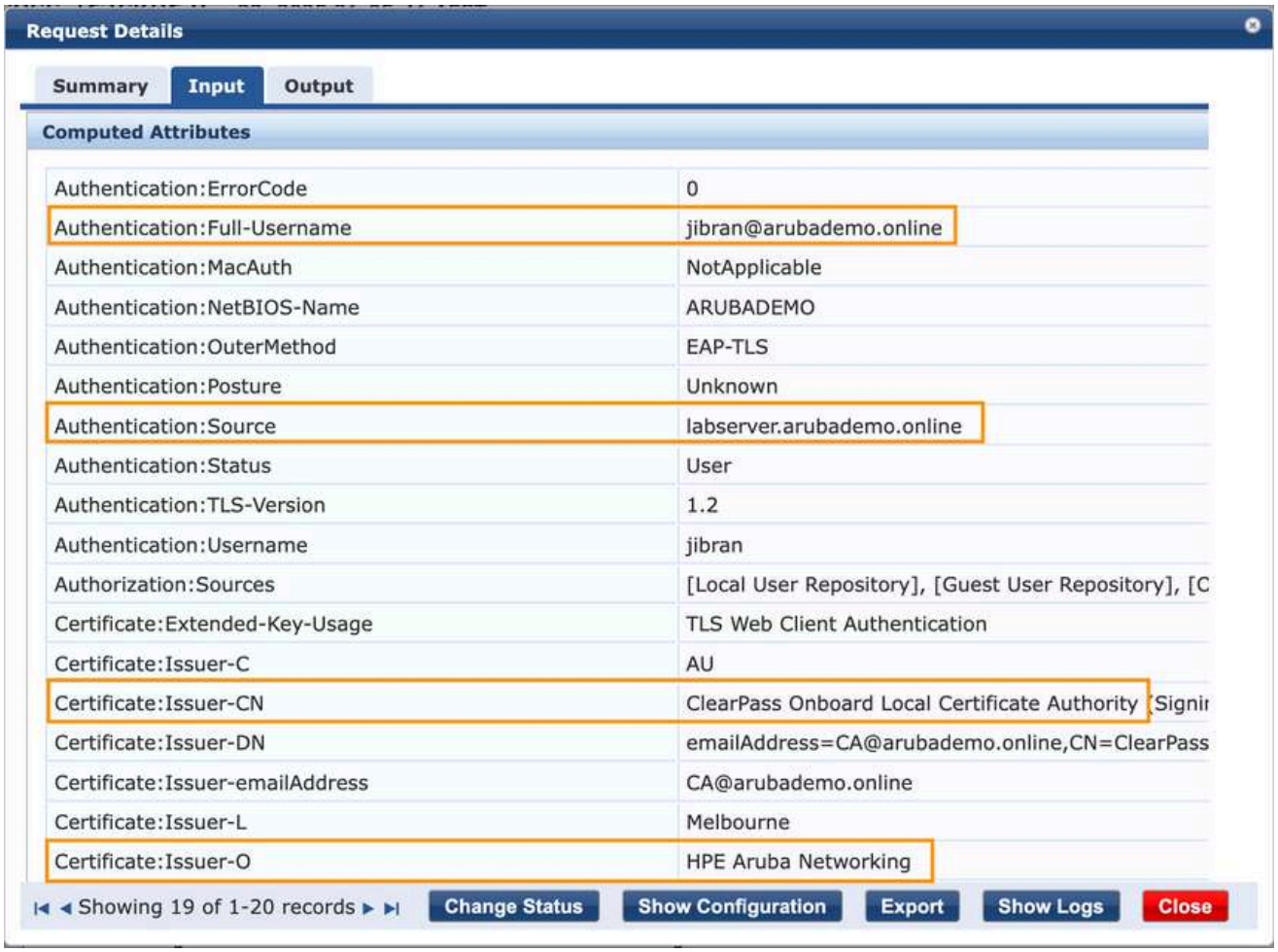


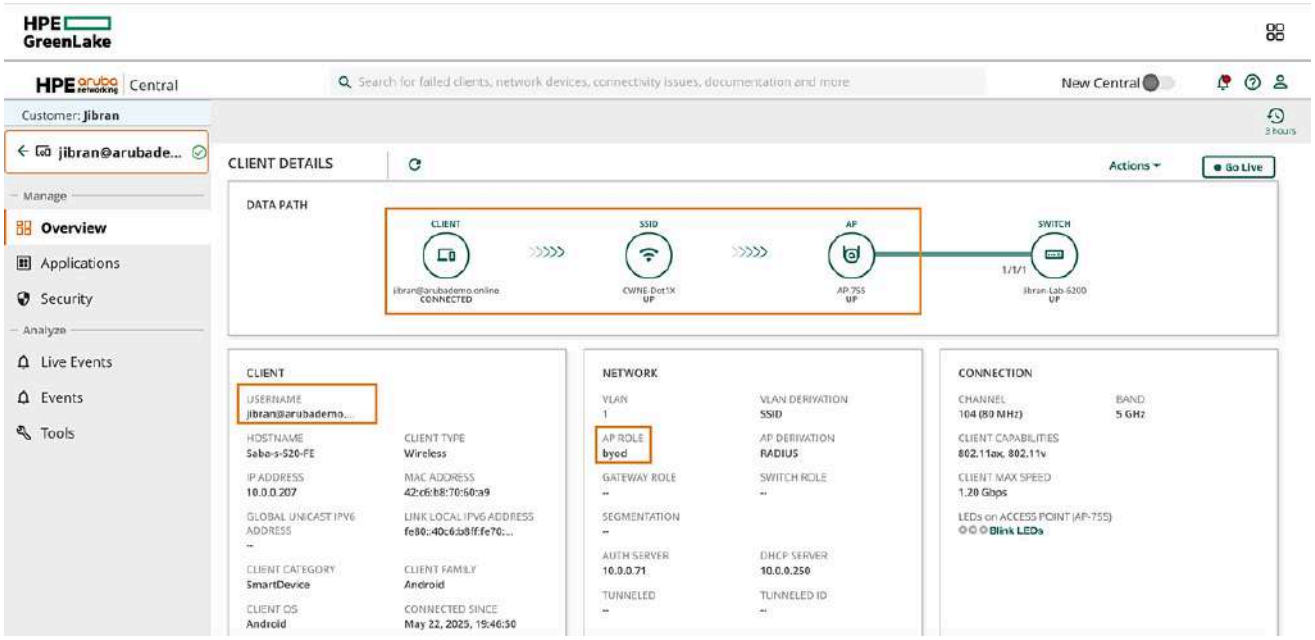
BYOD user connecting to CWNE-Dot1X SSID

Following series of screenshots (from ClearPass and Aruba Central) captures details of a user connecting to CWNE-Dot1X SSID using their personal device that has already been onboarded and how ClearPass policy authenticates the user against on-prem AD and assigns the appropriate user role based on the parameters “computed” from user’s RADIUS request. In this example, user has been assigned user role “byod”:


Request Details
Summary
Input
Output
Login Status: ACCEPT
Session Identifier: R00000281-01-682ef8cc
Date and Time: May 22, 2025 20:13:32 AEST
End-Host Identifier: 42-C6-B8-70-60-A9 Open in Central
End-Host Profile: -
End-Host Status: Unknown Mark as Known
Username: jibran@arubademo.online
Access Device IP (Port): 10.0.0.105
Access Device Name: 10.0.0.105 (CWNE-AP / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: CWNE-Dot1X
Authentication Method: EAP-TLS
Authentication Source: AD:labserver.arubademo.online
Authorization Source: [Local User Repository], [Guest User Repository], [Onboard Devices Repository], labserver.arubademo.online
Tips Role: [User Authenticated]
Enforcement Profiles: [Allow Access Profile], Aruba User Role - byod
Service Monitor Mode: Disabled
Showing 19 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

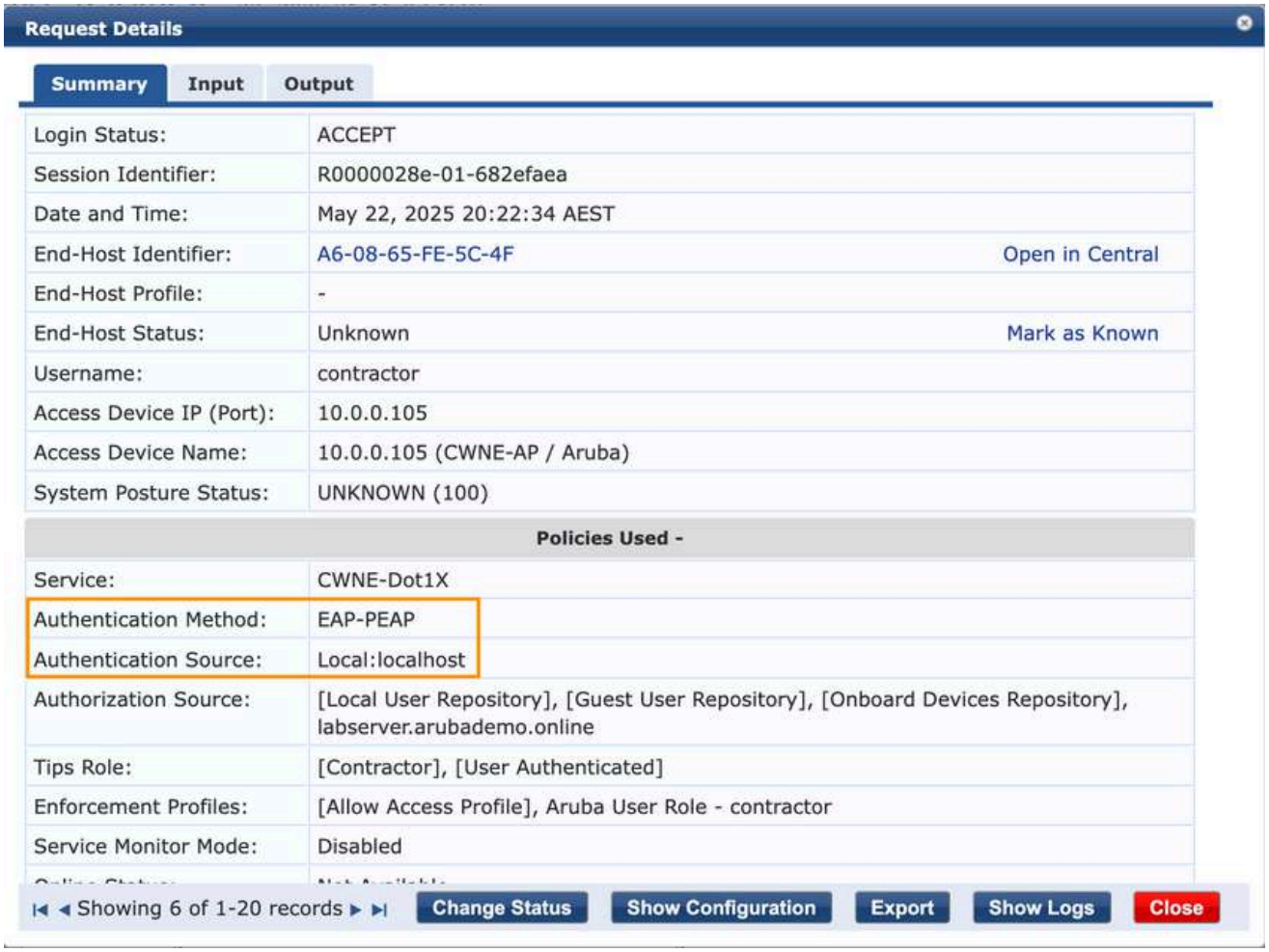

Request Details
Summary
Input
Output
RADIUS Request
Radius:Aruba:Aruba-AP-Group
CWNE-Lab
Radius:Aruba:Aruba-AP-MAC-Address
988f00c1f40c
Radius:Aruba:Aruba-Device-MAC-Address
42c6b87060a9
Radius:Aruba:Aruba-Essid-Name
CWNE-Dot1X
Radius:Aruba:Aruba-Location-Id
AP-755
Radius:IETF:Called-Station-Id
98-8F-00-C1-F4-0C
Radius:IETF:Calling-Station-Id
42-C6-B8-70-60-A9
Radius:IETF:Framed-MTU
1100
Radius:IETF:Location-Capable
9
Radius:IETF:NAS-Identifier
10.0.0.105
Radius:IETF:NAS-IP-Address
10.0.0.105
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Radius:IETF:Service-Type
2
Radius:IETF:User-Name
jibran@arubademo.online
Computed Attributes
Showing 19 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

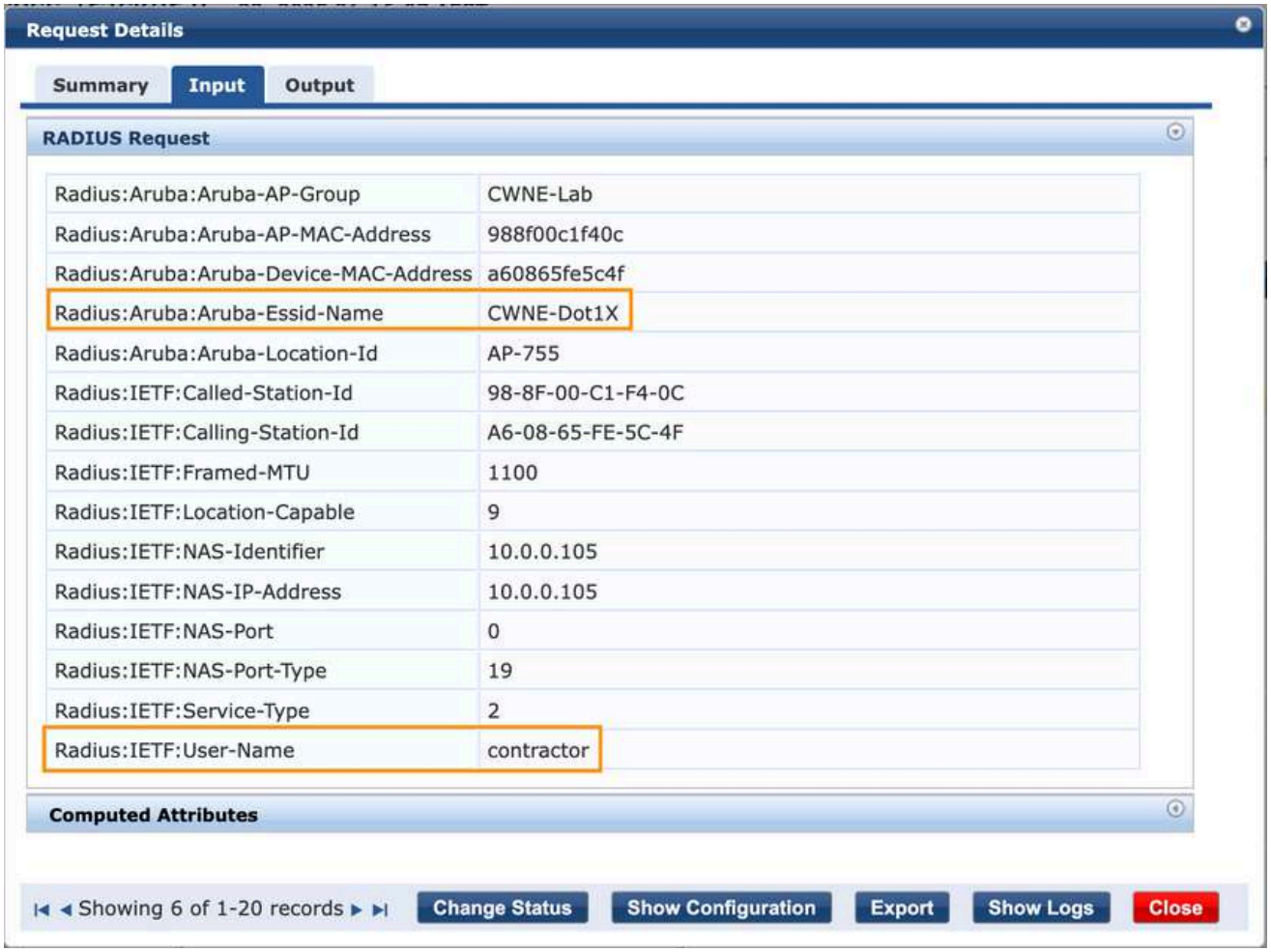

Request Details
Summary
Input
Output
Computed Attributes
Authentication:ErrorCode
0
Authentication:Full-Username
jibran@arubademo.online
Authentication:MacAuth
NotApplicable
Authentication:NetBIOS-Name
ARUBADEMO
Authentication:OuterMethod
EAP-TLS
Authentication:Posture
Unknown
Authentication:Source
labserver.arubademo.online
Authentication:Status
User
Authentication:TLS-Version
1.2
Authentication:Username
jibran
Authorization:Sources
[Local User Repository], [Guest User Repository], [C
Certificate:Extended-Key-Usage
TLS Web Client Authentication
Certificate:Issuer-C
AU
Certificate:Issuer-CN
ClearPass Onboard Local Certificate Authority
Certificate:Issuer-DN
emailAddress=CA@arubademo.online,CN=ClearPass
Certificate:Issuer-emailAddress
CA@arubademo.online
Certificate:Issuer-L
Melbourne
Certificate:Issuer-O
HPE Aruba Networking
Showing 19 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

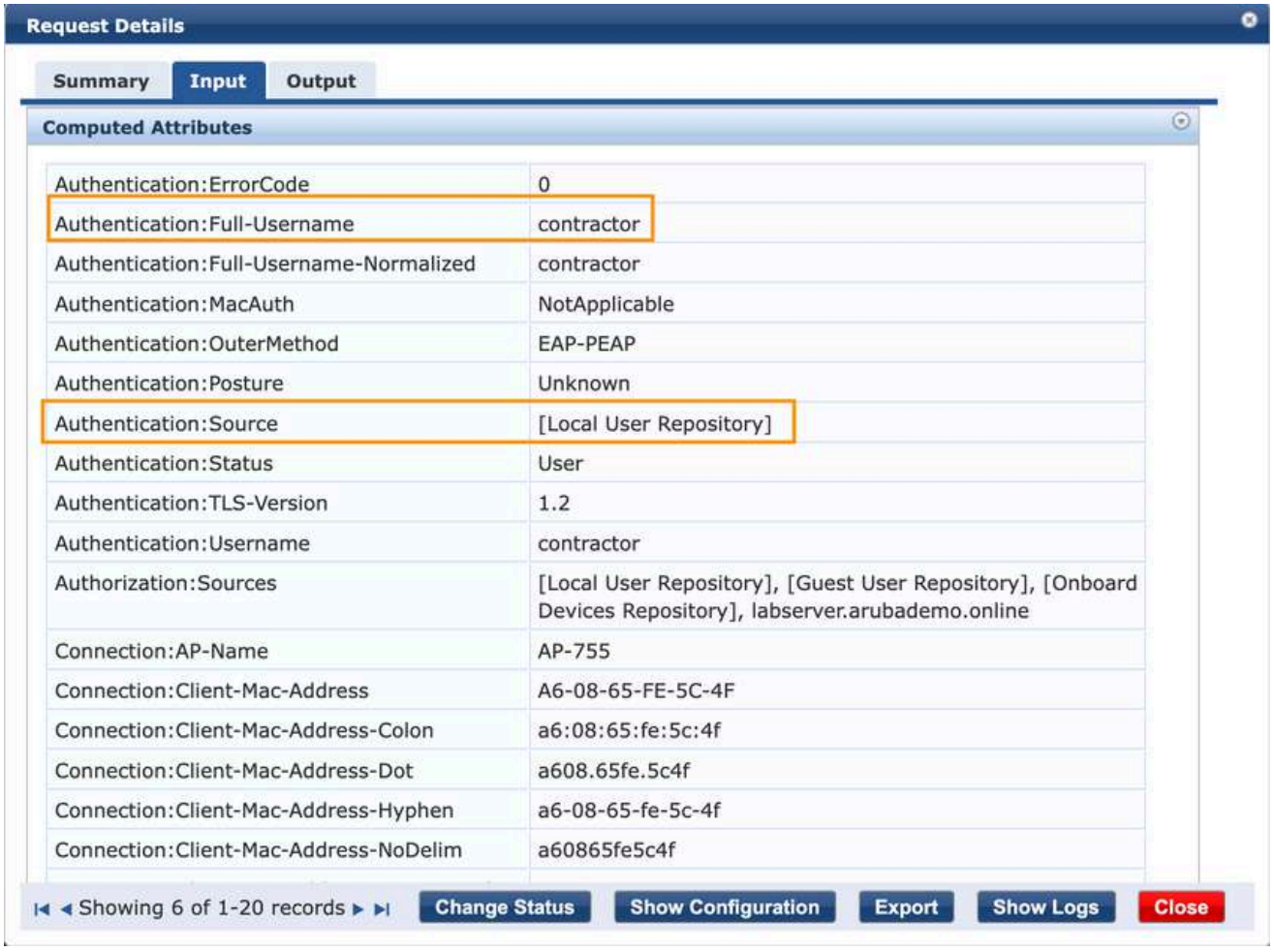


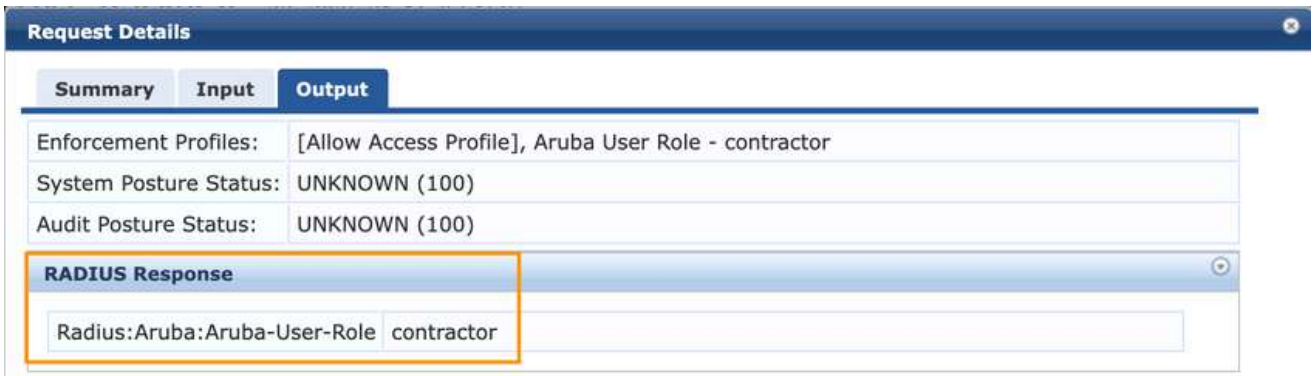
Contractor connecting to CWNE-Dot1X SSID:

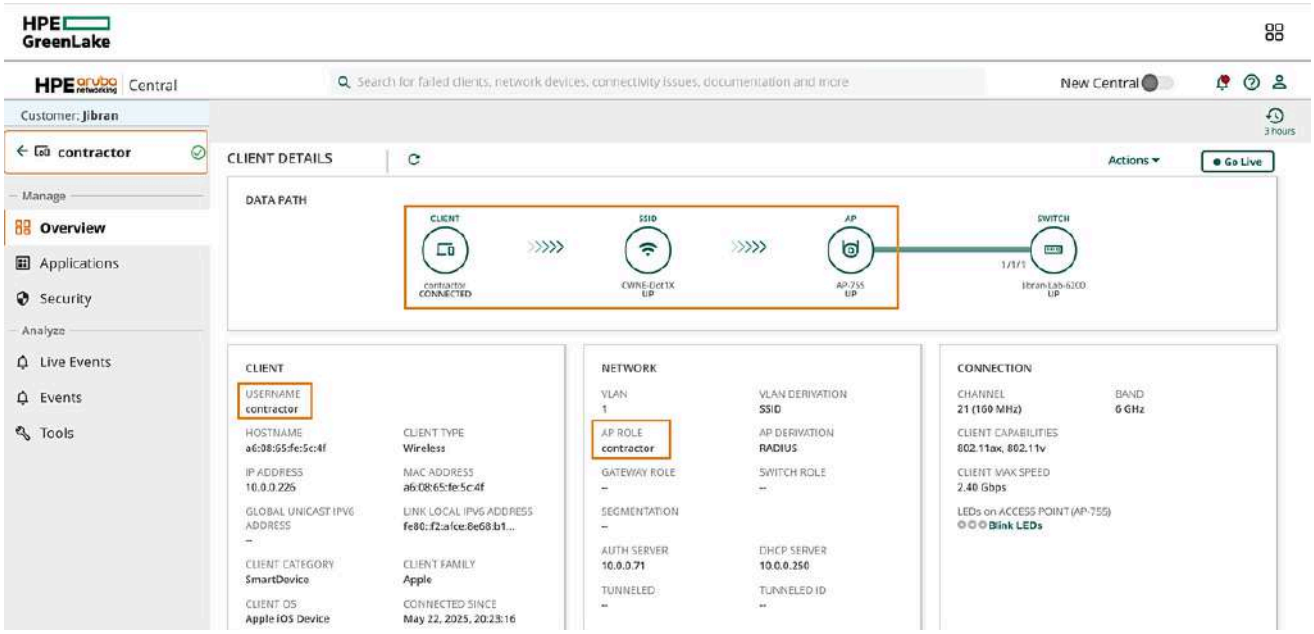
Following series of screenshots (from ClearPass and Aruba Central) captures details of a contractor connecting to CWNE-Dot1X SSID and how ClearPass policy authenticates the user against ClearPass local user repository and assigns the appropriate user role based on the parameters “computed” from user’s RADIUS request. In this example, user has been assigned user role “contractor”:


Request Details
Summary
Input
Output
Login Status: ACCEPT
Session Identifier: R0000028e-01-682efaea
Date and Time: May 22, 2025 20:22:34 AEST
End-Host Identifier: A6-08-65-FE-5C-4F
Open in Central
End-Host Profile: -
End-Host Status: Unknown
Mark as Known
Username: contractor
Access Device IP (Port): 10.0.0.105
Access Device Name: 10.0.0.105 (CWNE-AP / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: CWNE-Dot1X
Authentication Method: EAP-PEAP
Authentication Source: Local:localhost
Authorization Source: [Local User Repository], [Guest User Repository], [Onboard Devices Repository], labserver.arubademo.online
Tips Role: [Contractor], [User Authenticated]
Enforcement Profiles: [Allow Access Profile], Aruba User Role - contractor
Service Monitor Mode: Disabled
Showing 6 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
RADIUS Request
Radius:Aruba:Aruba-AP-Group
CWNE-Lab
Radius:Aruba:Aruba-AP-MAC-Address
988f00c1f40c
Radius:Aruba:Aruba-Device-MAC-Address
a60865fe5c4f
Radius:Aruba:Aruba-Essid-Name
CWNE-Dot1X
Radius:Aruba:Aruba-Location-Id
AP-755
Radius:IETF:Called-Station-Id
98-8F-00-C1-F4-0C
Radius:IETF:Calling-Station-Id
A6-08-65-FE-5C-4F
Radius:IETF:Framed-MTU
1100
Radius:IETF:Location-Capable
9
Radius:IETF:NAS-Identifier
10.0.0.105
Radius:IETF:NAS-IP-Address
10.0.0.105
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Radius:IETF:Service-Type
2
Radius:IETF:User-Name
contractor
Computed Attributes
Showing 6 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Computed Attributes
Authentication:ErrorCode
0
Authentication:Full-Username
contractor
Authentication:Full-Username-Normalized
contractor
Authentication:MacAuth
NotApplicable
Authentication:OuterMethod
EAP-PEAP
Authentication:Posture
Unknown
Authentication:Source
[Local User Repository]
Authentication:Status
User
Authentication:TLS-Version
1.2
Authentication:Username
contractor
Authorization:Sources
[Local User Repository], [Guest User Repository], [Onboard Devices Repository], labserver.arubademo.online
Connection:AP-Name
AP-755
Connection:Client-Mac-Address
A6-08-65-FE-5C-4F
Connection:Client-Mac-Address-Colon
a6:08:65:fe:5c:4f
Connection:Client-Mac-Address-Dot
a608.65fe.5c4f
Connection:Client-Mac-Address-Hyphen
a6-08-65-fe-5c-4f
Connection:Client-Mac-Address-NoDelim
a60865fe5c4f
Showing 6 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Enforcement Profiles:
[Allow Access Profile], Aruba User Role - contractor
System Posture Status:
UNKNOWN (100)
Audit Posture Status:
UNKNOWN (100)
RADIUS Response
Radius:Aruba:Aruba-User-Role
contractor



To summarize, we have used the same SSID to allow corporate users to connect to the network using their corporate devices, allow corporate users to connect their personal devices to the network and allow contractors to the network. Important to note that while they are all connecting to the same SSID, they have been assigned different user roles and have different level of network/resources access based on their roles.

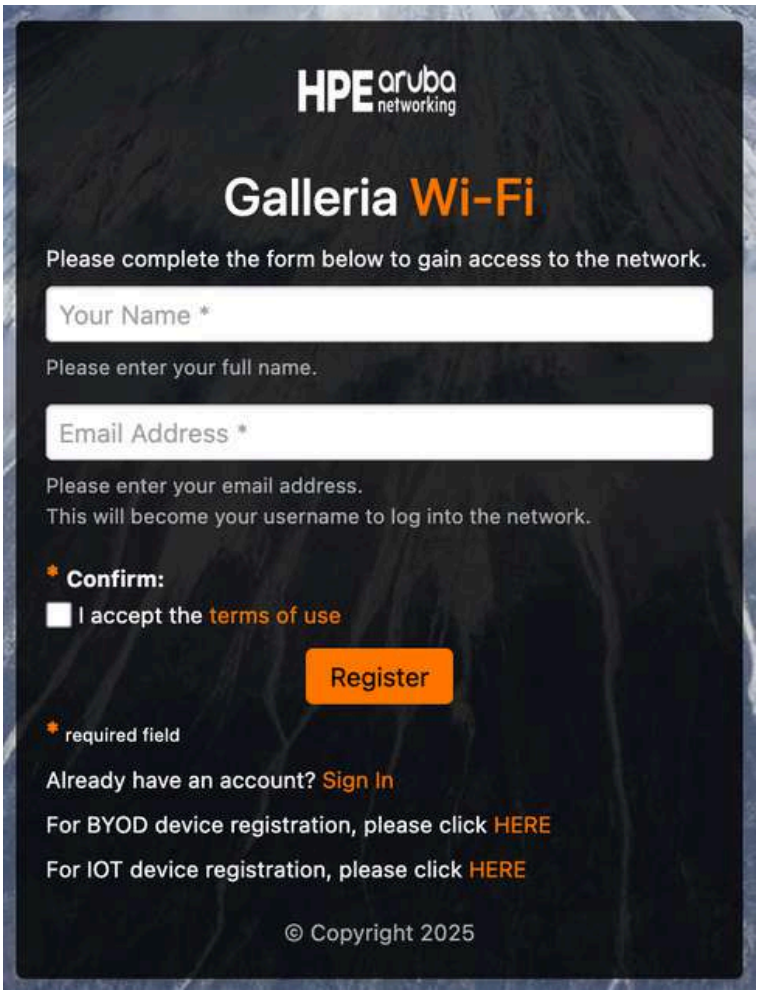
SSID 2 - CWNE-Guest

CWNE-Guest SSID has been configured to serve following functions:

- Connect guest users to the Wi-Fi network
- Enable BYOD users to onboard their personal devices

A user connected to the guest Wi-Fi network is redirected to the captive portal page that provides them following options:

- Register a new guest account or log In using existing guest credential
- Onboard a new personal device (BYOD)
- Register a new device mac address and create a unique pre-shared key for that device to connect to the MPSK SSID



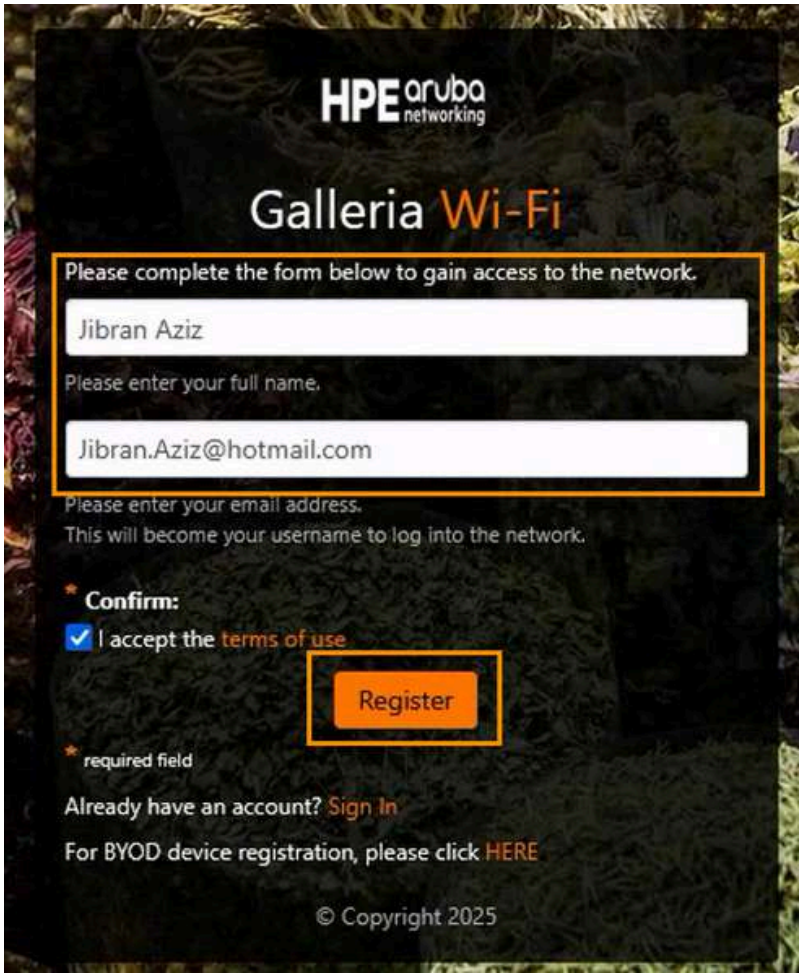
Guest user connecting to CWNE-Guest SSID

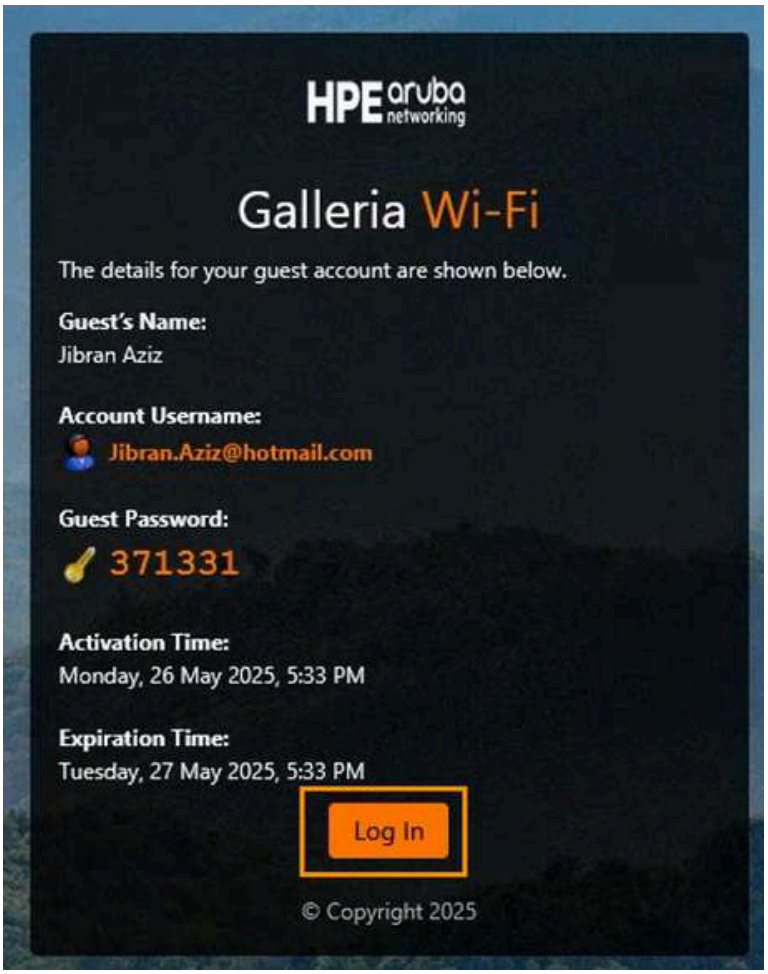
In order to avoid guest users being redirected to captive portal every time they authenticate to the network, MAC caching has been enabled. As part of the initial captive portal authentication, ClearPass will cache the mac address of the client and will automatically assign them network access with guest role for the subsequent authentication requests until their mac cache is valid. A user connecting to the guest network for the first time will see a mac authentication failure log on ClearPass as their MAC address will not be cached at that time:

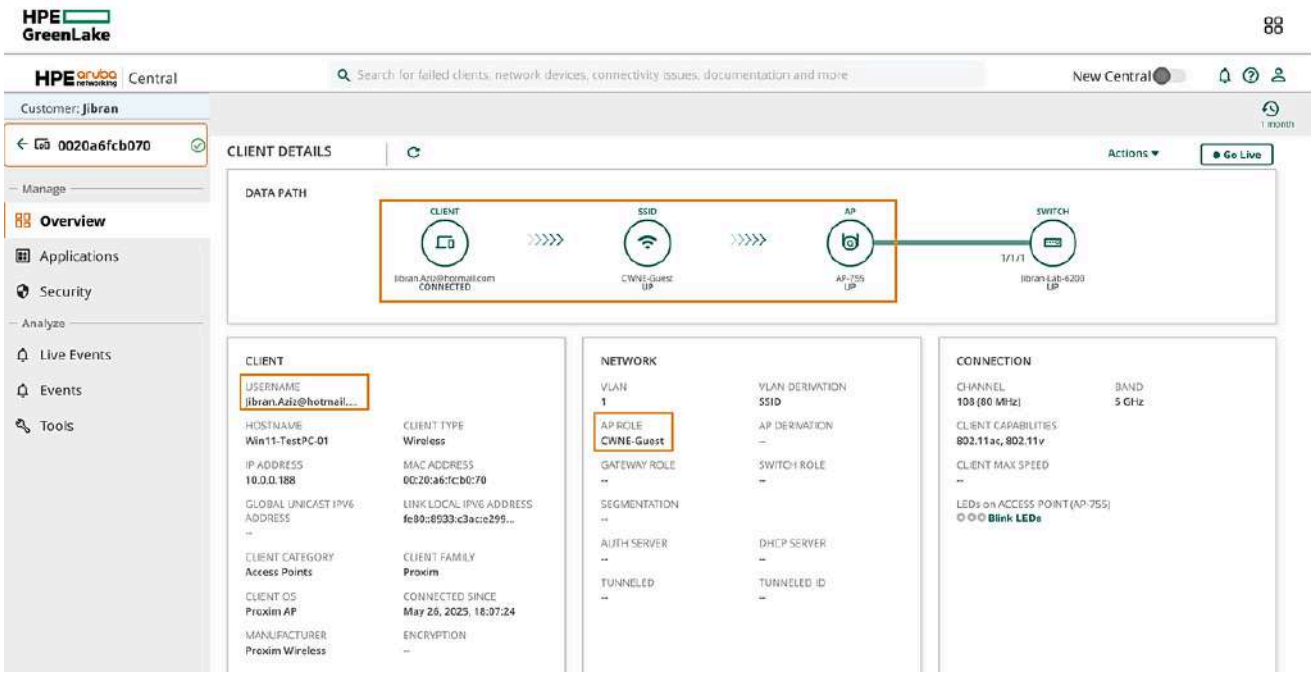
6.	0020a6fcb070	Guest MAC Authentication	REJECT	RADIUS	2025/05/26 17:02:25

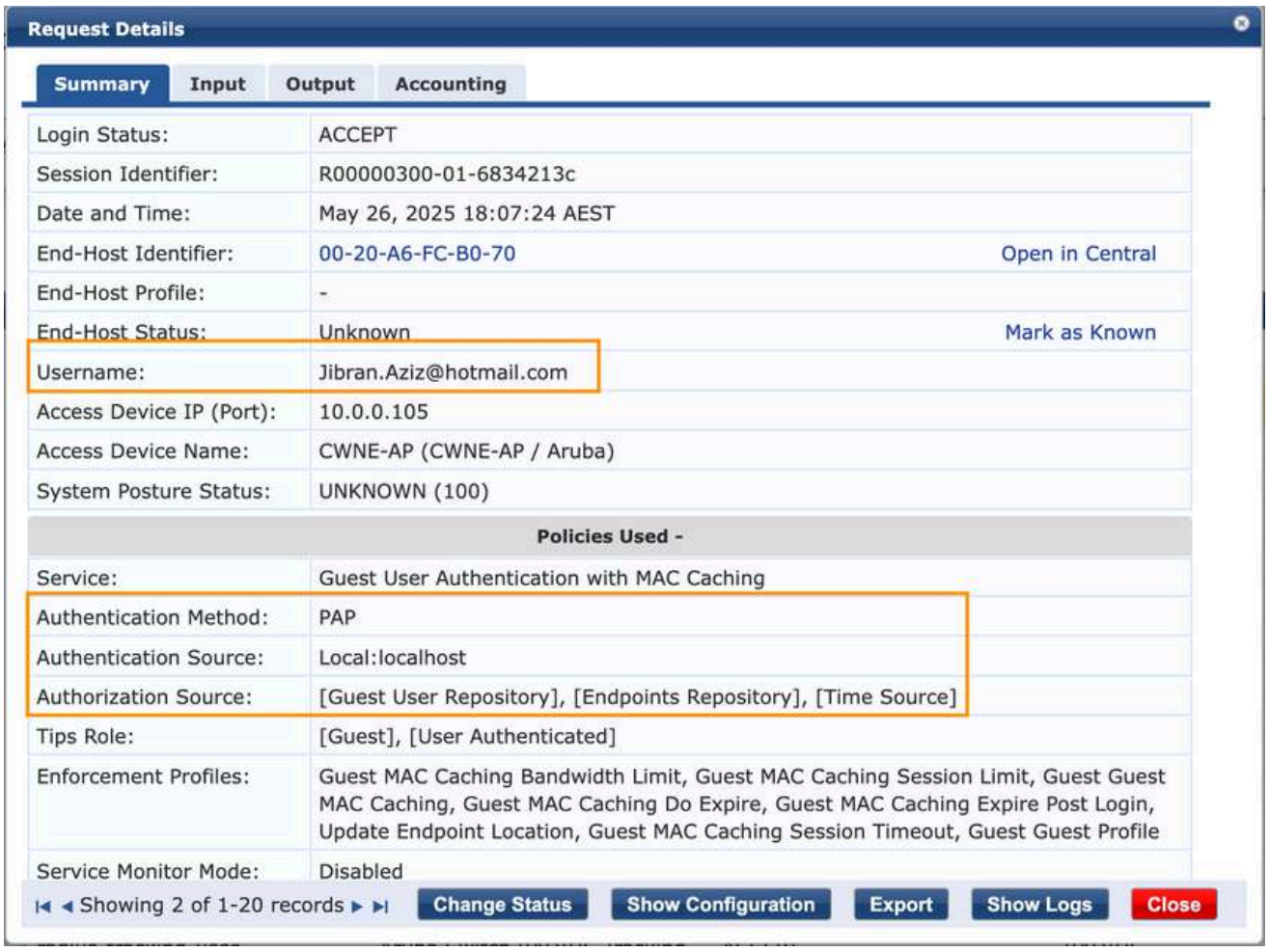
After initial MAC auth failure, user will be redirected to the captive portal page. The guest user registering for a new account will enter their details (name and email address in this case but these fields are customizable and can be changed based on the requirements).

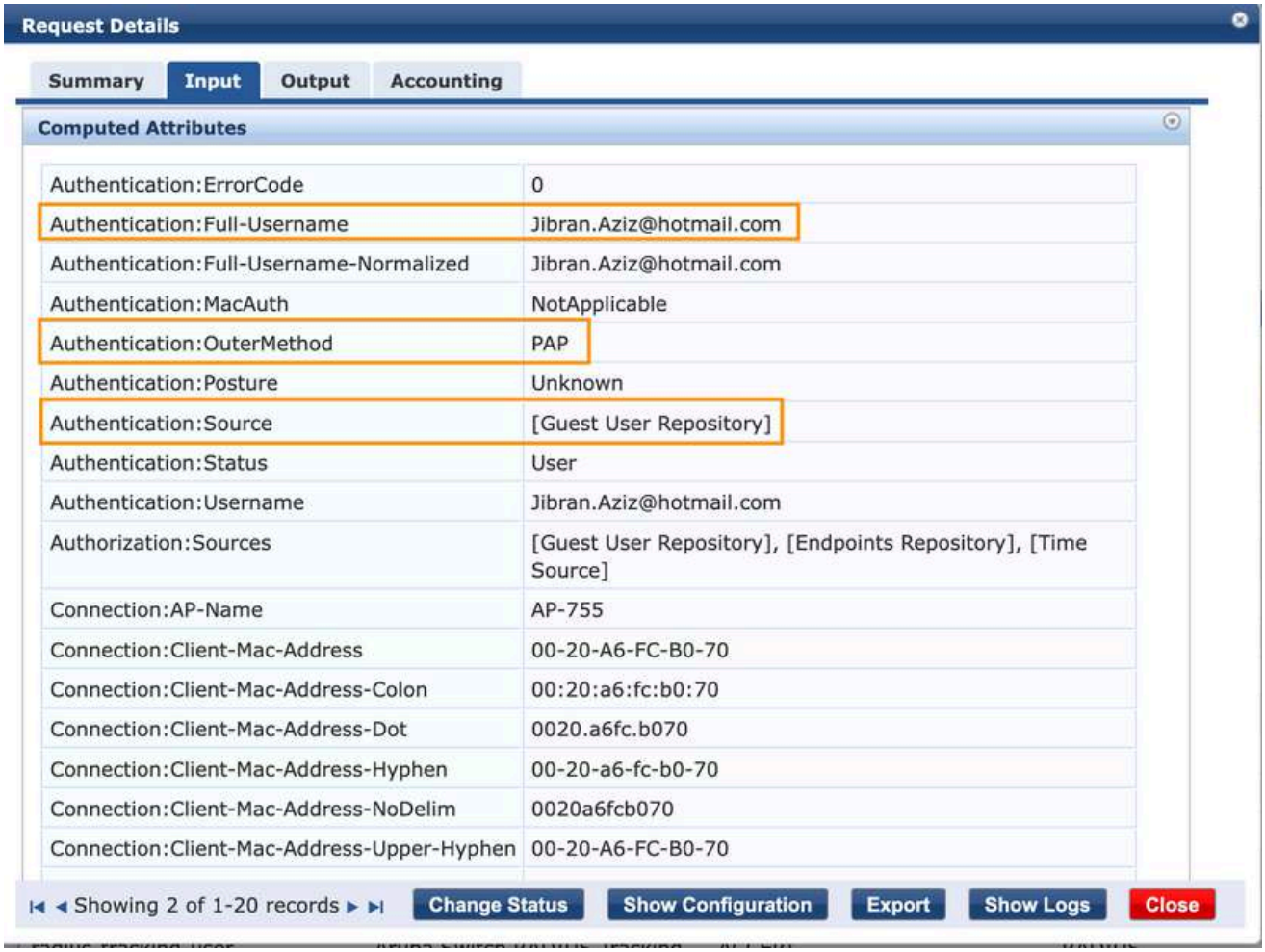
Following series of screenshots (from ClearPass and Aruba Central) captures details of a guest user connecting to CWNE-guest SSID and how ClearPass policy allows the user to register for a new account and log in to the guest Wi-Fi network:



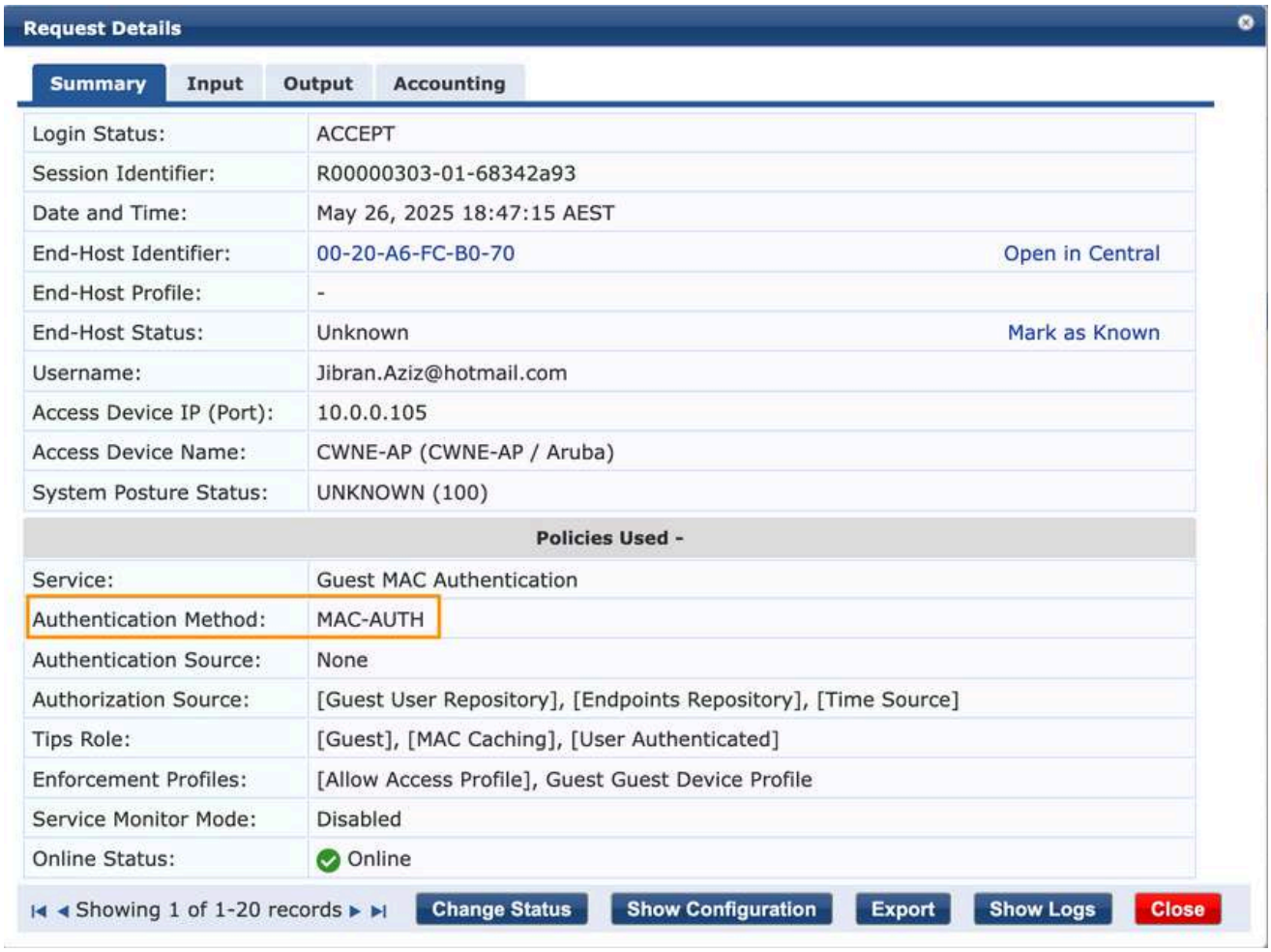

HPE aruba networking
Galleria Wi-Fi
The details for your guest account are shown below.
Guest's Name:
Jibran Aziz
Account Username:
Jibran.Aziz@hotmail.com
Guest Password:
371331
Activation Time:
Monday, 26 May 2025, 5:33 PM
Expiration Time:
Tuesday, 27 May 2025, 5:33 PM
Log In
© Copyright 2025

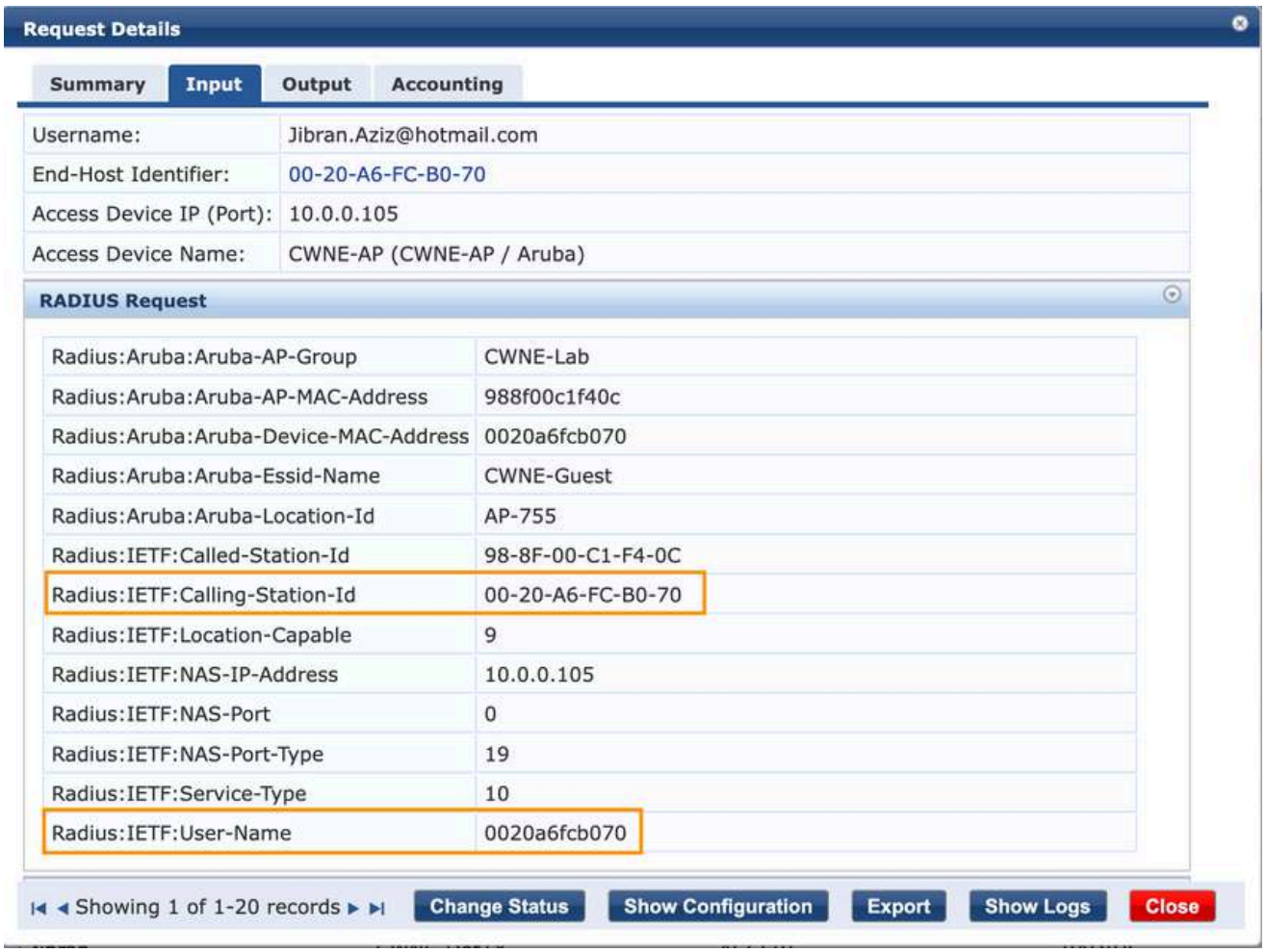

HPE GreenLake
HPE aruba networking Central
Search for failed clients, network devices, connectivity issues, documentation and more
New Central
Customer: Jibran
0020a6fcb070
CLIENT DETAILS
Actions
Go Live
Manage
Overview
Applications
Security
Analyze
Live Events
Events
Tools
DATA PATH
CLIENT
SSID
AP
SWITCH
CONNECTED
CWNE-Guest
1/1/1
CLIENT
USERNAME
HOSTNAME
Win11-TestPC-01
CLIENT TYPE
Wireless
IP ADDRESS
10.0.0.188
MAC ADDRESS
CLIENT CATEGORY
Access Points
CLIENT FAMILY
Proxim
CLIENT OS
Proxim AP
CONNECTED SINCE
May 26, 2025, 18:07:24
MANUFACTURER
Proxim Wireless
ENCRYPTION
NETWORK
VLAN
1
VLAN DERIVATION
SSID
AP ROLE
CWNE-Guest
AP DERIVATION
GATEWAY ROLE
SWITCH ROLE
SEGMENTATION
AUTH SERVER
DHCP SERVER
TUNNELED
TUNNELED ID
CONNECTION
CHANNEL
108 (80 MHz)
BAND
5 GHz
CLIENT CAPABILITIES
802.11ac, 802.11v
CLIENT MAX SPEED
LEDs on ACCESS POINT (AP-755)
Blink LEDs


Request Details
Summary
Input
Output
Accounting
Login Status: ACCEPT
Session Identifier: R00000300-01-6834213c
Date and Time: May 26, 2025 18:07:24 AEST
End-Host Identifier: 00-20-A6-FC-B0-70
Open in Central
End-Host Profile: -
End-Host Status: Unknown
Mark as Known
Username: Jibran.Aziz@hotmail.com
Access Device IP (Port): 10.0.0.105
Access Device Name: CWNE-AP (CWNE-AP / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: Guest User Authentication with MAC Caching
Authentication Method: PAP
Authentication Source: Local:localhost
Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]
Tips Role: [Guest], [User Authenticated]
Enforcement Profiles: Guest MAC Caching Bandwidth Limit, Guest MAC Caching Session Limit, Guest Guest MAC Caching, Guest MAC Caching Do Expire, Guest MAC Caching Expire Post Login, Update Endpoint Location, Guest MAC Caching Session Timeout, Guest Guest Profile
Service Monitor Mode: Disabled
Showing 2 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close



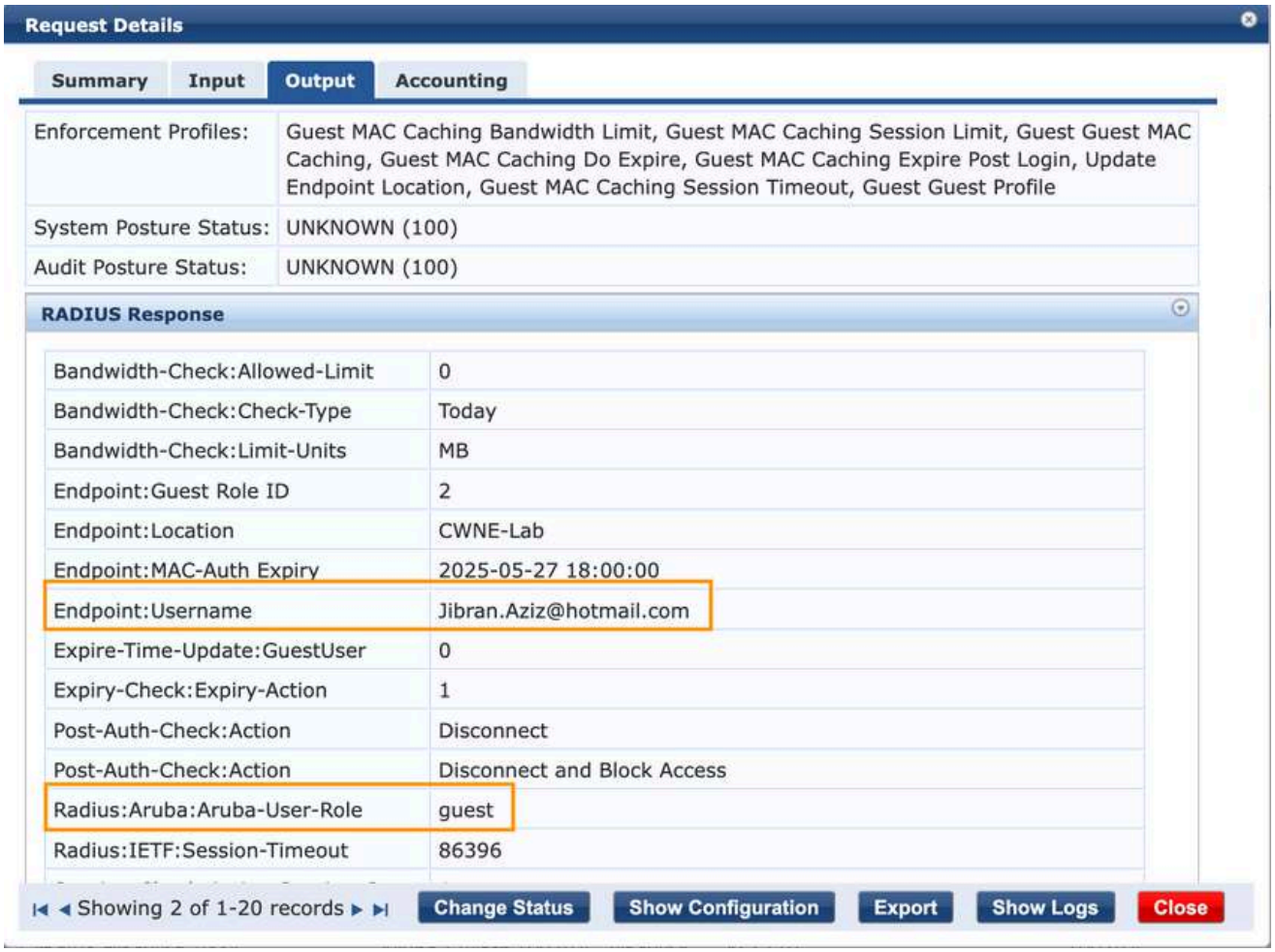
Following screenshots show how mac authentication for subsequent requests allows users to connect the network without going through the captive portal and can get network access while mac address cache is valid:


Request Details
Summary
Input
Output
Accounting
Login Status: ACCEPT
Session Identifier: R00000303-01-68342a93
Date and Time: May 26, 2025 18:47:15 AEST
End-Host Identifier: 00-20-A6-FC-B0-70
Open in Central
End-Host Profile: -
End-Host Status: Unknown
Mark as Known
Username: Jibran.Aziz@hotmail.com
Access Device IP (Port): 10.0.0.105
Access Device Name: CWNE-AP (CWNE-AP / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: Guest MAC Authentication
Authentication Method: MAC-AUTH
Authentication Source: None
Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]
Tips Role: [Guest], [MAC Caching], [User Authenticated]
Enforcement Profiles: [Allow Access Profile], Guest Guest Device Profile
Service Monitor Mode: Disabled
Online Status: Online
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Accounting
Username:
Jibran.Aziz@hotmail.com
End-Host Identifier:
00-20-A6-FC-B0-70
Access Device IP (Port):
10.0.0.105
Access Device Name:
CWNE-AP (CWNE-AP / Aruba)
RADIUS Request
Radius:Aruba:Aruba-AP-Group
CWNE-Lab
Radius:Aruba:Aruba-AP-MAC-Address
988f00c1f40c
Radius:Aruba:Aruba-Device-MAC-Address
0020a6fcb070
Radius:Aruba:Aruba-Essid-Name
CWNE-Guest
Radius:Aruba:Aruba-Location-Id
AP-755
Radius:IETF:Called-Station-Id
98-8F-00-C1-F4-0C
Radius:IETF:Calling-Station-Id
00-20-A6-FC-B0-70
Radius:IETF:Location-Capable
9
Radius:IETF:NAS-IP-Address
10.0.0.105
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Radius:IETF:Service-Type
10
Radius:IETF:User-Name
0020a6fcb070
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Accounting
Connection:Client-Mac-Address-NoDelim
0020a6fcb070
Connection:Client-Mac-Address-Upper-Hyphen
00-20-A6-FC-B0-70
Connection:Client-Mac-Vendor
Proxim Wireless
Connection:Dest-IP-Address
10.0.0.71
Connection:Dest-Port
1812
Connection:NAD-IP-Address
10.0.0.105
Connection:Protocol
RADIUS
Connection:Src-IP-Address
10.0.0.105
Connection:Src-Port
57426
Connection:SSID
CWNE-Guest
Date:Date-Time
2025-05-26 18:47:15
Endpoint:Device Name
Windows 10
Endpoint:Device Type
Windows
Endpoint:Expanded Device Type
Windows
Endpoint:Guest Role ID
2
Endpoint:Location
CWNE-Lab
Endpoint:MAC-Auth Expiry
2025-05-27 18:00:00
Endpoint:Owner
jibran
Endpoint:Username
Jibran.Aziz@hotmail.com
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

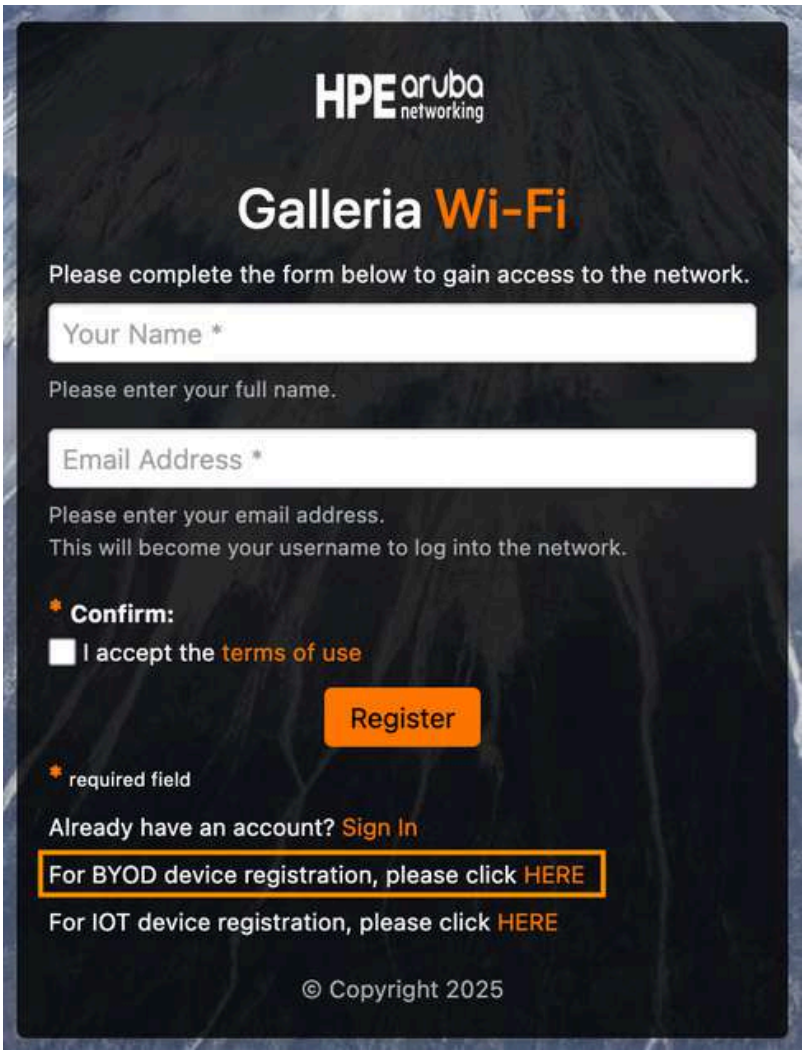

Request Details
Summary
Input
Output
Accounting
Enforcement Profiles:
[Allow Access Profile], Guest Guest Device Profile
System Posture Status:
UNKNOWN (100)
Audit Posture Status:
UNKNOWN (100)
RADIUS Response
Radius:Aruba:Aruba-User-Role
guest
Radius:IETF:User-Name
Jibran.Aziz@hotmail.com

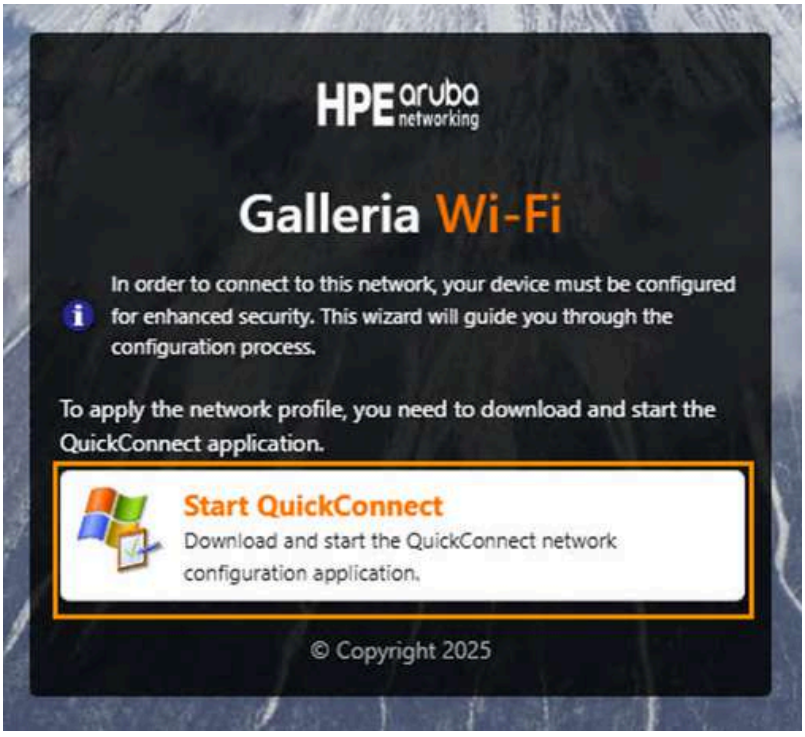


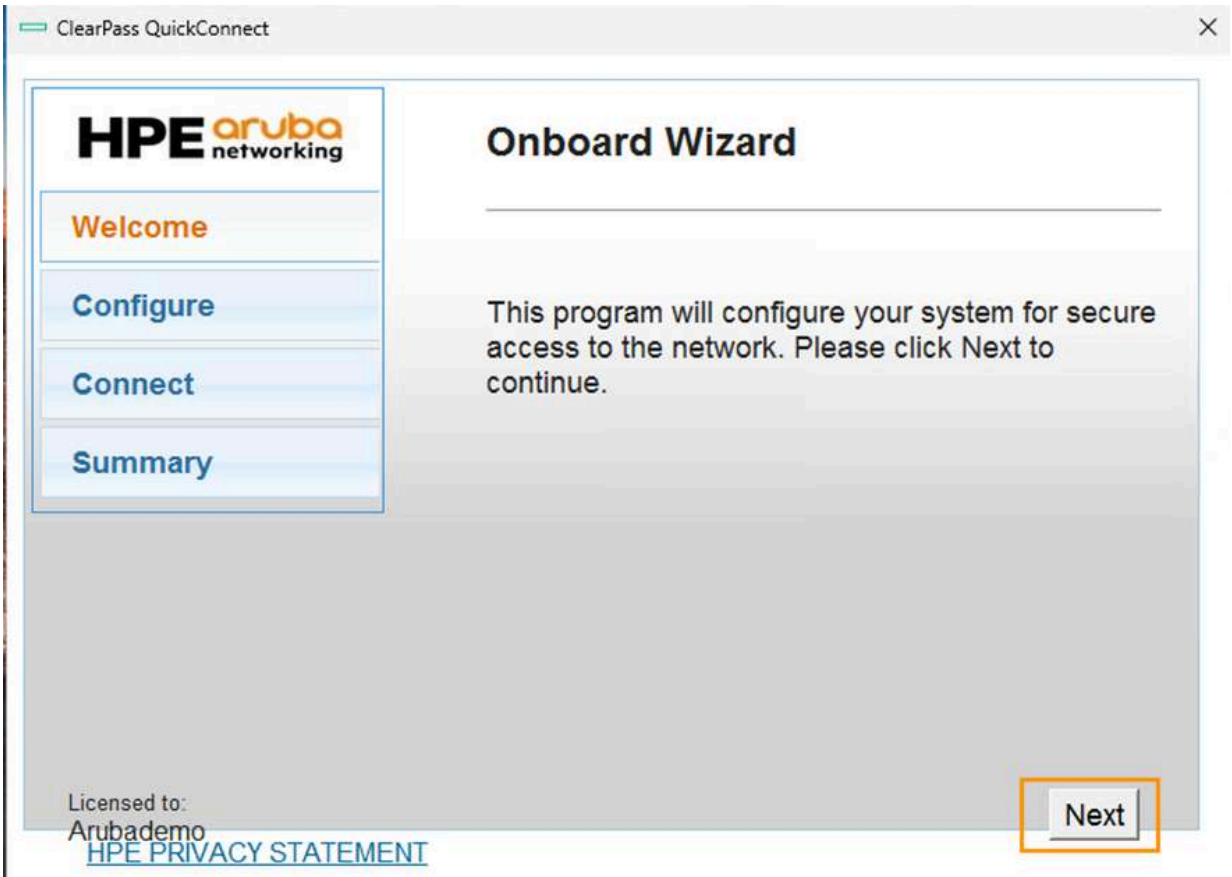
BYOD user connecting to CWNE-Guest SSID to onboard their device:

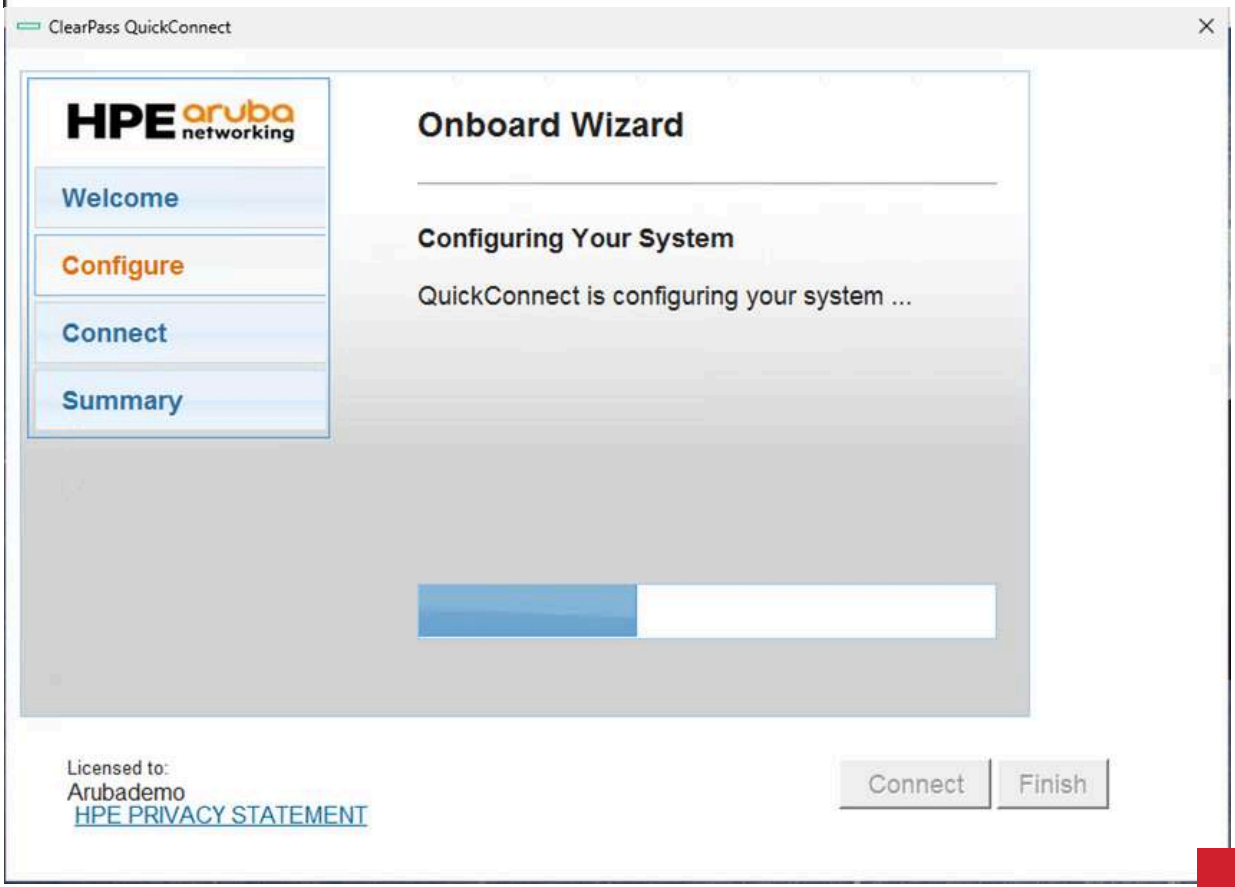
For corporate users trying to onboard their personal devices, they'll connect to the guest SSID and will be redirected to the captive portal page and click the BYOD registration link to onboard their device. After authenticating using their AD credentials, users will download the onboard client that will take them through the onboarding process.

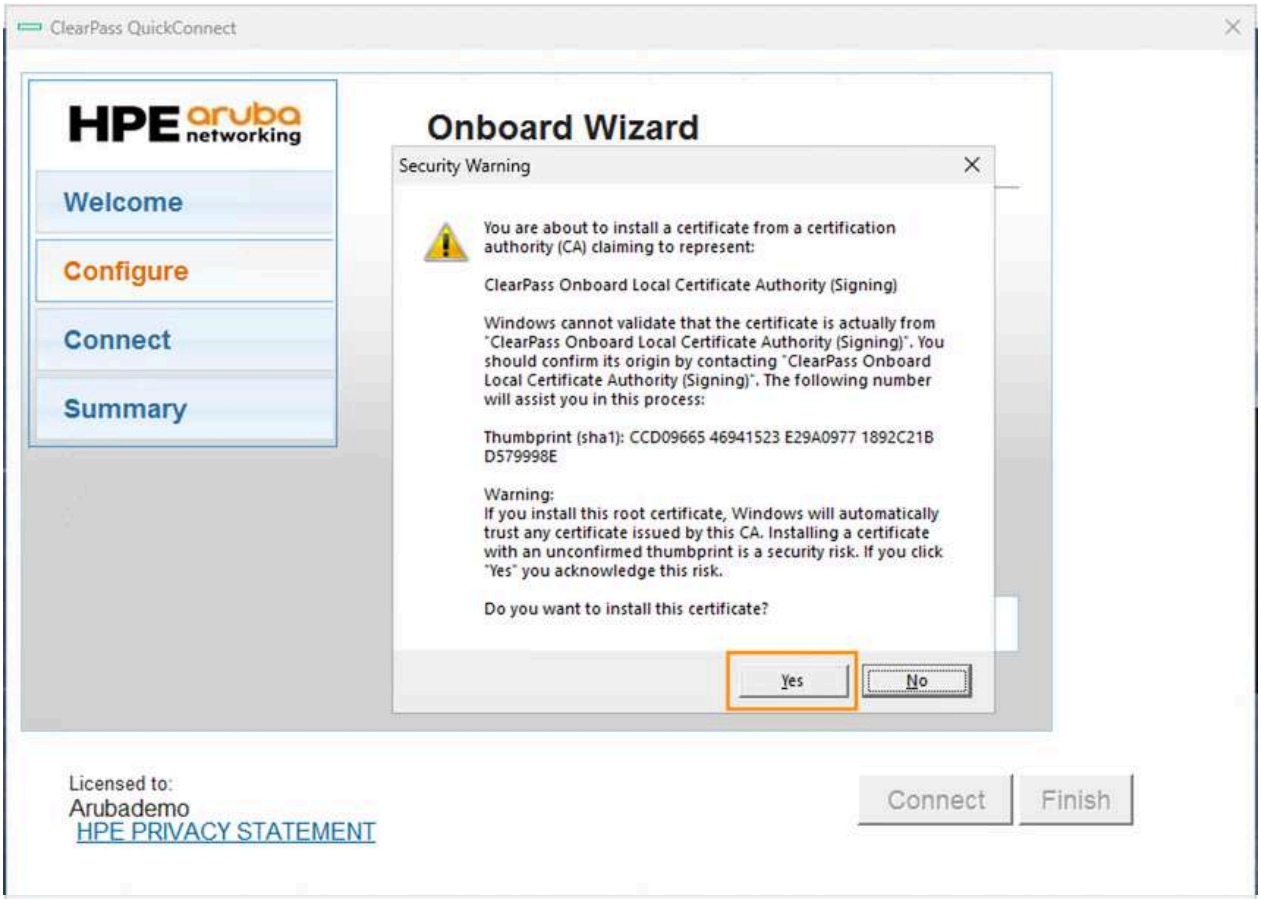
Following screenshots captures onboarding process for a user onboarding their personal devices. The actual user authentication connecting to CWNP-802.1X SSID post onboarding has been captured in the previous screenshots.

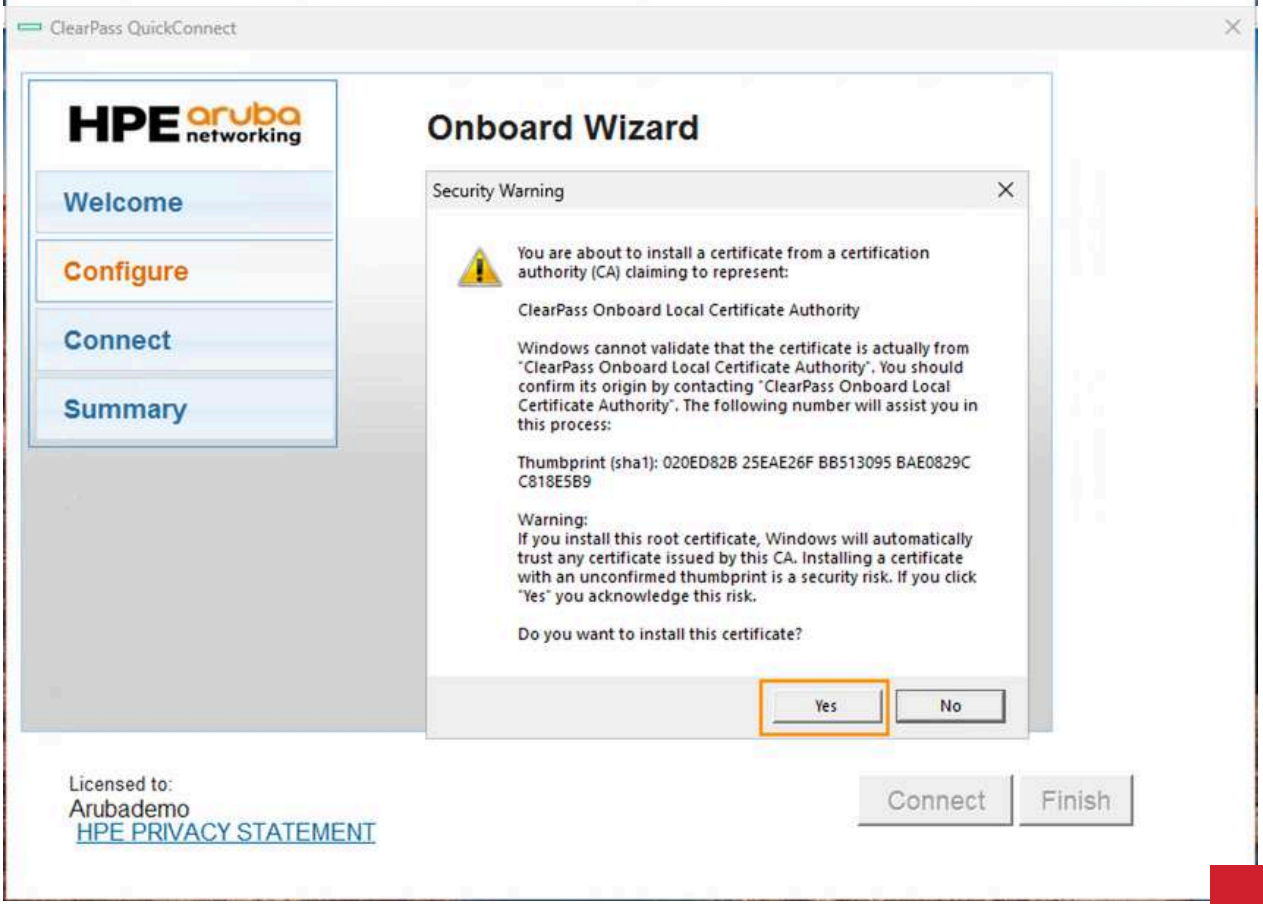

HPE aruba networking
Galleria Wi-Fi
Please complete the form below to gain access to the network.
Your Name *
Please enter your full name.
Email Address *
Please enter your email address.
This will become your username to log into the network.
* Confirm:
I accept the terms of use
Register
* required field
Already have an account? Sign In
For BYOD device registration, please click HERE
For IOT device registration, please click HERE
© Copyright 2025

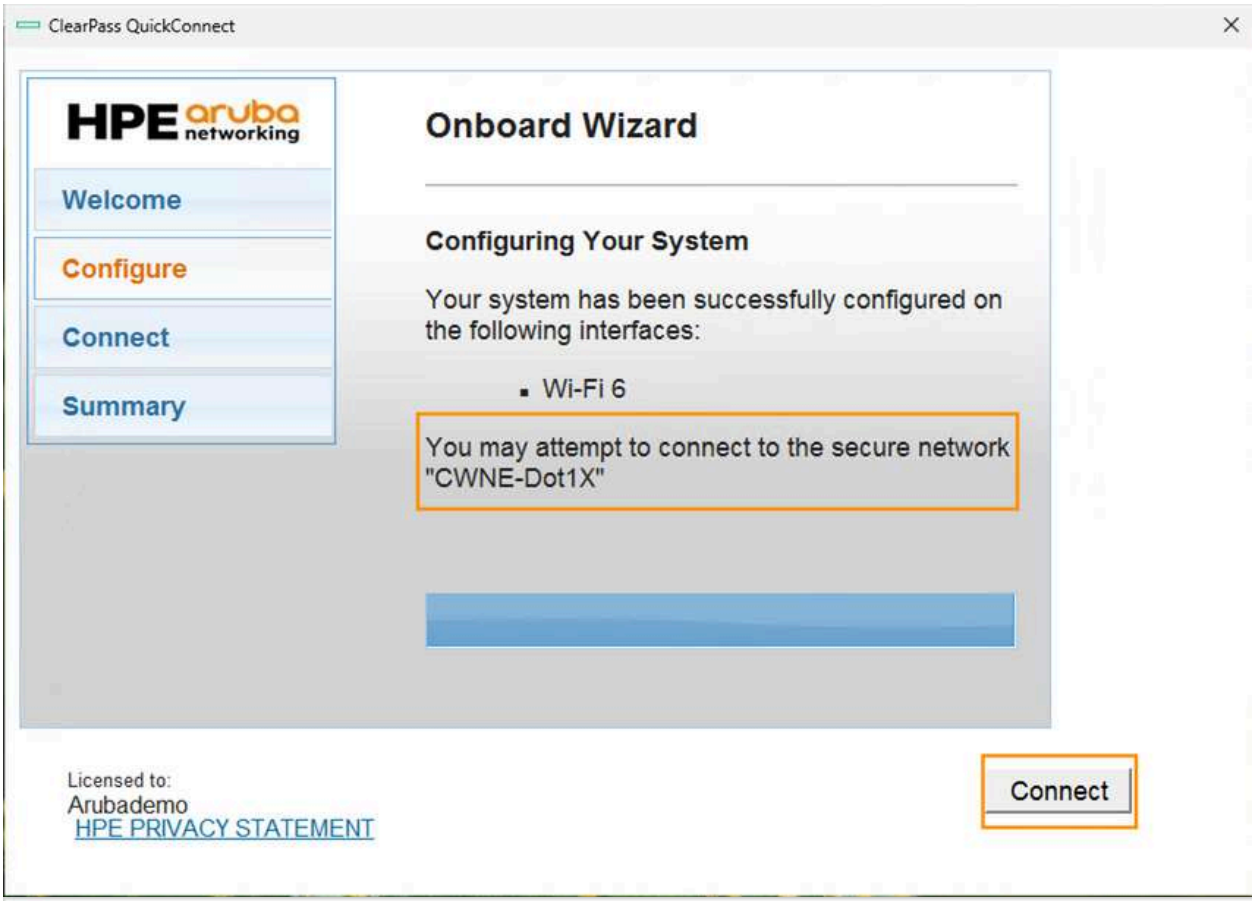

HPE aruba networking
Galleria Wi-Fi
In order to connect to this network, your device must be configured for enhanced security. This wizard will guide you through the configuration process.
To apply the network profile, you need to download and start the QuickConnect application.
Start QuickConnect
Download and start the QuickConnect network configuration application.
© Copyright 2025

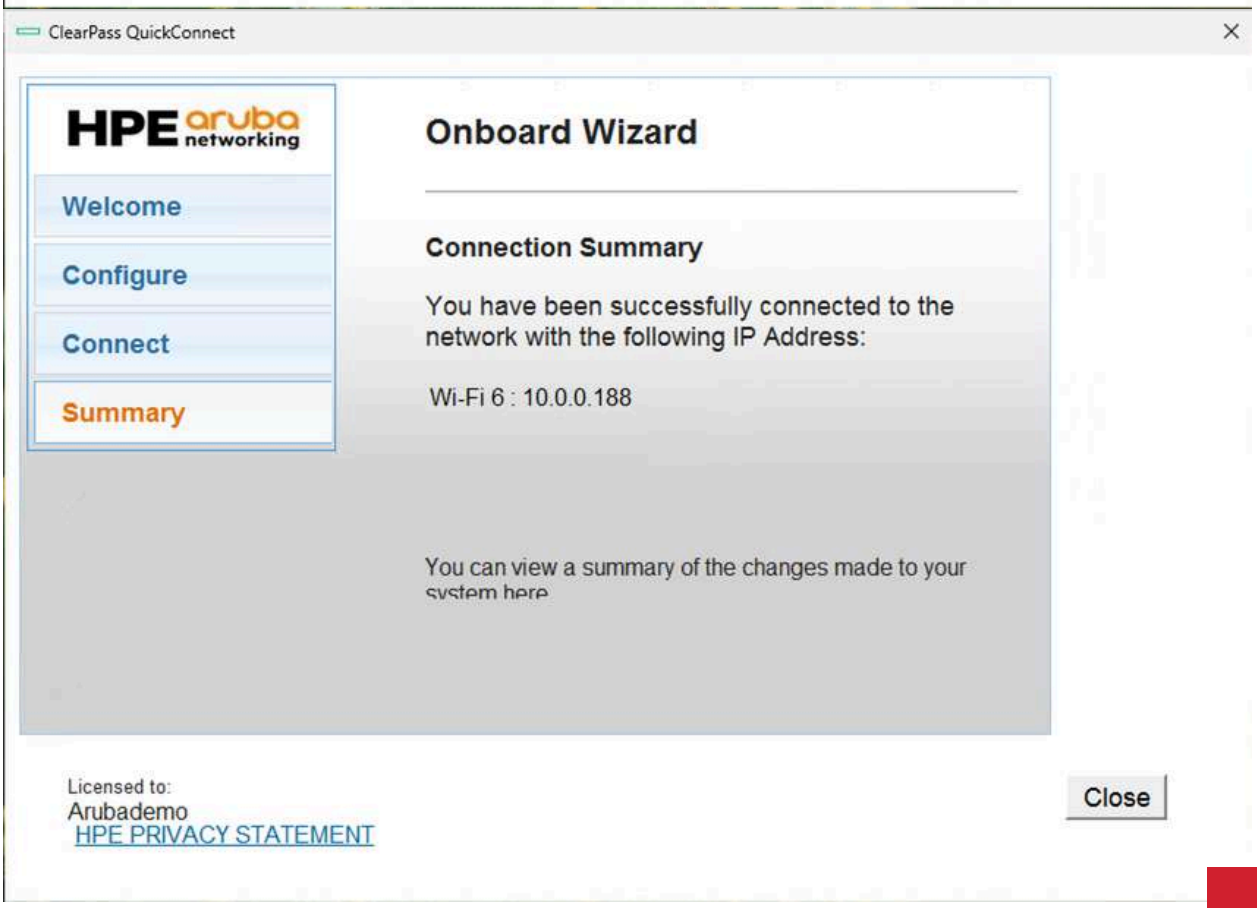

ClearPass QuickConnect
HPE aruba networking
Welcome
Configure
Connect
Summary
Onboard Wizard
This program will configure your system for secure access to the network. Please click Next to continue.
Licensed to:
Arubademo
HPE PRIVACY STATEMENT
Next


ClearPass QuickConnect
HPE aruba networking
Welcome
Configure
Connect
Summary
Onboard Wizard
Configuring Your System
QuickConnect is configuring your system ...
Licensed to:
Arubademo
HPE PRIVACY STATEMENT
Connect
Finish


ClearPass QuickConnect
HPE aruba networking
Welcome
Configure
Connect
Summary
Onboard Wizard
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
ClearPass Onboard Local Certificate Authority (Signing)
Windows cannot validate that the certificate is actually from "ClearPass Onboard Local Certificate Authority (Signing)". You should confirm its origin by contacting "ClearPass Onboard Local Certificate Authority (Signing)". The following number will assist you in this process:
Thumbprint (sha1): CCD09665 46941523 E29A0977 1892C21B D579998E
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No
Licensed to:
Arubademo
HPE PRIVACY STATEMENT
Connect
Finish


ClearPass QuickConnect
HPE aruba networking
Welcome
Configure
Connect
Summary
Onboard Wizard
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
ClearPass Onboard Local Certificate Authority
Windows cannot validate that the certificate is actually from "ClearPass Onboard Local Certificate Authority". You should confirm its origin by contacting "ClearPass Onboard Local Certificate Authority". The following number will assist you in this process:
Thumbprint (sha1): 020ED82B 25EAE26F BB513095 BAE0829C C818E5B9
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No
Licensed to:
Arubademo
HPE PRIVACY STATEMENT
Connect
Finish

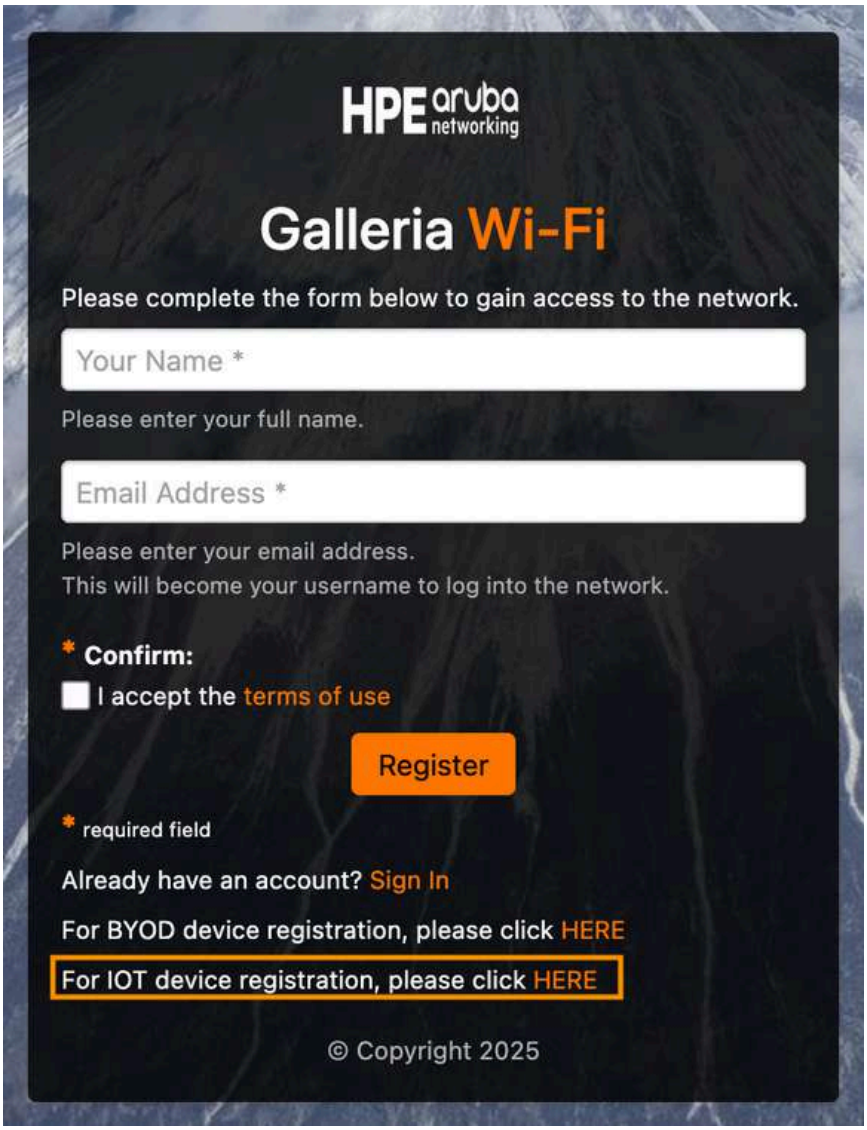

ClearPass QuickConnect
HPE aruba networking
Welcome
Configure
Connect
Summary
Onboard Wizard
Configuring Your System
Your system has been successfully configured on the following interfaces:
Wi-Fi 6
You may attempt to connect to the secure network "CWNE-Dot1X"
Licensed to:
Arubademo
HPE PRIVACY STATEMENT
Connect

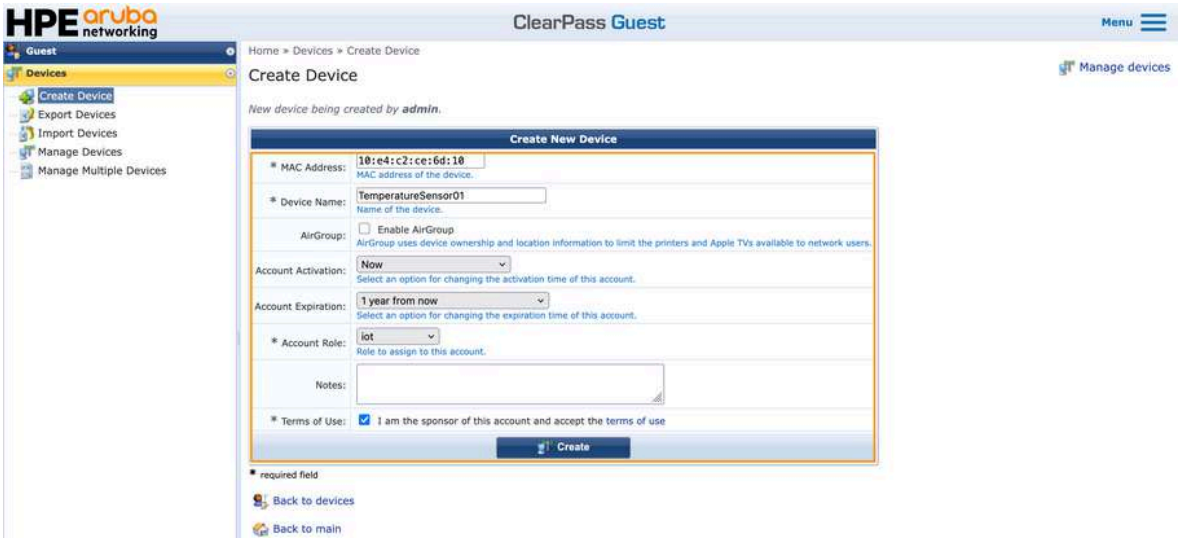

ClearPass QuickConnect
HPE aruba networking
Welcome
Configure
Connect
Summary
Onboard Wizard
Connection Summary
You have been successfully connected to the network with the following IP Address:
Wi-Fi 6 : 10.0.0.188
You can view a summary of the changes made to your system here
Licensed to:
Arubademo
HPE PRIVACY STATEMENT
Close

Network admin connecting to CWNE-Guest SSID to create unique PSK for a specific device:

For corporate users trying to onboard their personal devices, they'll connect to the guest SSID and will be redirected to the captive portal page and click the BYOD registration link to onboard their device. After authenticating using their AD credentials, users will download the onboard client that will take them through the onboarding process.

Following screenshots captures onboarding process for a user onboarding their personal devices. The actual user authentication connecting to CWNP-802.1X SSID post onboarding has been captured in the previous screenshots.



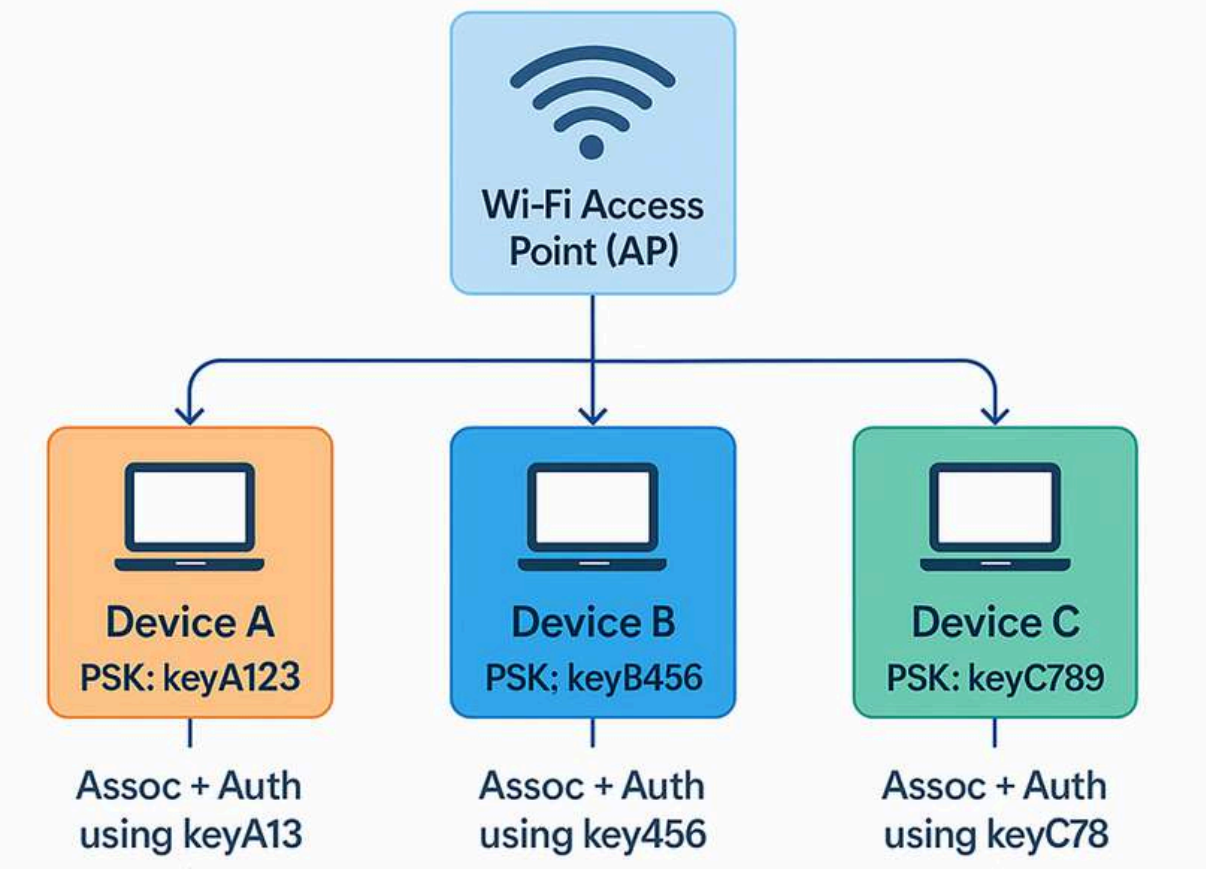


To summarize, CWNE-Guest SSID is not only allowing Guest users to connect to the network, it is also allowing corporate users to onboard their personal devices as well as allowing administrators/authorized corporate users to register their devices for a unique pre-shared key and connect to the MPSK enabled SSID.

SSID 3 - CWNE-MPSK

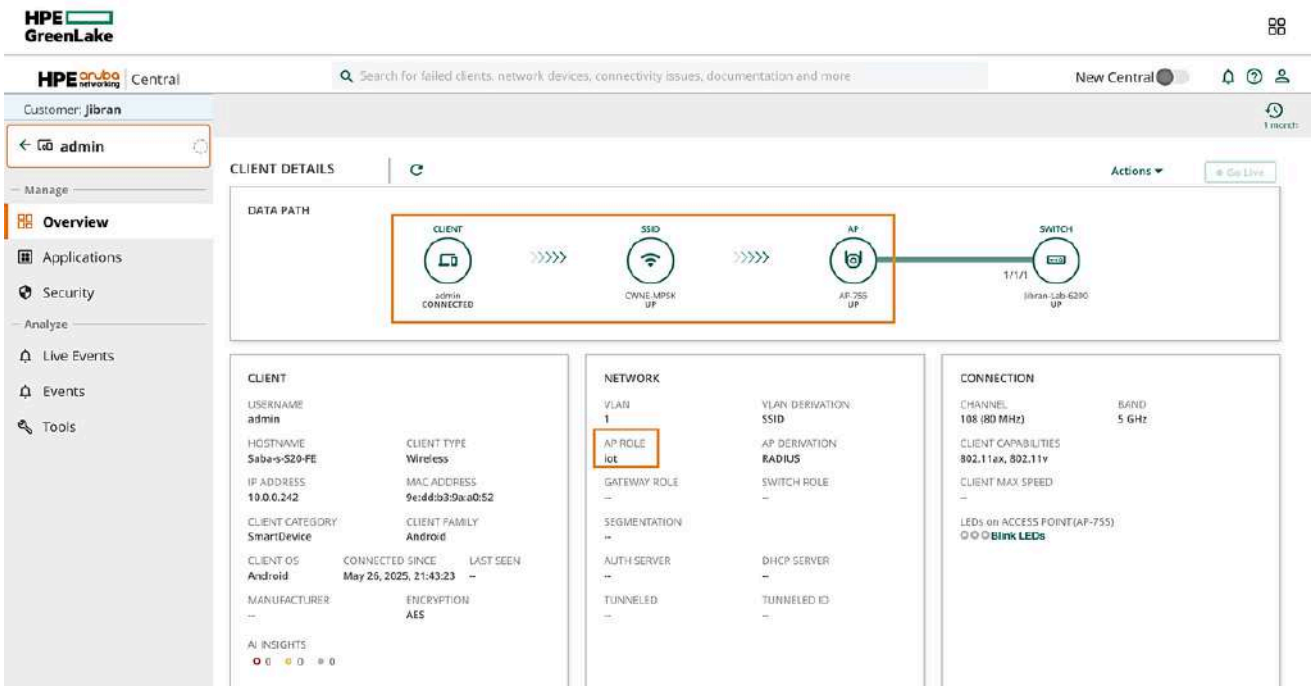
The third SSID has been configured to allow personal headless and IoT devices (that does not support 802.1X or captive portal authentication) to connect to the network using pre-shared key. The problem with traditional pre-shared key (PSK) based SSID is that all devices share the same pre-shared key and does not provide granular control for each client connected using the same pre-shared key. Using Multi-Pre-Shared Key (MPSK) allows multiple unique pre-shared keys to be used under a single SSID. This allows different devices connecting to the same SSID to be assigned different user roles or access levels.

Multi Pre-Shared Key (MPSK) Operation



Device 1 connecting to CWNE-MPSK SSID:

Following snippets shows a device assigned iot role while connecting to the CWNE-MPSK SSID. The device has connected to the network using its own pre-shared key that was generated via ClearPass portal by accessing the MPSK device registration portal while connected to the CWNE-Guest network.



Request Details

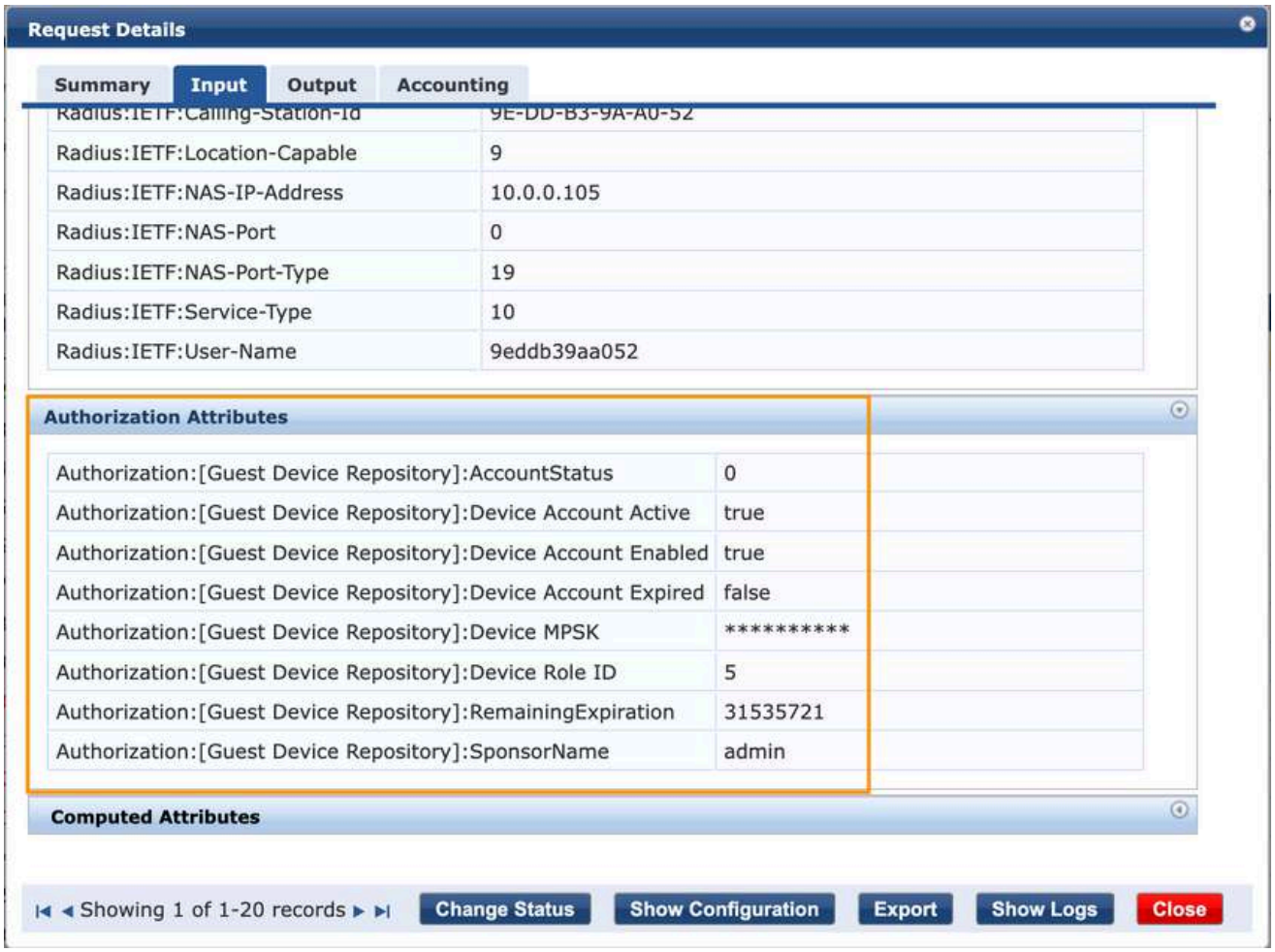
Summary | Input | Output | Accounting

Username:	admin
End-Host Identifier:	9E-DD-B3-9A-A0-52
Access Device IP (Port):	10.0.0.105
Access Device Name:	CWNE-AP (CWNE-AP / Aruba)

RADIUS Request

Radius:Aruba:Aruba-AP-Group	CWNE-Lab
Radius:Aruba:Aruba-AP-MAC-Address	988f00c1f40c
Radius:Aruba:Aruba-Device-MAC-Address	9eddb39aa052
Radius:Aruba:Aruba-Essid-Name	CWNE-MPSK
Radius:Aruba:Aruba-Location-Id	AP-755
Radius:IETF:Called-Station-Id	98-8F-00-C1-F4-0C
Radius:IETF:Calling-Station-Id	9E-DD-B3-9A-A0-52
Radius:IETF:Location-Capable	9
Radius:IETF:NAS-IP-Address	10.0.0.105
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	10
Radius:IETF:User-Name	9eddb39aa052

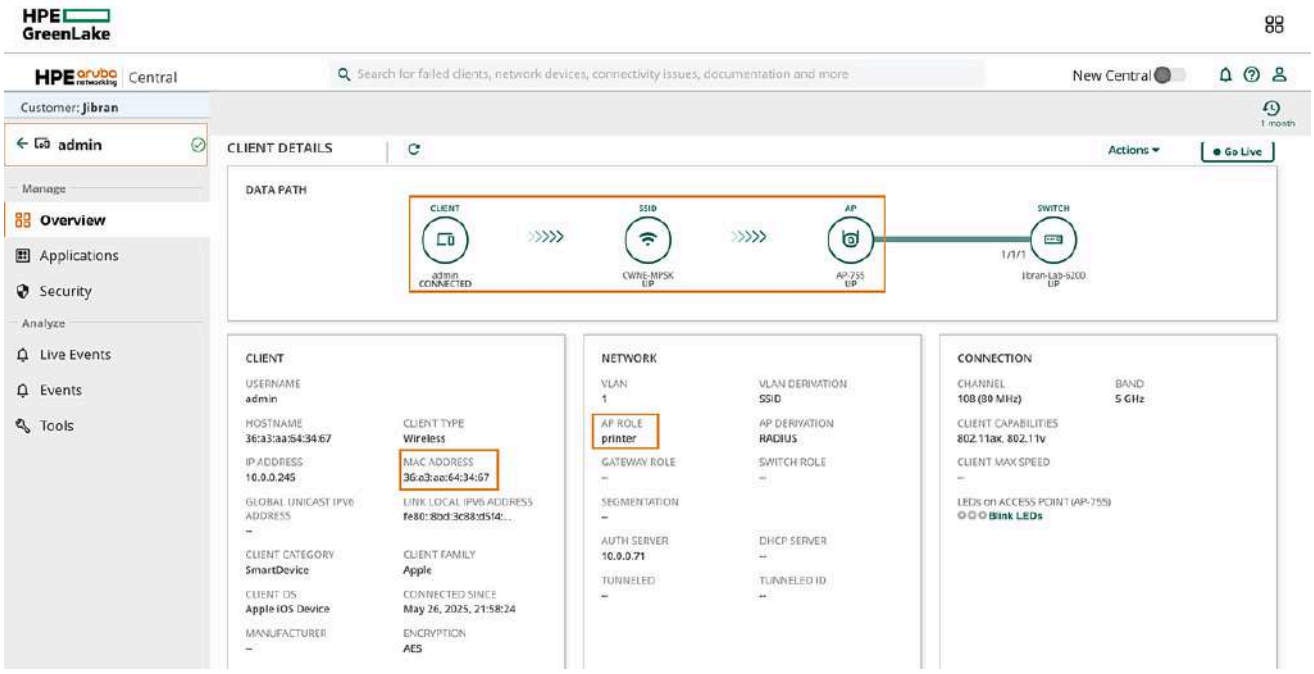
◀ Showing 1 of 1-20 records ▶ | Change Status | Show Configuration | Export | Show Logs | Close

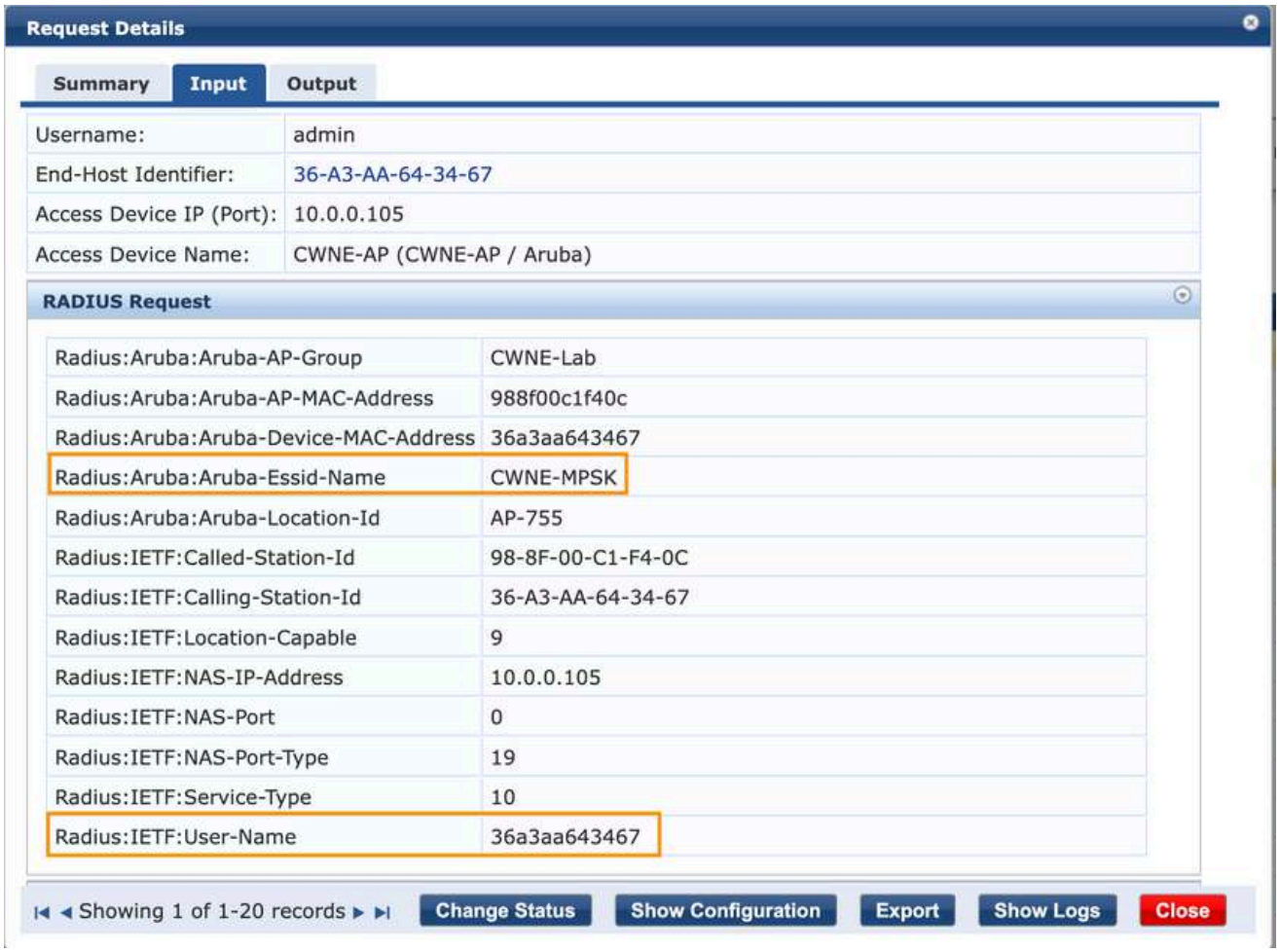

Request Details
Summary
Input
Output
Accounting
Radius:IETF:Calling-Station-Id
9E-DD-B3-9A-A0-52
Radius:IETF:Location-Capable
9
Radius:IETF:NAS-IP-Address
10.0.0.105
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Radius:IETF:Service-Type
10
Radius:IETF:User-Name
9eddb39aa052
Authorization Attributes
Authorization:[Guest Device Repository]:AccountStatus
0
Authorization:[Guest Device Repository]:Device Account Active
true
Authorization:[Guest Device Repository]:Device Account Enabled
true
Authorization:[Guest Device Repository]:Device Account Expired
false
Authorization:[Guest Device Repository]:Device MPSK
****
Authorization:[Guest Device Repository]:Device Role ID
5
Authorization:[Guest Device Repository]:RemainingExpiration
31535721
Authorization:[Guest Device Repository]:SponsorName
admin
Computed Attributes
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close

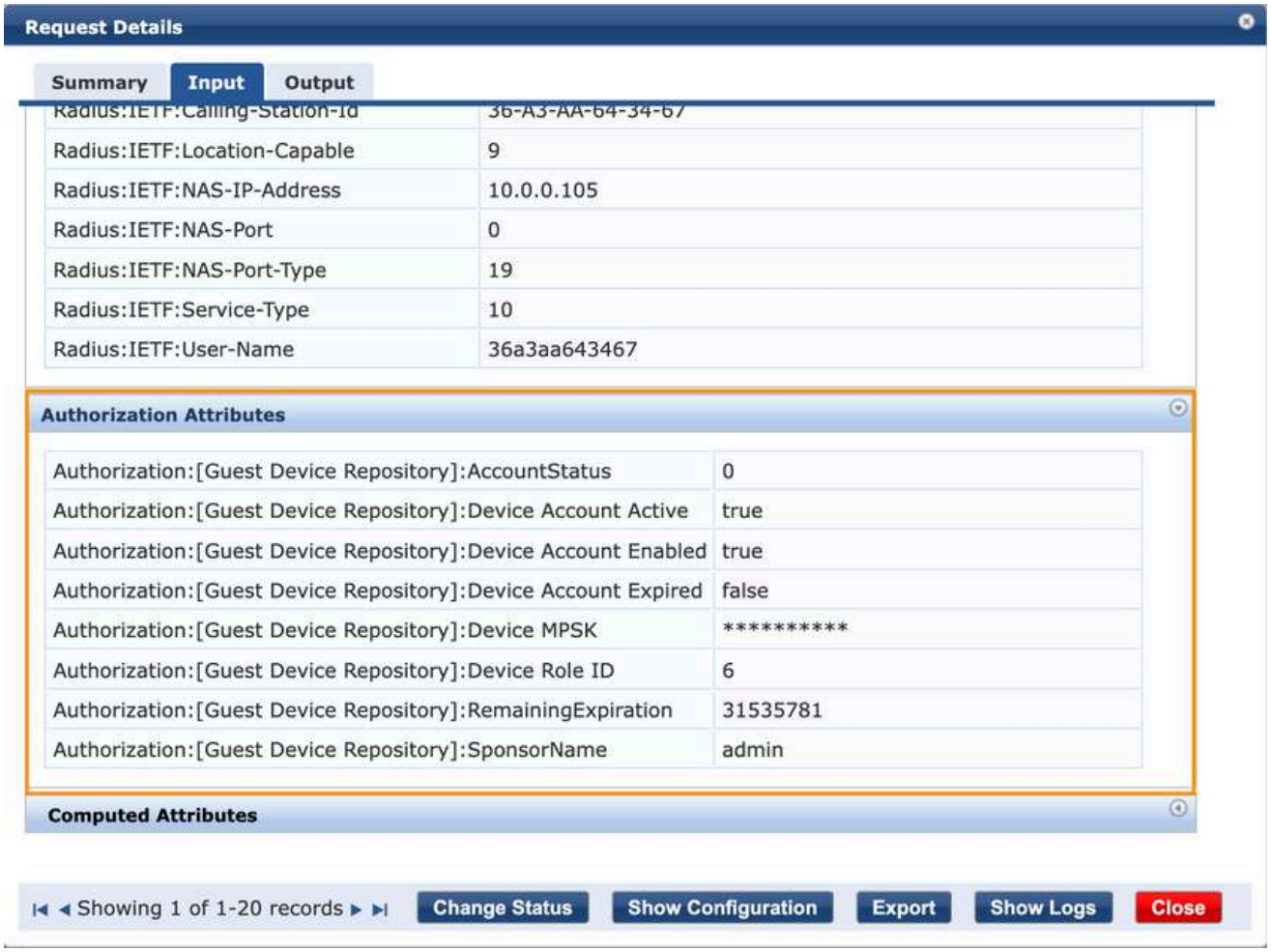

Request Details
Summary
Input
Output
Accounting
Enforcement Profiles:
[Registered Device MPSK], [Return Device Sponsor Name - RADIUS User-Name], Aruba User Role - iot
System Posture Status:
UNKNOWN (100)
Audit Posture Status:
UNKNOWN (100)
RADIUS Response
Radius:Aruba:Aruba-MPSK-Passphrase
****
Radius:Aruba:Aruba-User-Role
iot
Radius:IETF:User-Name
admin

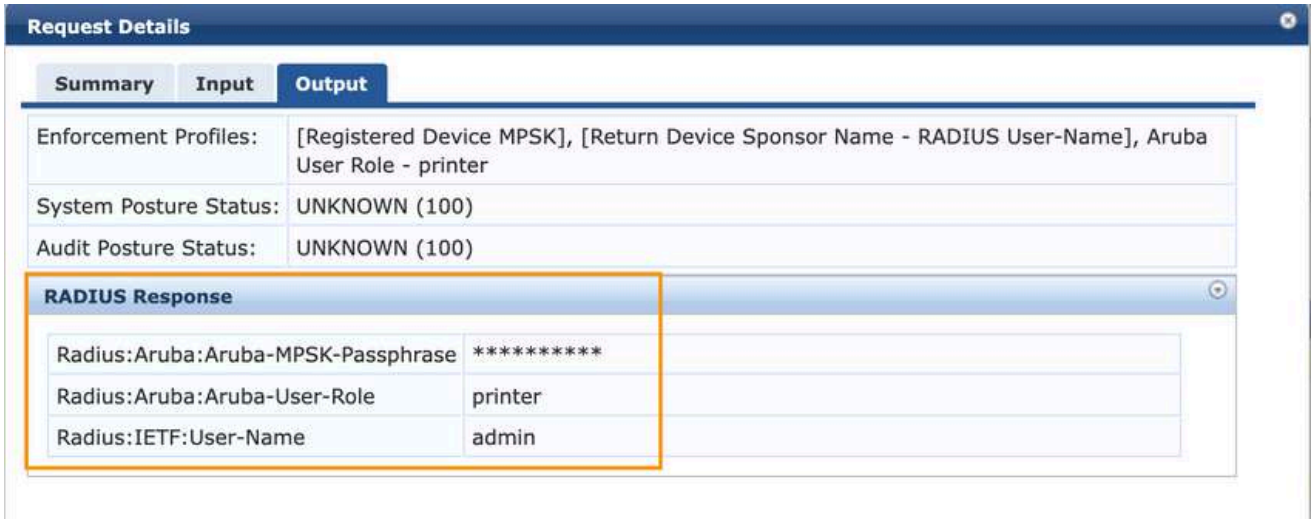
Device 2 connecting to CWNE-MPSK SSID:

Following screenshots show a device assigned printer role while connecting to the CWNE-MPSK SSID. The device has connected to the network using its own pre-shared key that was generated via ClearPass portal by accessing the MPSK device registration portal while connected to the CWNE-Guest network.




Request Details
Summary
Input
Output
Username:
admin
End-Host Identifier:
36-A3-AA-64-34-67
Access Device IP (Port):
10.0.0.105
Access Device Name:
CWNE-AP (CWNE-AP / Aruba)
RADIUS Request
Radius:Aruba:Aruba-AP-Group
CWNE-Lab
Radius:Aruba:Aruba-AP-MAC-Address
988f00c1f40c
Radius:Aruba:Aruba-Device-MAC-Address
36a3aa643467
Radius:Aruba:Aruba-Essid-Name
CWNE-MPSK
Radius:Aruba:Aruba-Location-Id
AP-755
Radius:IETF:Called-Station-Id
98-8F-00-C1-F4-0C
Radius:IETF:Calling-Station-Id
36-A3-AA-64-34-67
Radius:IETF:Location-Capable
9
Radius:IETF:NAS-IP-Address
10.0.0.105
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Radius:IETF:Service-Type
10
Radius:IETF:User-Name
36a3aa643467
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Radius:IETF:Calling-Station-Id
36-A3-AA-64-34-67
Radius:IETF:Location-Capable
9
Radius:IETF:NAS-IP-Address
10.0.0.105
Radius:IETF:NAS-Port
0
Radius:IETF:NAS-Port-Type
19
Radius:IETF:Service-Type
10
Radius:IETF:User-Name
36a3aa643467
Authorization Attributes
Authorization:[Guest Device Repository]:AccountStatus
0
Authorization:[Guest Device Repository]:Device Account Active
true
Authorization:[Guest Device Repository]:Device Account Enabled
true
Authorization:[Guest Device Repository]:Device Account Expired
false
Authorization:[Guest Device Repository]:Device MPSK
****
Authorization:[Guest Device Repository]:Device Role ID
6
Authorization:[Guest Device Repository]:RemainingExpiration
31535781
Authorization:[Guest Device Repository]:SponsorName
admin
Computed Attributes
Showing 1 of 1-20 records
Change Status
Show Configuration
Export
Show Logs
Close


Request Details
Summary
Input
Output
Enforcement Profiles:
[Registered Device MPSK], [Return Device Sponsor Name - RADIUS User-Name], Aruba User Role - printer
System Posture Status:
UNKNOWN (100)
Audit Posture Status:
UNKNOWN (100)
RADIUS Response
Radius:Aruba:Aruba-MPSK-Passphrase
****
Radius:Aruba:Aruba-User-Role
printer
Radius:IETF:User-Name
admin

To summarize, CWNE-MPSK SSID is allowing different headless and IoT devices to connect to the network using their own pre-shared key and are being assigned different user roles based on the policies configured. This allows more granular control on each device that is not possible using the traditional PSK SSIDs.

As we have seen throughout this document, effective use of NAC has helped consolidating the number of SSIDs that are required to cover typical use-cases of a typical enterprise environment without compromising the end user experience. This will result in better airtime utilization and better network performance and RF resources utilization.

References

Figure 2
SSIDs Requirement for a Typical Enterprise – AI generated image based on input to convert the provided text in to photo

Figure 3
Proposed SSIDs Consolidation– AI generated image based on input to convert the provided text in to photo

Figure 4
802.1x Authentication Roles - CloudRadius - https://www.cloudradius.com/the-stages-of-802-1x-authentication/

Figure 5
MPSK SSID in operation - AI generated image based on input provided