SonicWall and Aruba Integration Guide

Overview

This document serves as a guide for field engineering, customers and channel partners seeking to integrate ClearPass Policy Manager with SonicWall. The integration enables customers to utilize ClearPass identity tracking features for both known enterprise users from Active Directory and LDAP servers and unknown guest/public users in Guest and Hotspot networks. This integration enhances network security and management by leveraging ClearPass capabilities for user identification and access control.

Why Integrate with Aruba ClearPass?

SonicWall next-generation firewalls (NGFWs) offer context-based security for all users for safe enablement of internet access. Integrating with Aruba ClearPass offers several benefits for organizations looking to enhance network security and manage access effectively.

ClearPass helps enforce security policies by ensuring that only authorized devices and users can access the network. It provides visibility into devices connected to the network, allowing organizations to detect and respond to potential security threats.

Integrating with Aruba ClearPass allows organizations to define and enforce access policies based on user roles, device types and other contextual factors. Policies can be dynamically applied and adjusted based on changing conditions, ensuring that security measures are always aligned with the current network environment.

Aruba ClearPass can profile devices connecting to the network, identifying their type, operating system and other attributes. Posture assessment ensures that devices meet predefined security standards before being granted access, reducing the risk of compromised or non-compliant devices.

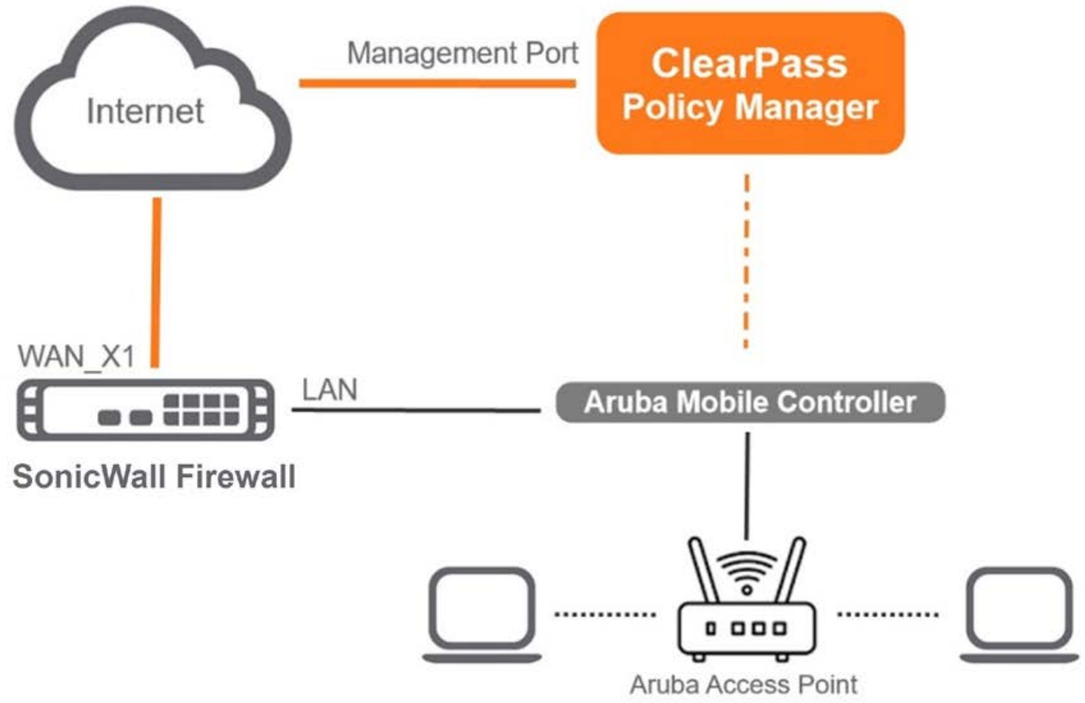
SonicWall and Aruba ClearPass Integration Overview

Aruba ClearPass provides total visibility of connected and connecting users as well as devices in wired and wireless multi-vendor environments.

SonicWall's NGFWs provide Restful Threat API which integrates with Aruba ClearPass as network access control (NAC). ClearPass can pass the security context vectors to SonicWall NGFWs using the Restful Threat API which includes Source IP, Source MAC, User ID, User Role, Domain, Device Category, Device Family, Device Name, OS Type, Hostname and Health Posture. This will enforce real-time rules based on Device Type, OS and device health posture at every point of control. When an alert is generated on a client machine, it can be shared with the SonicWall NGFW using ClearPass, which would trigger a range of predetermined, policy-based actions, from quarantine to blocking. This seamless, automated enforcement can help prevent one compromised machine from becoming a thousand.

INTEGRATION GUIDE

Topology



Software Requirements

The minimum software version required on the ClearPass policy Manager is CPPM 6.10.

The minimum SonicOS version on the SonicWall Firewall is SonicOS 7.1.1, released December 2023.

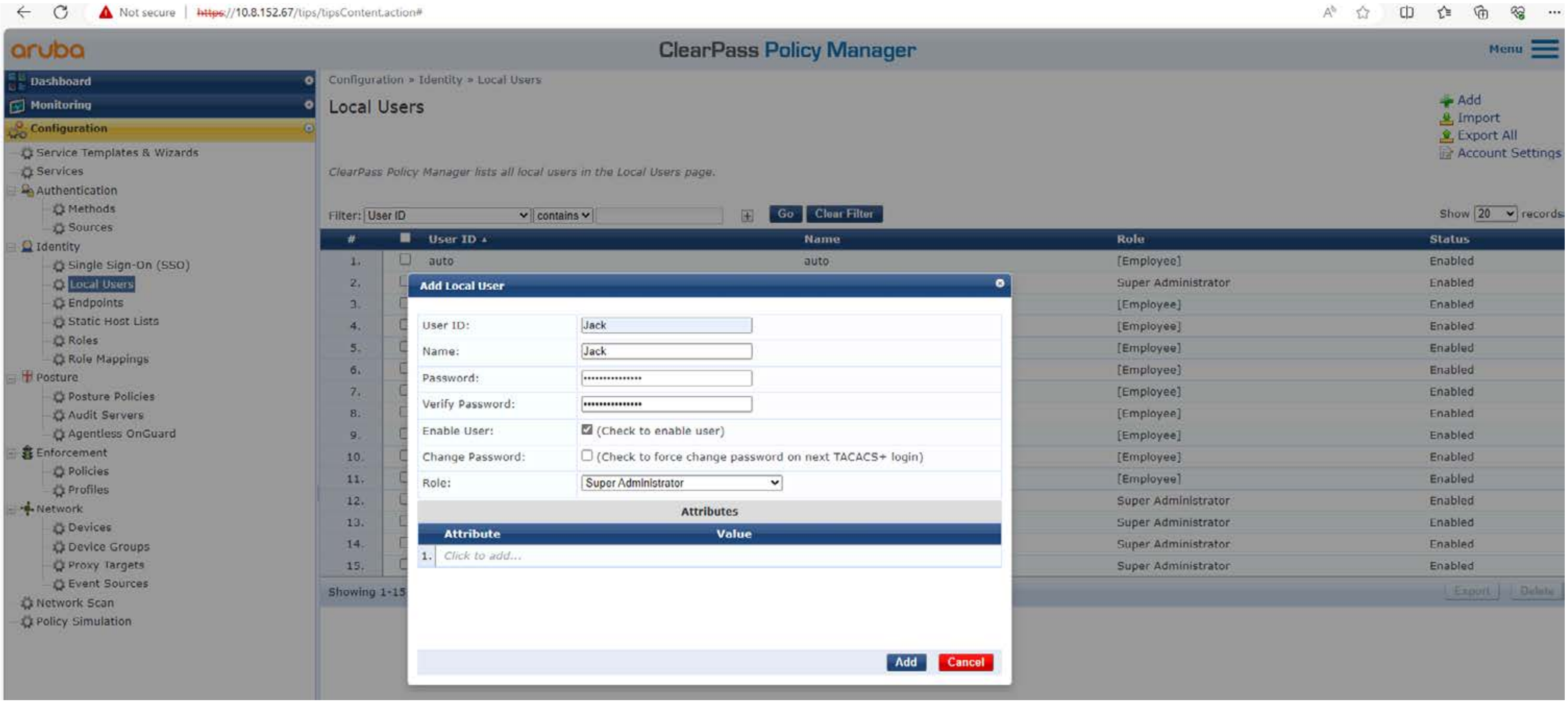
ClearPass Configuration

Configuring ClearPass Policy Manager for SonicWall integration is a simple, straightforward process. Step-by-step instructions are outlined in the following sections. The configuration has been separated into several sections.

Create a user named “Jack” to act as a test user in the CPPM portal.

Configuration > Identity > Local Users

It should appear as follows:



Configuration » Identity » Local Users

Local Users

ClearPass Policy Manager lists all local users in the Local Users page.

Filter: User ID contains

Show 20 records

#	User ID ▴	Name	Role	Status
1.	auto	auto	[Employee]	Enabled
2.			Super Administrator	Enabled
3.			[Employee]	Enabled
4.			[Employee]	Enabled
5.			[Employee]	Enabled
6.			[Employee]	Enabled
7.			[Employee]	Enabled
8.			[Employee]	Enabled
9.			[Employee]	Enabled
10.			[Employee]	Enabled
11.			[Employee]	Enabled
12.			Super Administrator	Enabled
13.			Super Administrator	Enabled
14.			Super Administrator	Enabled
15.			Super Administrator	Enabled

Showing 1-15

Add Local User

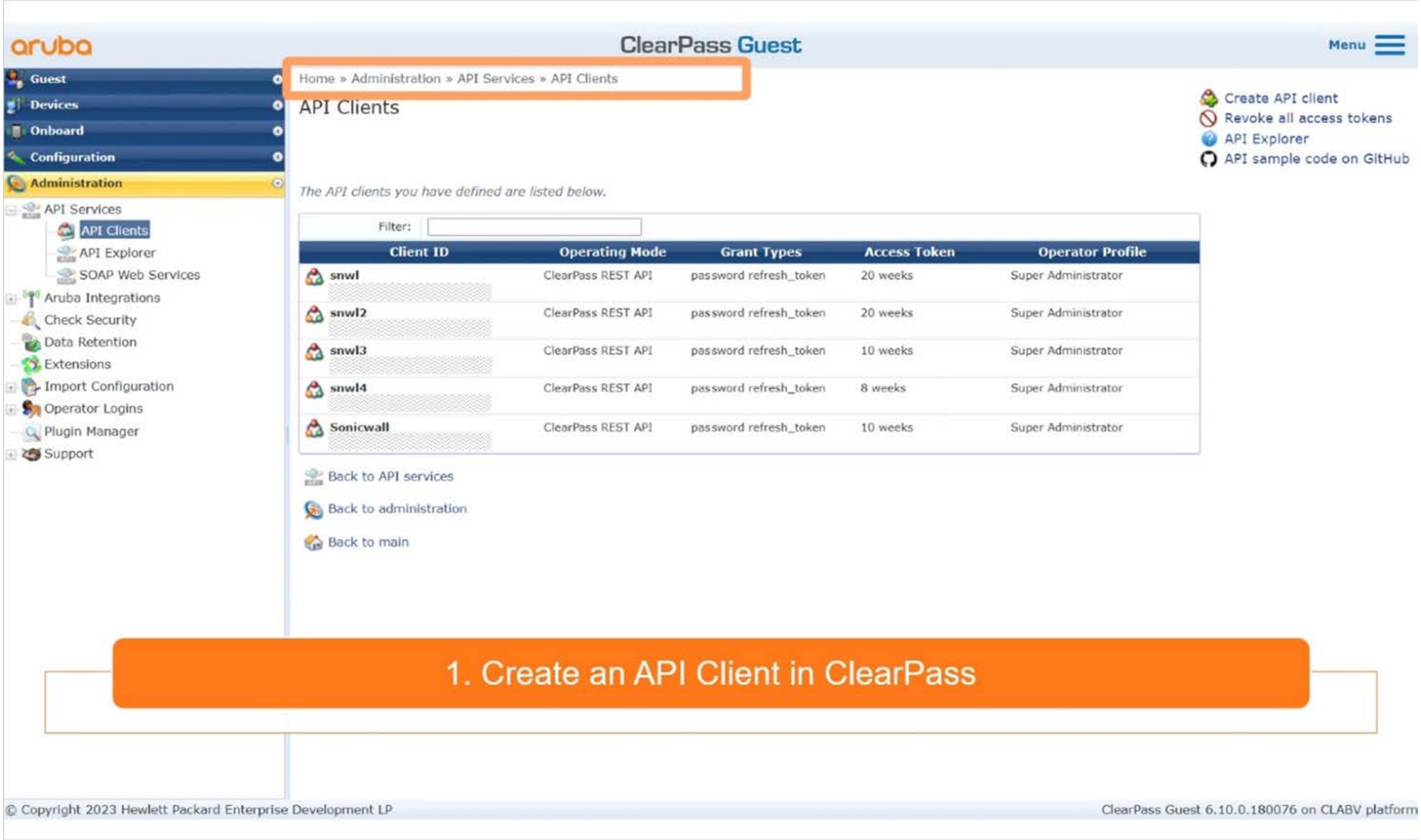
User ID:	Jack
Name:	Jack
Password:	•••••••••••••••
Verify Password:	•••••••••••••••
Enable User:	☑ (Check to enable user)
Change Password:	□ (Check to force change password on next TACACS+ login)
Role:	Super Administrator

Attributes

	Attribute	Value
1.	*Click to add...*	

Add Cancel

Now, we are logged into ClearPass as a guest user. First, we will create an API Client in ClearPass. The **Administration > API Services > API Clients** page is displayed on the screen. Click **Create Client** on the top-right corner of the screen.



API Clients

The API clients you have defined are listed below.

Client ID	Operating Mode	Grant Types	Access Token	Operator Profile
snwl [redacted]	ClearPass REST API	password refresh_token	20 weeks	Super Administrator
snwl2 [redacted]	ClearPass REST API	password refresh_token	20 weeks	Super Administrator
snwl3 [redacted]	ClearPass REST API	password refresh_token	10 weeks	Super Administrator
snwl4 [redacted]	ClearPass REST API	password refresh_token	8 weeks	Super Administrator
Sonicwall [redacted]	ClearPass REST API	password refresh_token	10 weeks	Super Administrator

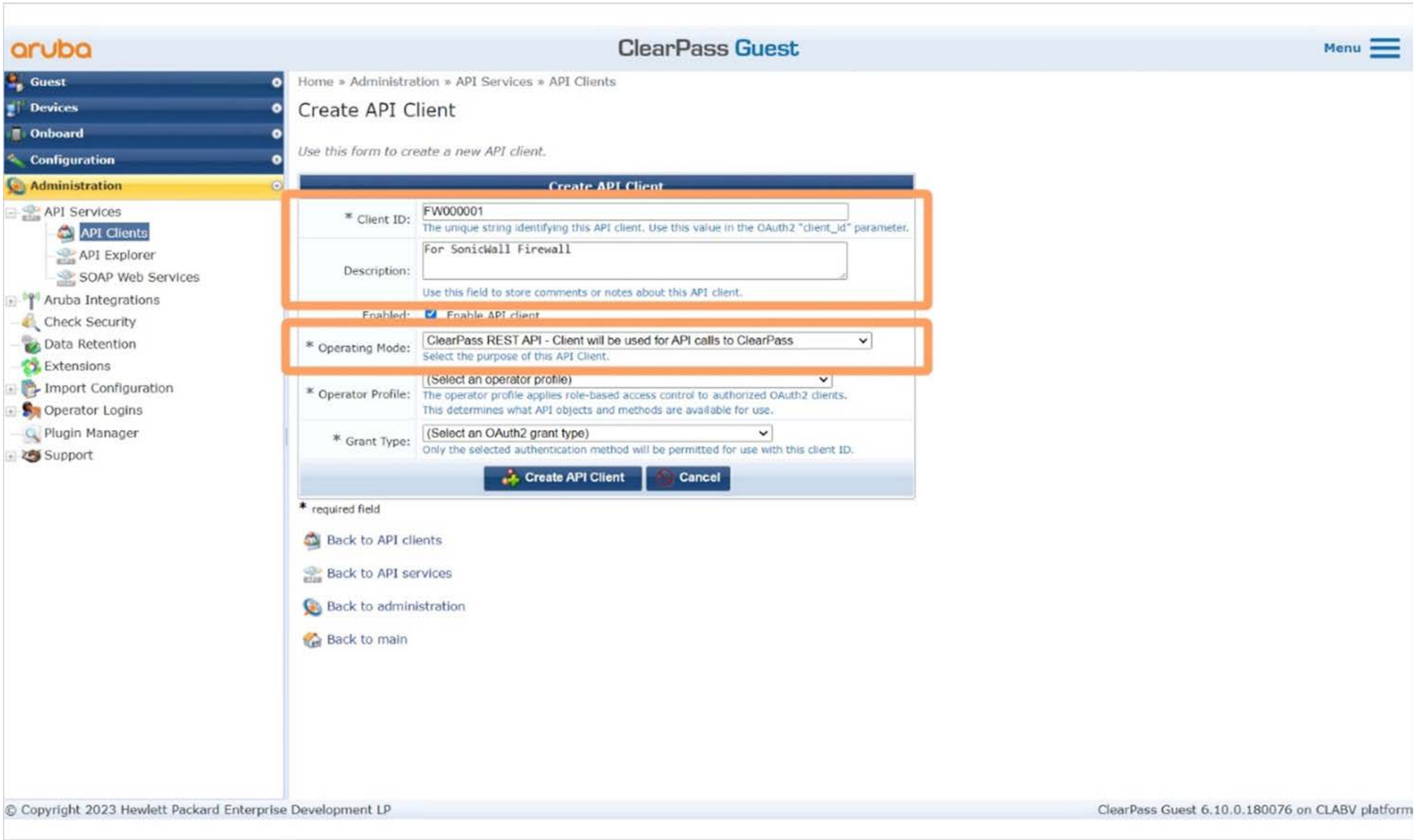
1. Create an API Client in ClearPass

© Copyright 2023 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.10.0.180076 on CLABV platform

The **Create API Client** page displays.

A sample **Client ID** and **Description** have been entered. We will retain the original selection **ClearPass REST API** option for the **Operating Mode**. Next, click the option **Operator Profile**.



Home » Administration » API Services » API Clients

Create API Client

Use this form to create a new API client.

Create API Client

* Client ID: FW000001
The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.

Description: For SonicWall Firewall
Use this field to store comments or notes about this API client.

Enabled: ☑ Enable API client

* Operating Mode: ClearPass REST API - Client will be used for API calls to ClearPass
Select the purpose of this API Client.

* Operator Profile: (Select an operator profile)
The operator profile applies role-based access control to authorized OAuth2 clients.
This determines what API objects and methods are available for use.

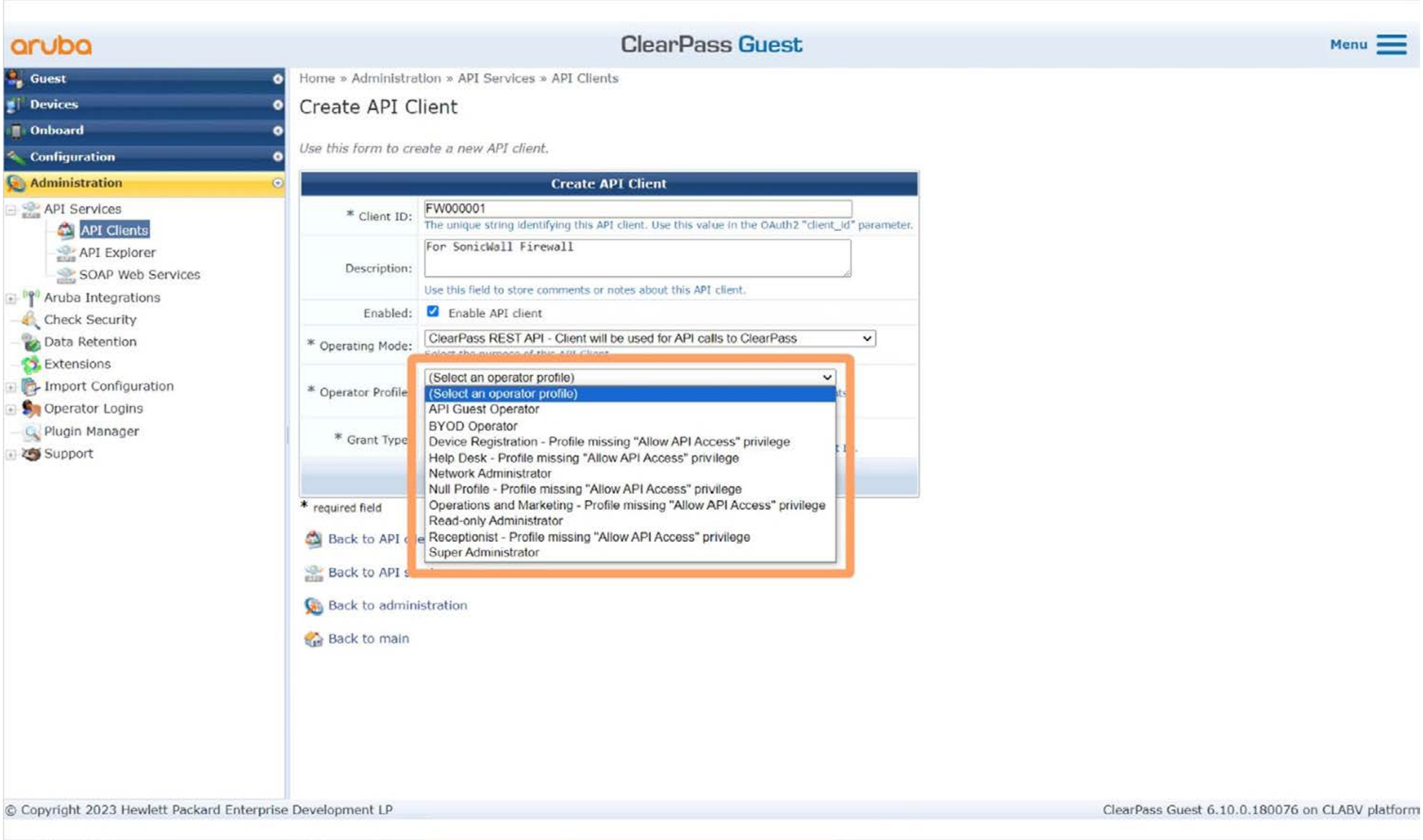
* Grant Type: (Select an OAuth2 grant type)
Only the selected authentication method will be permitted for use with this client ID.

* required field

© Copyright 2023 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.10.0.180076 on CLABV platform

All the existing profiles are listed. In this example, we will select a profile that has the highest authority. In the drop-down list, click **Super Administrator**.



Create API Client

Use this form to create a new API client.

Create API Client

* Client ID: FW000001
The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.

Description: For SonicWall Firewall
Use this field to store comments or notes about this API client.

Enabled: ☑ Enable API client

* Operating Mode: ClearPass REST API - Client will be used for API calls to ClearPass

* Operator Profile: (Select an operator profile)

- (Select an operator profile)
- API Guest Operator
- BYOD Operator
- Device Registration - Profile missing "Allow API Access" privilege
- Help Desk - Profile missing "Allow API Access" privilege
- Network Administrator
- Null Profile - Profile missing "Allow API Access" privilege
- Operations and Marketing - Profile missing "Allow API Access" privilege
- Read-only Administrator
- Receptionist - Profile missing "Allow API Access" privilege
- Super Administrator

* Grant Type

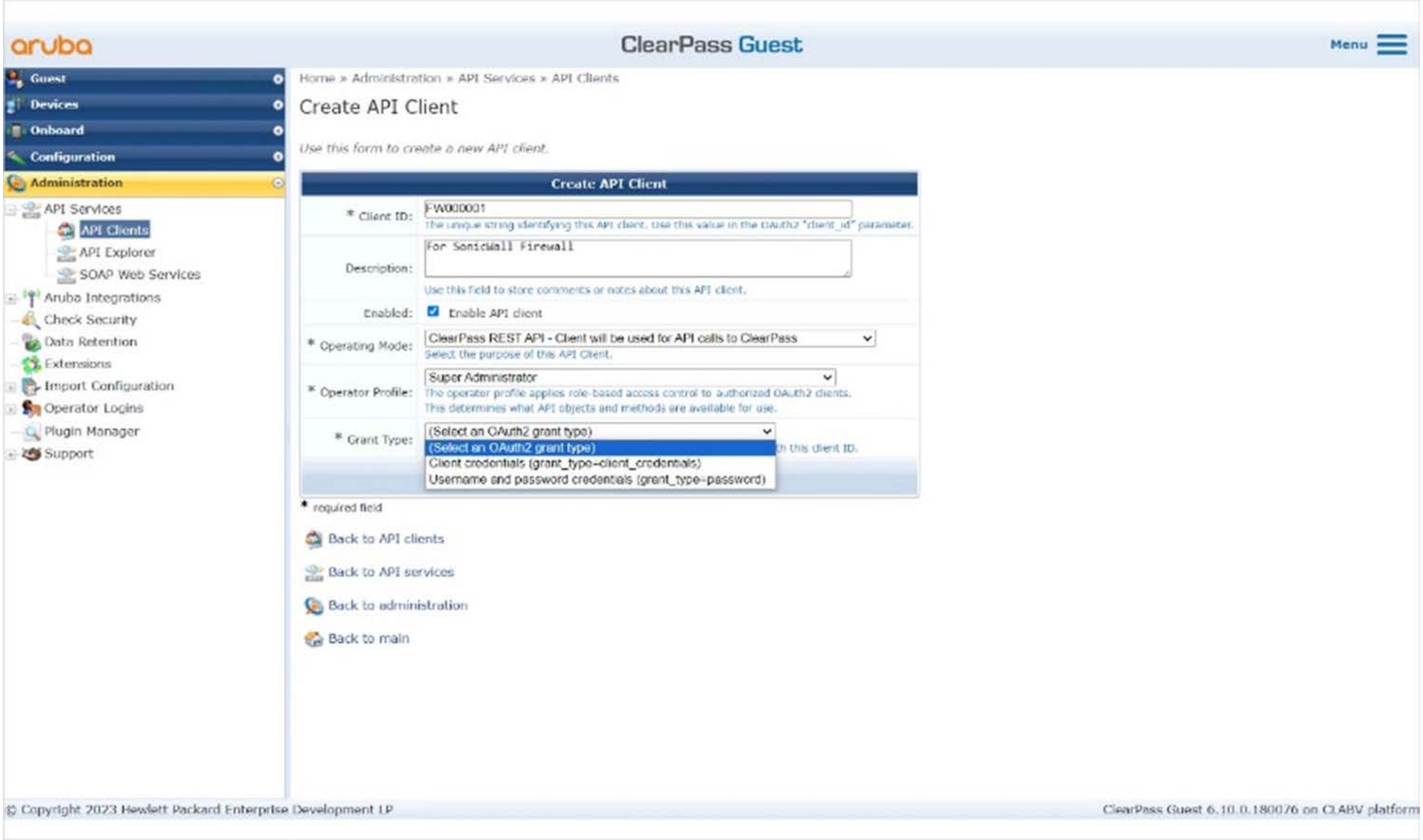
* required field

© Copyright 2023 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.10.0.180076 on CLABV platform

Next, click the option **Grant Type**.

To enable connection between the SonicWall NGFW and ClearPass, select **Username and password credentials** from the list.



Home » Administration » API Services » API Clients

Create API Client

Use this form to create a new API client.

Create API Client

* Client ID:	FW000001 The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.
Description:	For SonicWall Firewall Use this field to store comments or notes about this API client.
Enabled:	☑ Enable API client
* Operating Mode:	ClearPass REST API - Client will be used for API calls to ClearPass Select the purpose of this API Client.
* Operator Profile:	Super Administrator The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.
* Grant Type:	(Select an OAuth2 grant type) (Select an OAuth2 grant type) Client credentials (grant_type=client_credentials) Username and password credentials (grant_type=password) ...h this client ID.

* required field

Back to API clients

Back to API services

Back to administration

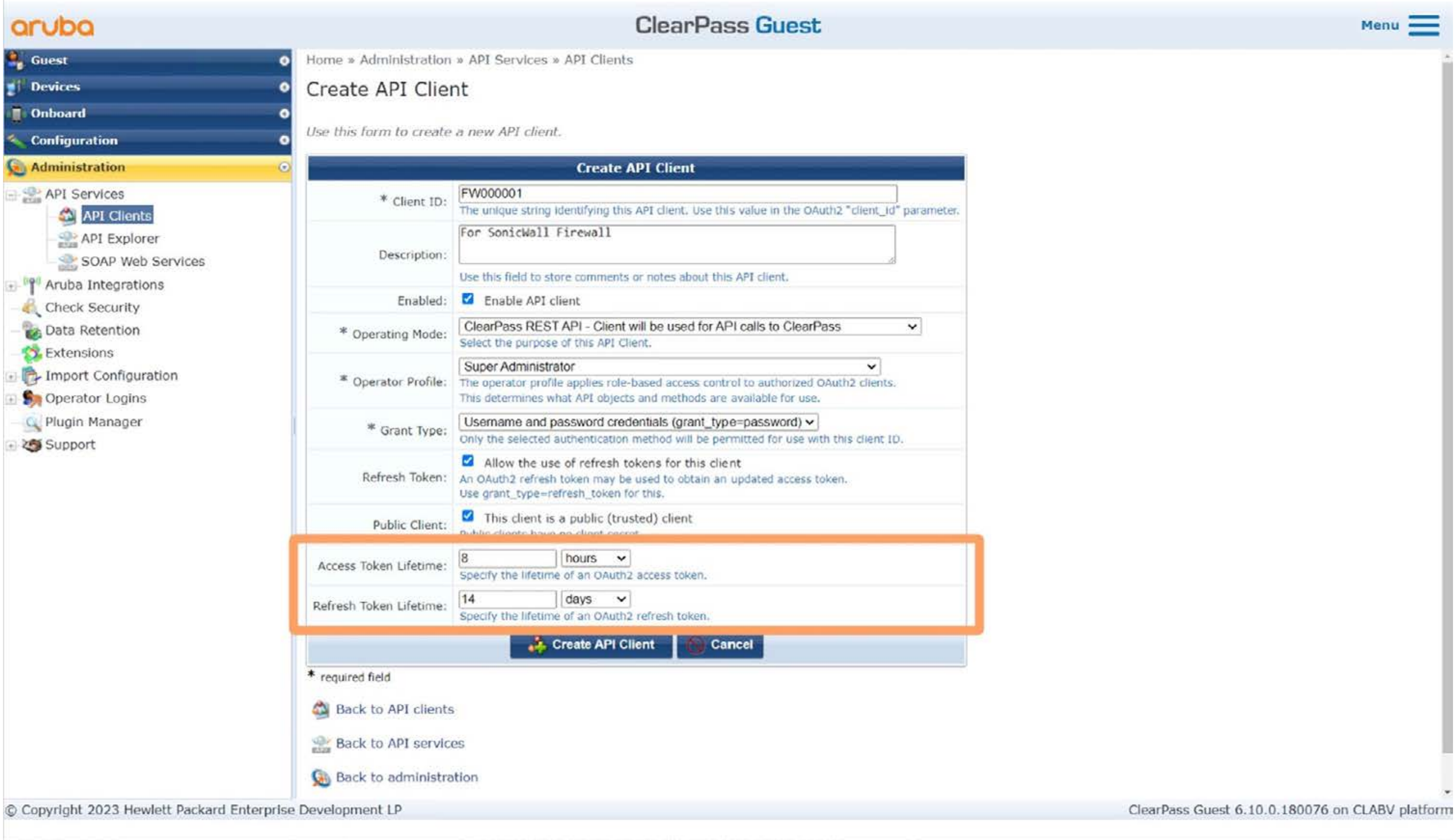
Back to main

© Copyright 2023 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.10.0.180076 on CLABV platform

In the **Public Client** area, select the check box for the option **This client is a public (trusted) client**.

Next, you can update the **Access Token Lifetime** and **Refresh Token Lifetime** according to your organization's requirements.



Home » Administration » API Services » API Clients

Create API Client

Use this form to create a new API client.

Create API Client

* Client ID:	FW000001 The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.
Description:	For SonicWall Firewall Use this field to store comments or notes about this API client.
Enabled:	☑ Enable API client
* Operating Mode:	ClearPass REST API - Client will be used for API calls to ClearPass Select the purpose of this API Client.
* Operator Profile:	Super Administrator The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.
* Grant Type:	Username and password credentials (grant_type=password) Only the selected authentication method will be permitted for use with this client ID.
Refresh Token:	☑ Allow the use of refresh tokens for this client An OAuth2 refresh token may be used to obtain an updated access token. Use grant_type=refresh_token for this.
Public Client:	☑ This client is a public (trusted) client Public clients have no client secret.
Access Token Lifetime:	8 hours Specify the lifetime of an OAuth2 access token.
Refresh Token Lifetime:	14 days Specify the lifetime of an OAuth2 refresh token.

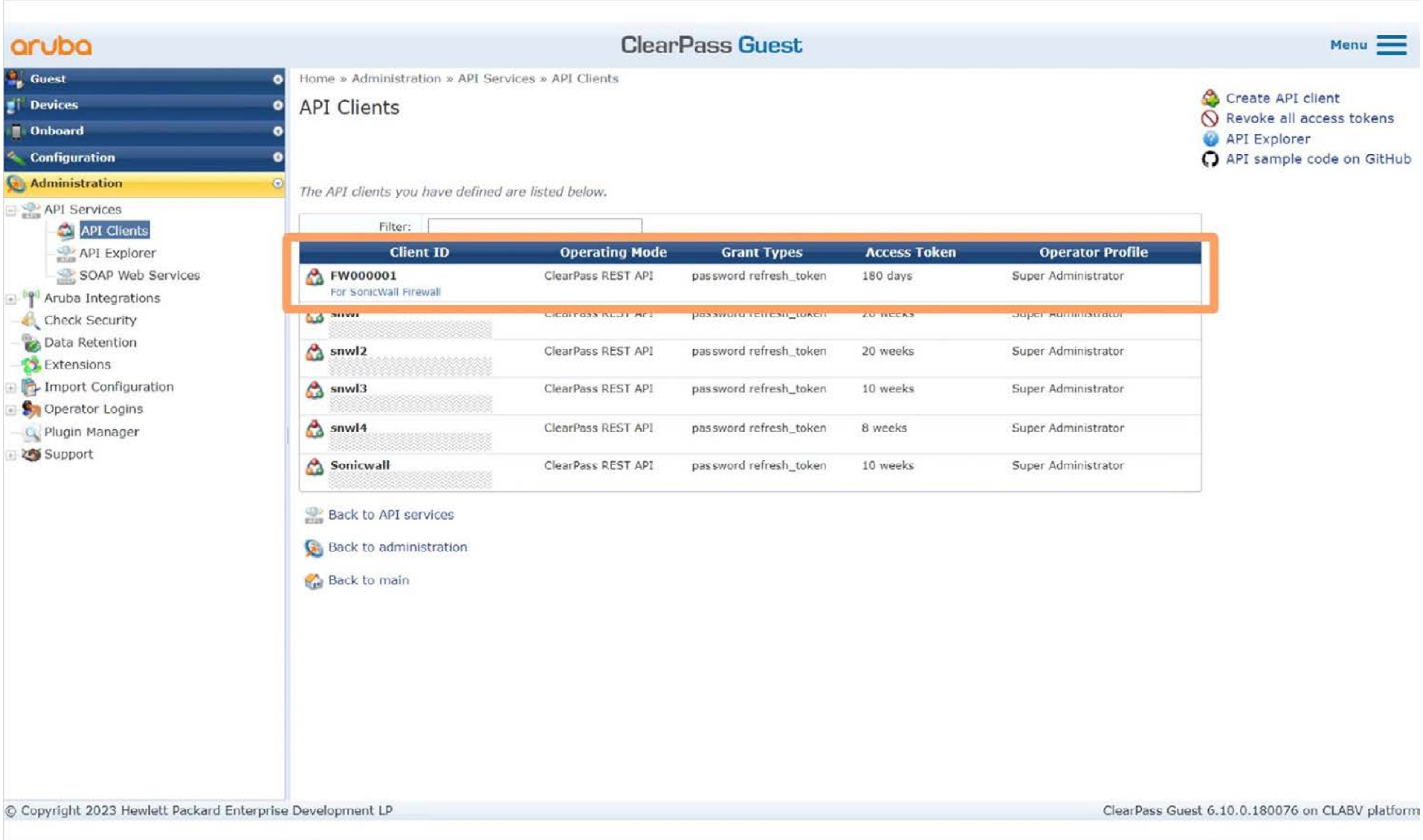
* required field

© Copyright 2023 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.10.0.180076 on CLABV platform

Sample selections have been made for the context of this example. To submit the API Client settings, click the button **Create API Client**.

The API Client for the SonicWall NGFW has been successfully created. Note that a user with the **Super Administrator** profile is required to enable communication between the NGFW and ClearPass.



API Clients

The API clients you have defined are listed below.

Client ID	Operating Mode	Grant Types	Access Token	Operator Profile
FW000001 For SonicWall Firewall	ClearPass REST API	password refresh_token	180 days	Super Administrator
snwl [redacted]	ClearPass REST API	password refresh_token	20 weeks	Super Administrator
snwl2 [redacted]	ClearPass REST API	password refresh_token	20 weeks	Super Administrator
snwl3 [redacted]	ClearPass REST API	password refresh_token	10 weeks	Super Administrator
snwl4 [redacted]	ClearPass REST API	password refresh_token	8 weeks	Super Administrator
Sonicwall [redacted]	ClearPass REST API	password refresh_token	10 weeks	Super Administrator

© Copyright 2023 Hewlett Packard Enterprise Development LP

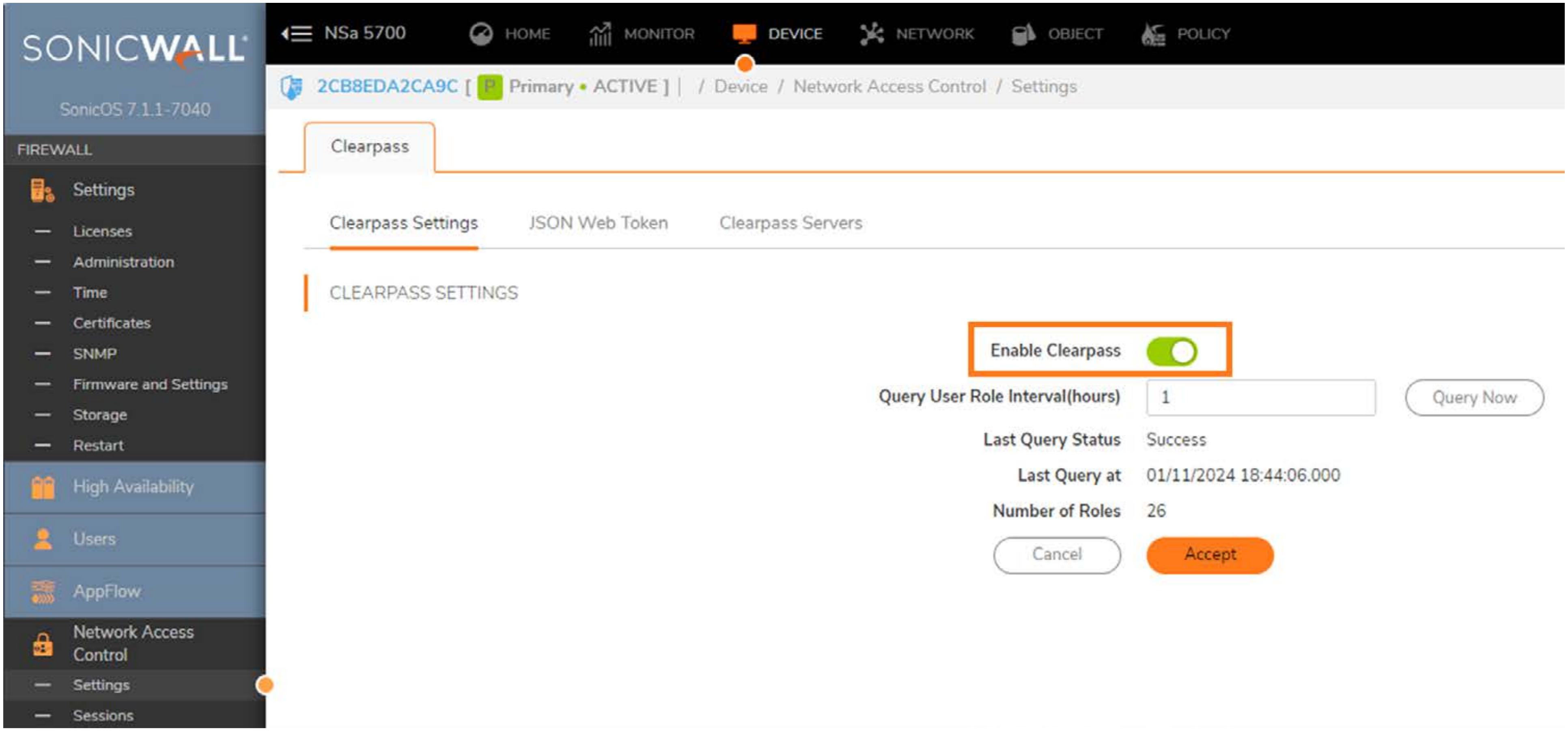
ClearPass Guest 6.10.0.180076 on CLABV platform

Configuring the SonicWall NGFW

SonicOS provides Restful Threat API which supports Aruba ClearPass as NAC to integrate with SonicWall NGFWs. ClearPass can pass security context vectors including Source-IP, Source-MAC, User-ID, User-Role, Domain, Device-Category, Device-Family, Device-Name, OS-Type, Hostname and Health-Posture to SonicWall NGFWs to build policies for mitigation actions.

Enabling NAC on the NGFW

Login to the Firewall, browse to **Device > Network Access Control > Settings**.



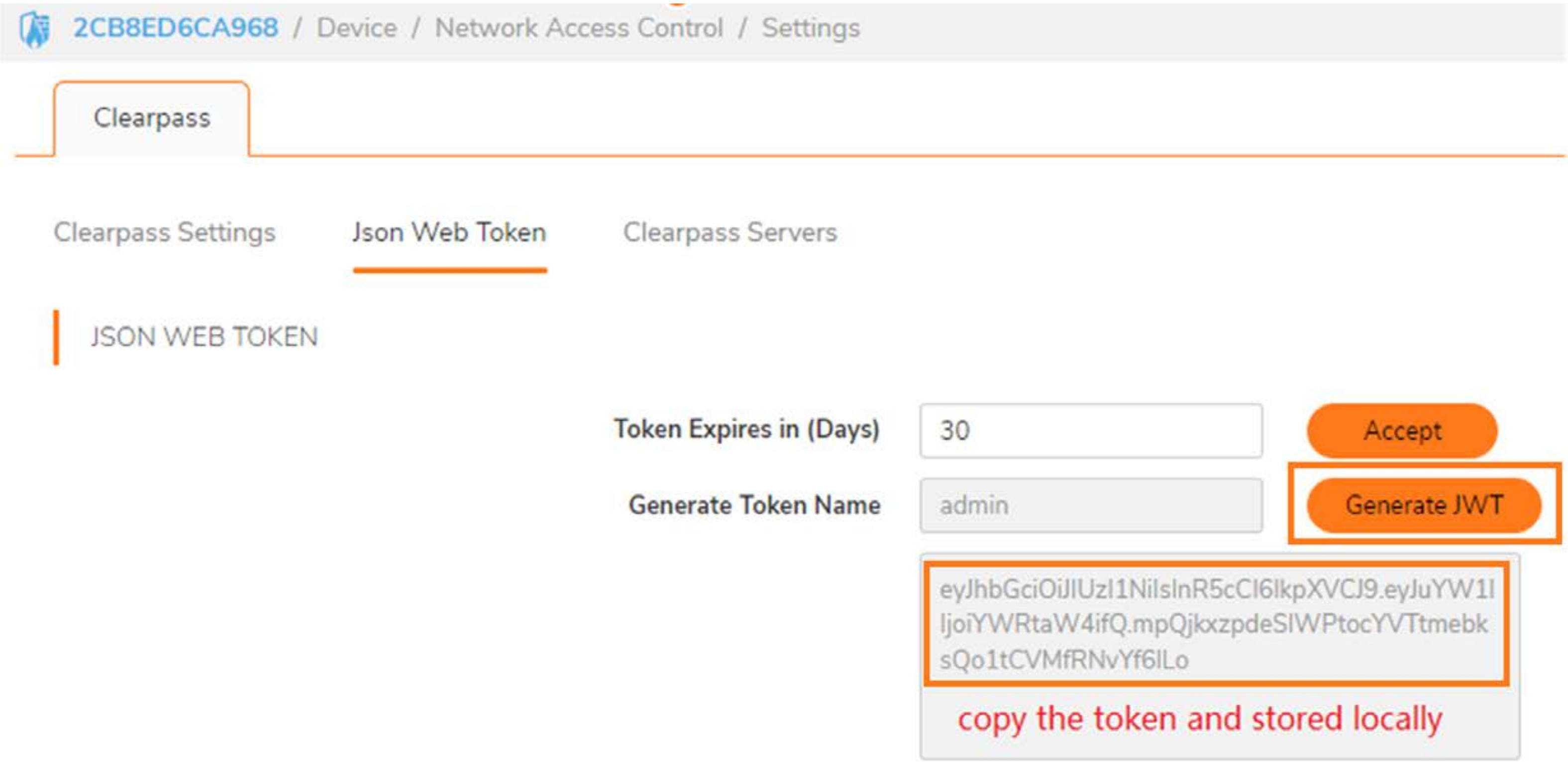
CLEARPASS SETTINGS

Enable Clearpass	●
Query User Role Interval(hours)	1
Last Query Status	Success
Last Query at	01/11/2024 18:44:06.000
Number of Roles	26

Generate a JSON Token on the NGFW and apply this token into Aruba ClearPass Policy Manager (CPPM).

Navigate to the JSON Web Token and Click on **Generate JWT**.

Copy the token.



Token Expires in (Days) 30

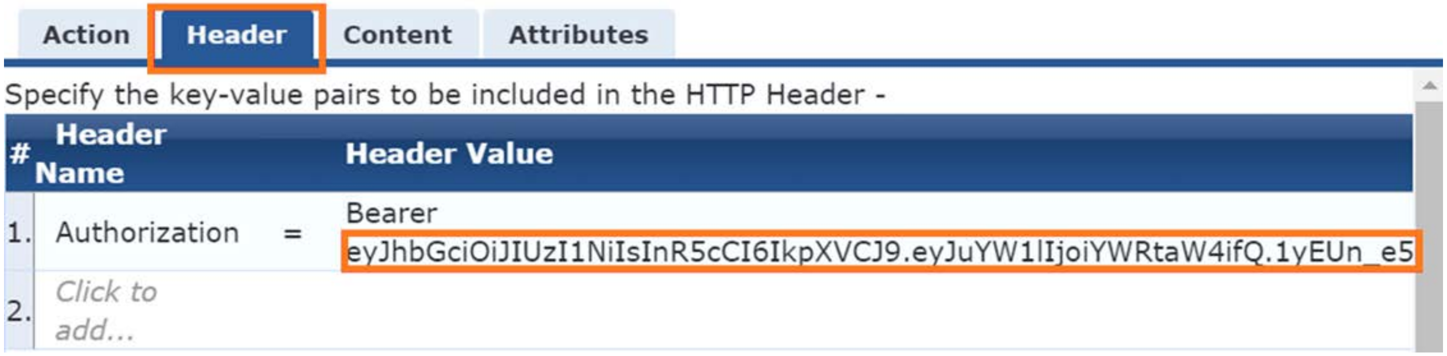
Generate Token Name admin

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1l
IjoiYWRtaW4ifQ.mpQjkxzpdeSIWPtocYVTtmebk
sQo1tCVMfRNvYf6ILo

copy the token and stored locally

Apply this token into Aruba CPPM:

Navigate to **Administration > Dictionaries > Context Server Actions**, edit and replace the token with the newly generated one here.

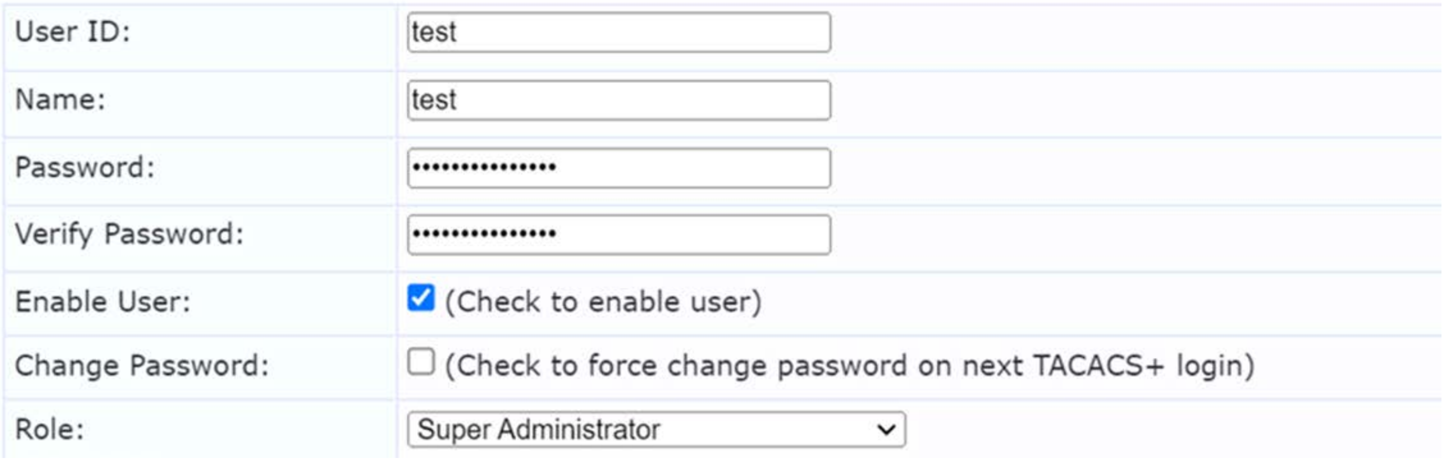


Specify the key-value pairs to be included in the HTTP Header -

#	Header Name		Header Value
1.	Authorization	=	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoiYWRtaW4ifQ.1yEUn_e5
2.	*Click to add...*		

Creating Local Users on CPPM

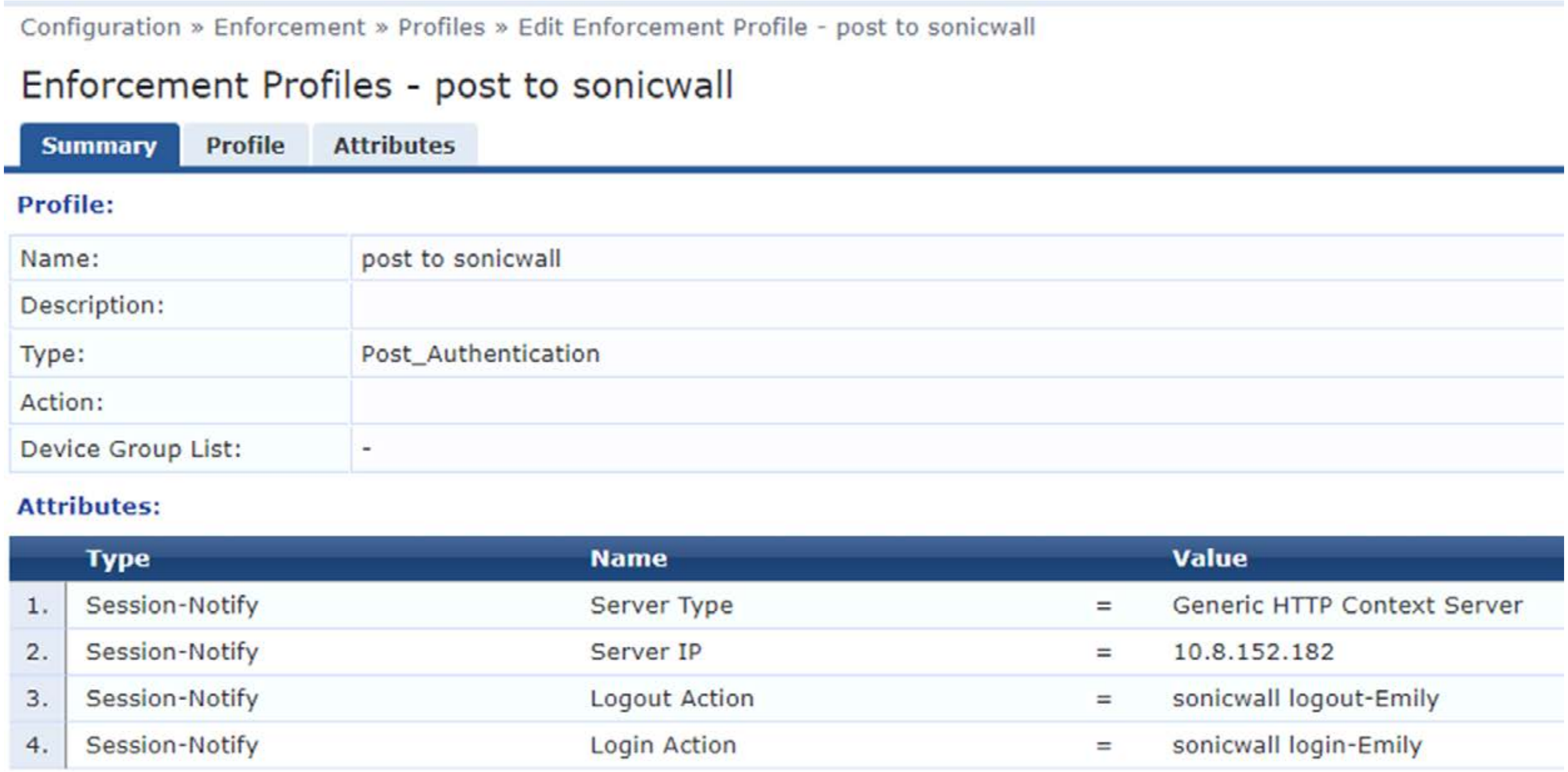
Navigate to Configuration > Identity > Local Users, create a Super Administrator with the username “xxx” and password “xxx” for SonicWall, example below:



User ID:	test
Name:	test
Password:	•••••••••••••••
Verify Password:	•••••••••••••••
Enable User:	☑ (Check to enable user)
Change Password:	□ (Check to force change password on next TACACS+ login)
Role:	Super Administrator

Creating Profiles on CPPM

Navigate to **Configuration > Enforcement > Profiles** and add an **Enforcement Profile** as shown below:



Configuration » Enforcement » Profiles » Edit Enforcement Profile - post to sonicwall

Enforcement Profiles - post to sonicwall

Profile:

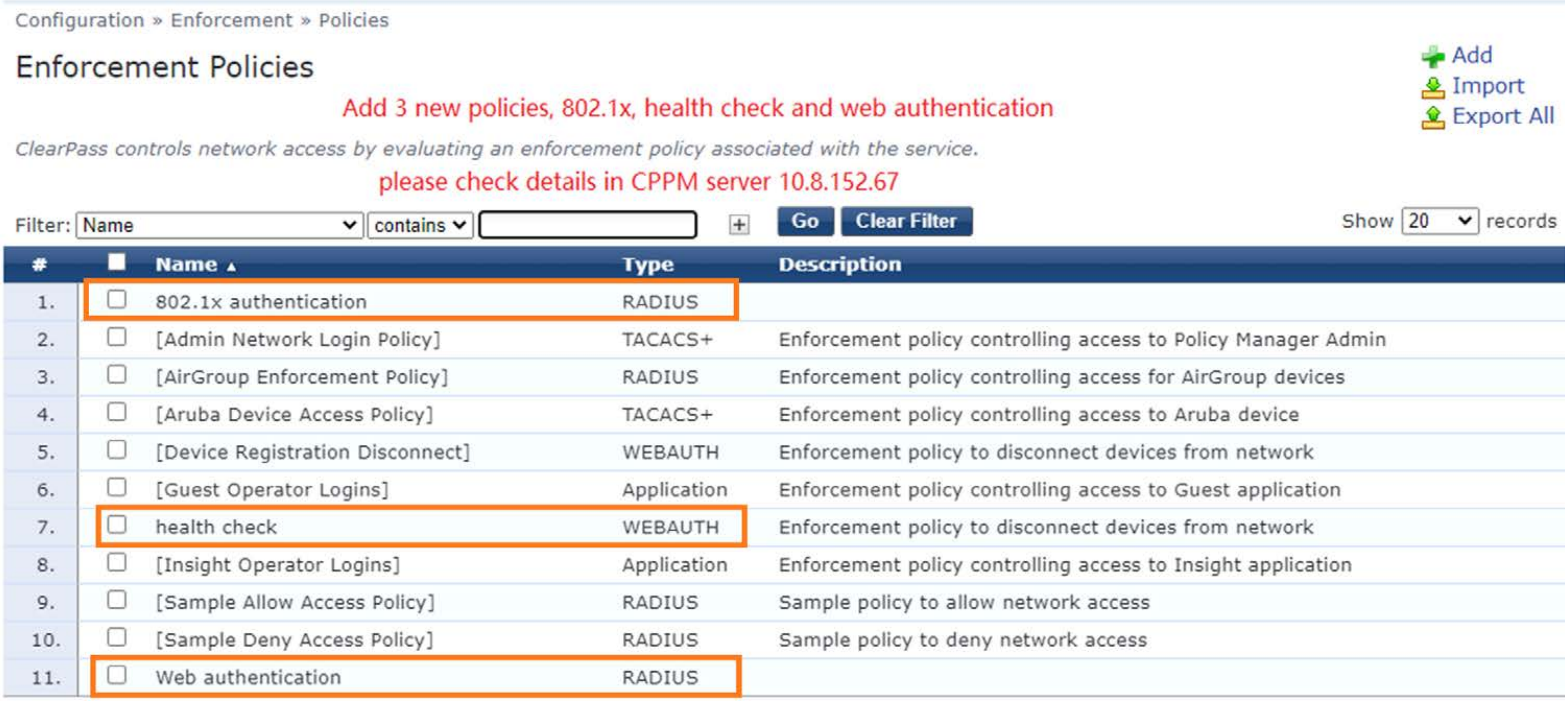
Name:	post to sonicwall
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Session-Notify	Server Type	=	Generic HTTP Context Server
2.	Session-Notify	Server IP	=	10.8.152.182
3.	Session-Notify	Logout Action	=	sonicwall logout-Emily
4.	Session-Notify	Login Action	=	sonicwall login-Emily

Creating Policies on CPPM

Navigate to Configuration > Enforcement > Policies, add Enforcement Policies as shown below:



Configuration » Enforcement » Policies

Enforcement Policies

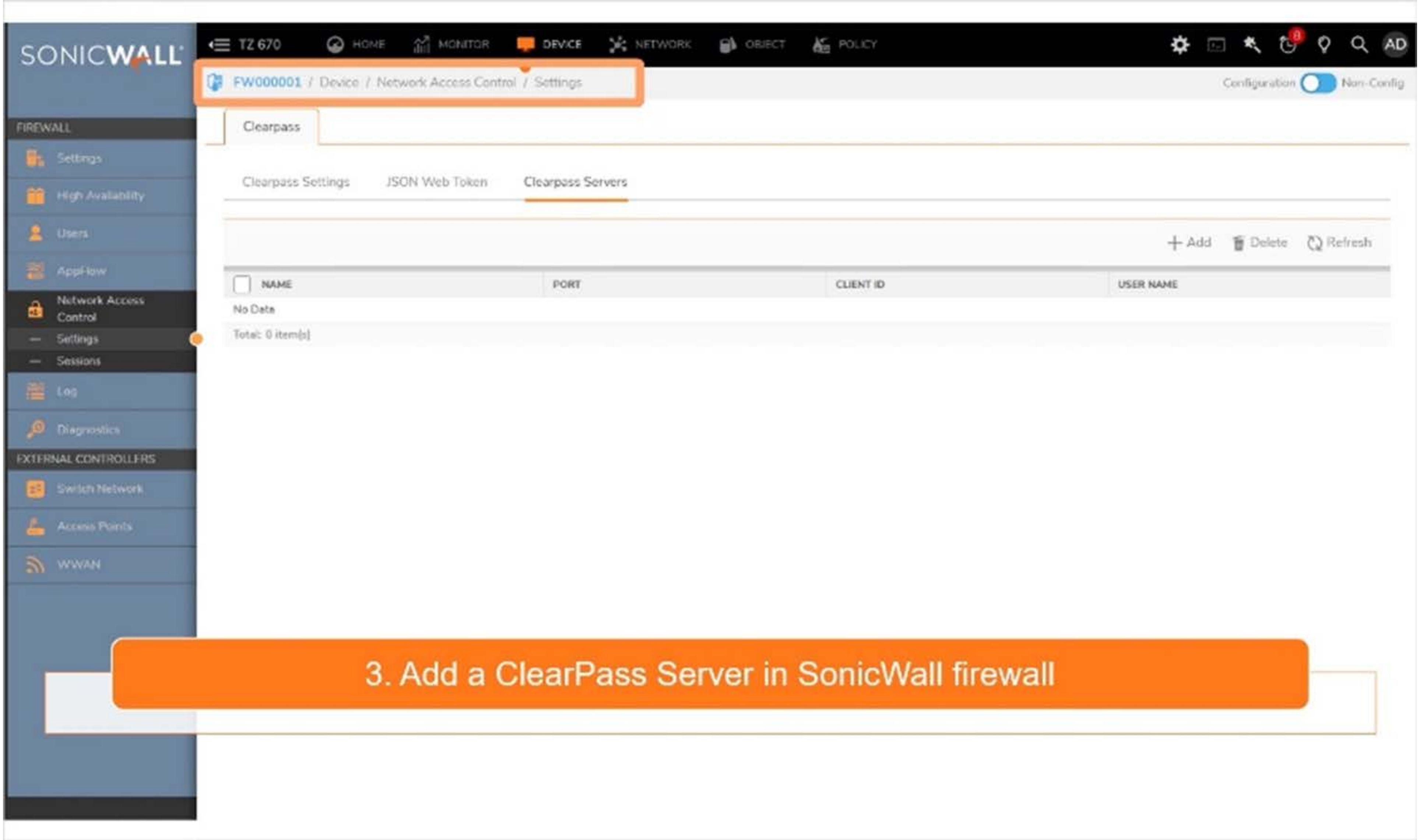
Add 3 new policies, 802.1x, health check and web authentication

ClearPass controls network access by evaluating an enforcement policy associated with the service.

please check details in CPPM server 10.8.152.67

#	□	Name ▲	Type	Description
1.	□	802.1x authentication	RADIUS	
2.	□	[Admin Network Login Policy]	TACACS+	Enforcement policy controlling access to Policy Manager Admin
3.	□	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
4.	□	[Aruba Device Access Policy]	TACACS+	Enforcement policy controlling access to Aruba device
5.	□	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network
6.	□	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
7.	□	health check	WEBAUTH	Enforcement policy to disconnect devices from network
8.	□	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
9.	□	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
10.	□	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access
11.	□	Web authentication	RADIUS	

Now, let's add the ClearPass Server in the SonicWall NGFW. The **ClearPass Servers** tab of **Device > Network Access Control > Settings** page is displayed on the screen. On the page, click **Add** in the top-right corner of the screen.

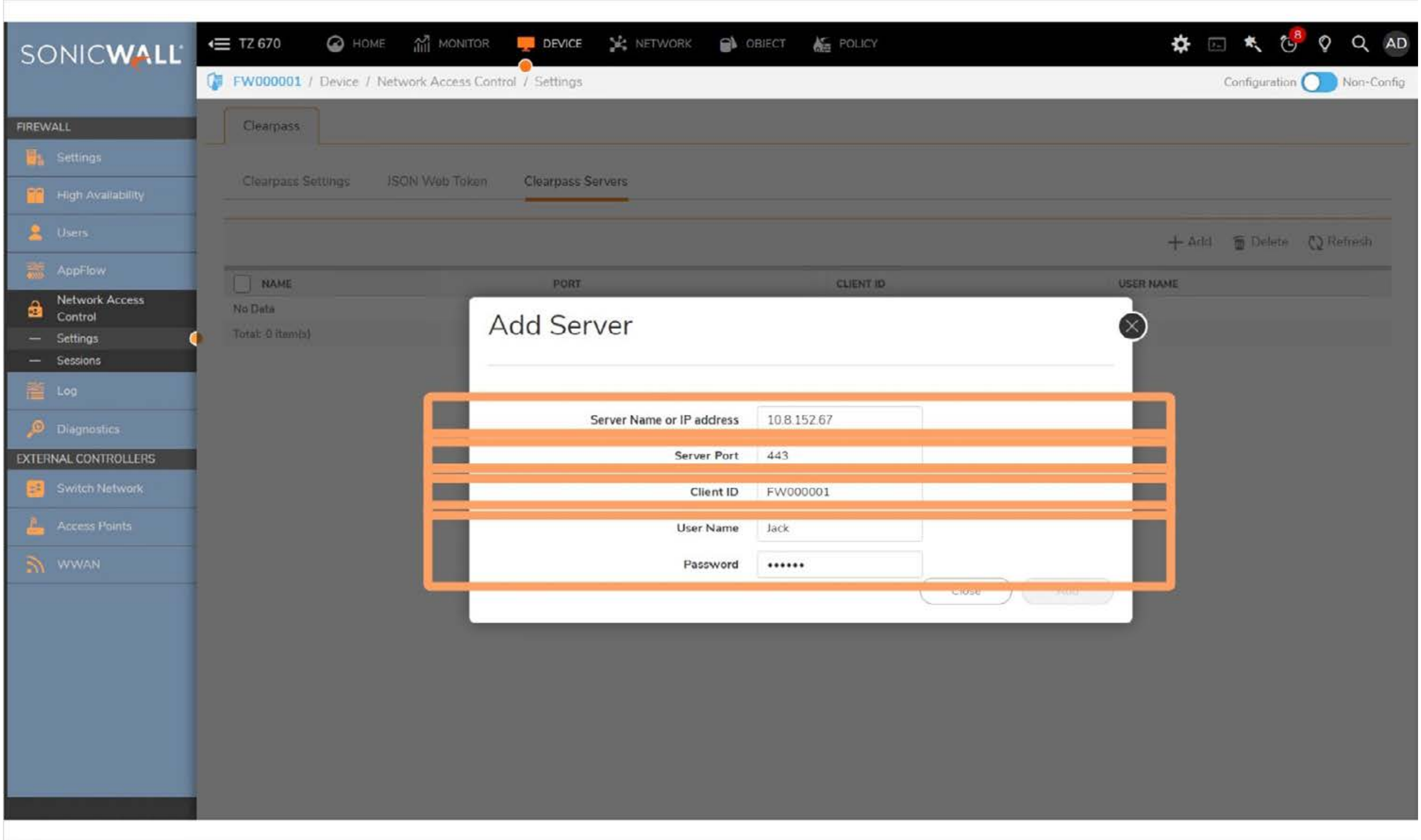


□ NAME	PORT	CLIENT ID	USER NAME
No Data			

Total: 0 item(s)

3. Add a ClearPass Server in SonicWall firewall

The various fields have been filled out for the purpose of this example. In the **Server Name or IP address** area, we entered the **ClearPass Policy Manager** IP address. In this example, the **Server Port** will be the default port 443. The **Client ID** is the one that was created in ClearPass. The **Username** and **Password** we configured for the **Client ID** have been entered in their respective fields. Click **Close**.



Add Server

Server Name or IP address 10.8.152.67

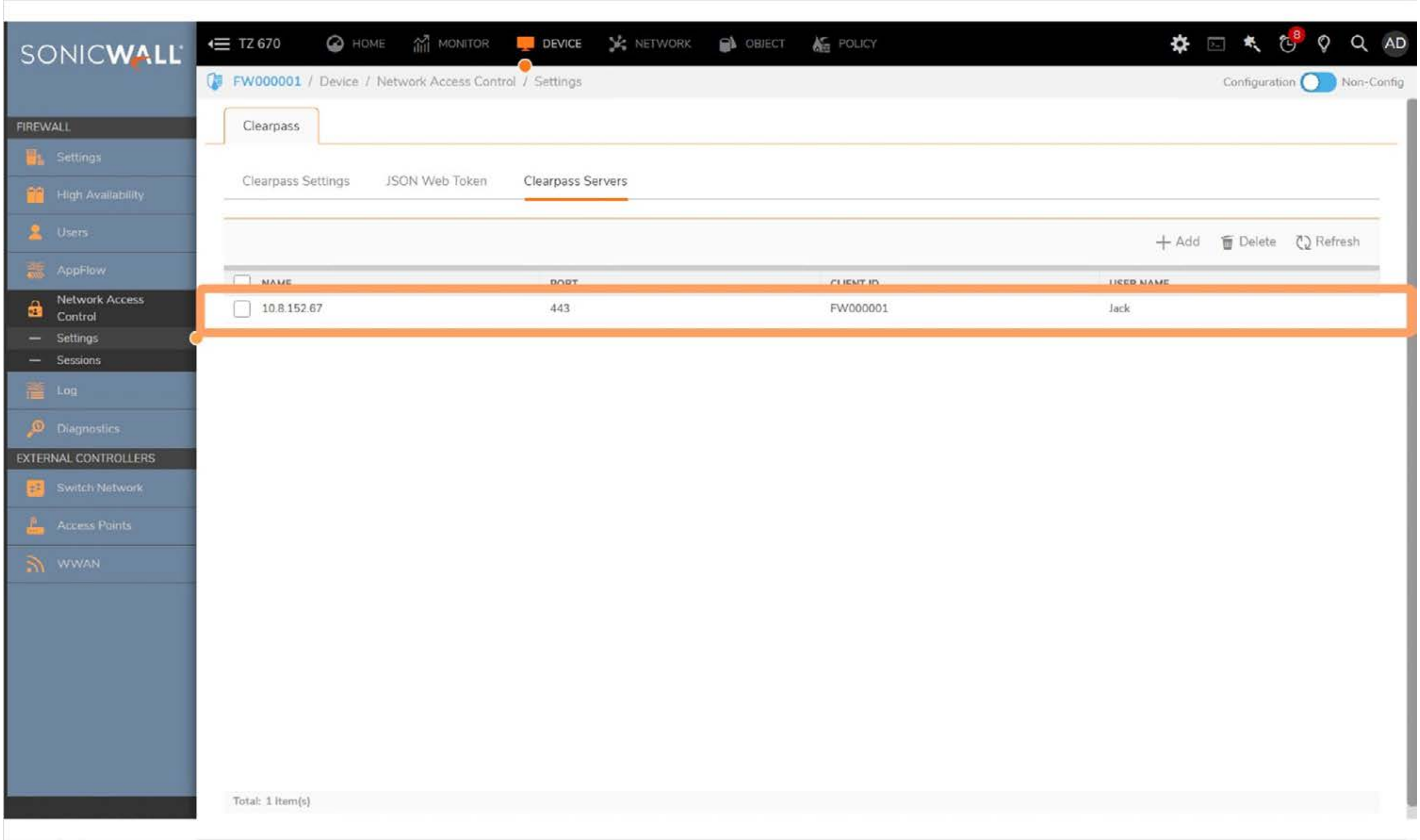
Server Port 443

Client ID FW000001

User Name Jack

Password ••••••

Notice on the screen that the **ClearPass Server** has been successfully added.



FW000001 / Device / Network Access Control / Settings

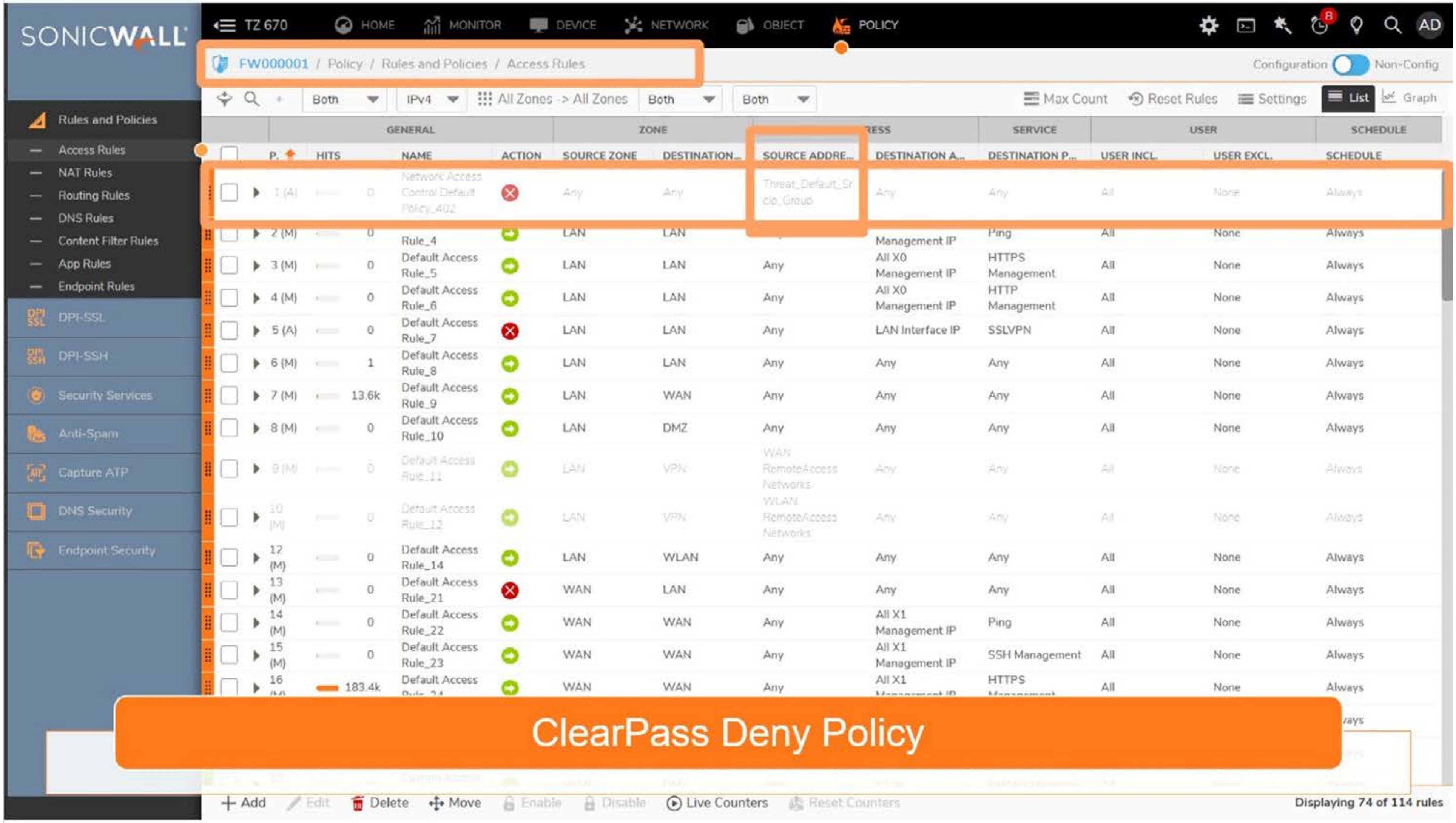
NAME	PORT	CLIENT ID	USER NAME
10.8.152.67	443	FW000001	Jack

Total: 1 item(s)

SonicOS will automatically generate a default **ClearPass Access Control Policy** and relevant **ClearPass Group Objects** when ClearPass is enabled in the firewall.

The **Policy > Rules and Policies > Access Rules** page is displayed on the screen. The firewall automatically creates a **ClearPass Deny Policy** for the traffic from the endpoint in **Threat_Default_SrcIP_Group**. This indicates that the Aruba wireless client traffic will be blocked if the rule is matched.

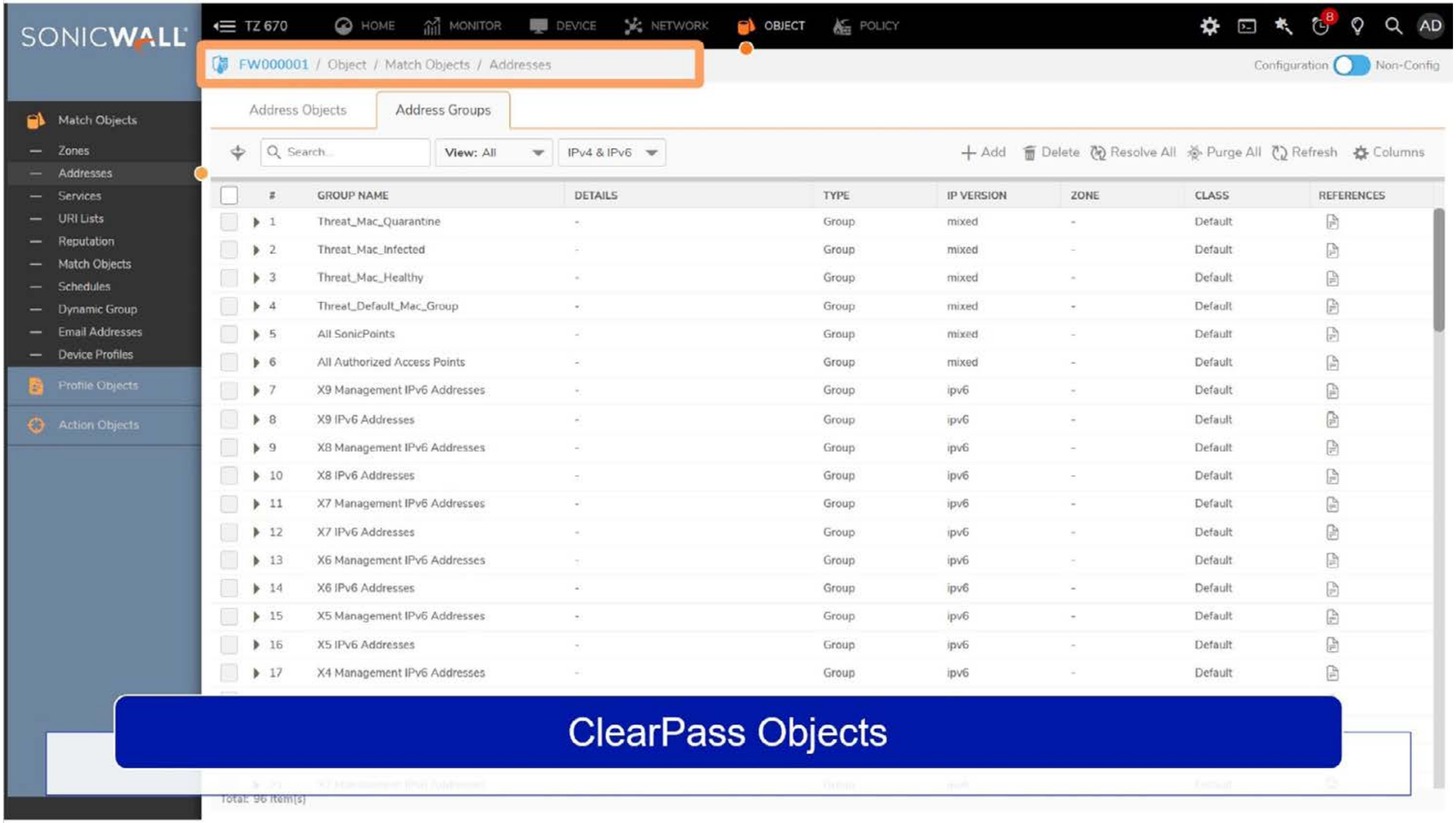
Note that the default ClearPass policy is editable. You can also customize a new ClearPass policy according to your organizational requirements.



GENERAL				ZONE		ADDRESS		SERVICE	USER		SCHEDULE
P.	HITS	NAME	ACTION	SOURCE ZONE	DESTINATION...	SOURCE ADDRE...	DESTINATION A...	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
1 (A)	0	Network Access Control Default Policy_402	✕	Any	Any	Threat_Default_Srcip_Group	Any	Any	All	None	Always
2 (M)	0	Rule_4	→	LAN	LAN		Management IP	Ping	All	None	Always
3 (M)	0	Default Access Rule_5	→	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
4 (M)	0	Default Access Rule_6	→	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
5 (A)	0	Default Access Rule_7	✕	LAN	LAN	Any	LAN Interface IP	SSLVPN	All	None	Always
6 (M)	1	Default Access Rule_8	→	LAN	LAN	Any	Any	Any	All	None	Always
7 (M)	13.6k	Default Access Rule_9	→	LAN	WAN	Any	Any	Any	All	None	Always
8 (M)	0	Default Access Rule_10	→	LAN	DMZ	Any	Any	Any	All	None	Always
9 (M)	0	Default Access Rule_11	→	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always
10 (M)	0	Default Access Rule_12	→	LAN	VPN	WLAN RemoteAccess Networks	Any	Any	All	None	Always
12 (M)	0	Default Access Rule_14	→	LAN	WLAN	Any	Any	Any	All	None	Always
13 (M)	0	Default Access Rule_21	✕	WAN	LAN	Any	Any	Any	All	None	Always
14 (M)	0	Default Access Rule_22	→	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always
15 (M)	0	Default Access Rule_23	→	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always
16	183.4k	Default Access	→	WAN	WAN	Any	All X1	HTTPS	All	None	Always

ClearPass Deny Policy

The **Address Groups** tab of **Object > Match Objects > Addresses** will have the default objects that have been automatically created when ClearPass is enabled in the NGFW.

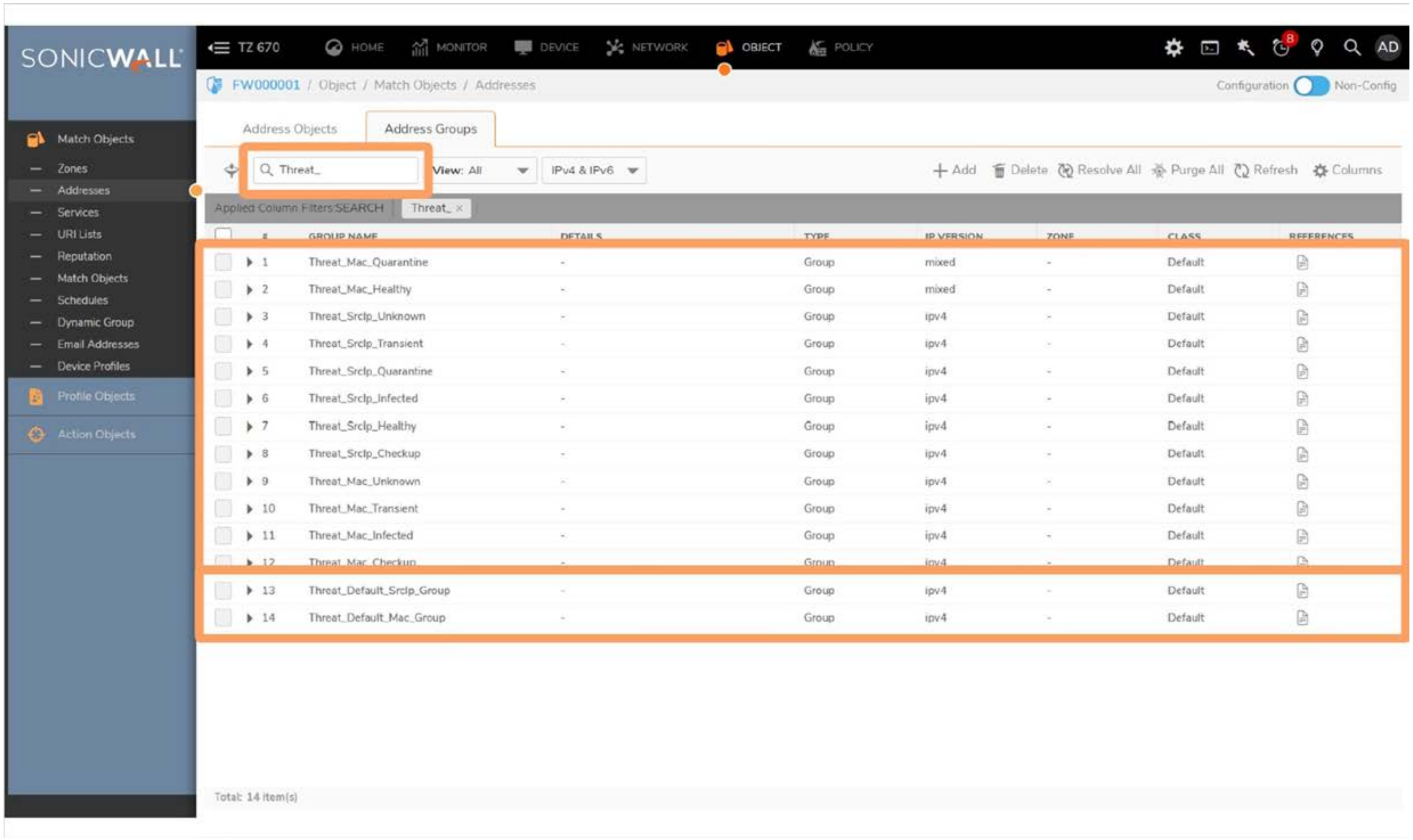


#	GROUP NAME	DETAILS	TYPE	IP VERSION	ZONE	CLASS	REFERENCES
1	Threat_Mac_Quarantine	-	Group	mixed	-	Default	
2	Threat_Mac_Infected	-	Group	mixed	-	Default	
3	Threat_Mac_Healthy	-	Group	mixed	-	Default	
4	Threat_Default_Mac_Group	-	Group	mixed	-	Default	
5	All SonicPoints	-	Group	mixed	-	Default	
6	All Authorized Access Points	-	Group	mixed	-	Default	
7	X9 Management IPv6 Addresses	-	Group	ipv6	-	Default	
8	X9 IPv6 Addresses	-	Group	ipv6	-	Default	
9	X8 Management IPv6 Addresses	-	Group	ipv6	-	Default	
10	X8 IPv6 Addresses	-	Group	ipv6	-	Default	
11	X7 Management IPv6 Addresses	-	Group	ipv6	-	Default	
12	X7 IPv6 Addresses	-	Group	ipv6	-	Default	
13	X6 Management IPv6 Addresses	-	Group	ipv6	-	Default	
14	X6 IPv6 Addresses	-	Group	ipv6	-	Default	
15	X5 Management IPv6 Addresses	-	Group	ipv6	-	Default	
16	X5 IPv6 Addresses	-	Group	ipv6	-	Default	
17	X4 Management IPv6 Addresses	-	Group	ipv6	-	Default	

Total: 96 item(s)

There are 14 **ClearPass Group Objects** which are created. These groups are categorized into six postures that ClearPass defines for an endpoint. These are **Healthy, Checkup, Transient, Quarantine, Infected** and **Unknown**. When the client device is connected and posted to the firewall, the MAC and IP addresses of the device will be updated into the relevant objects based on its posture.

- **Healthy** - Client is compliant. There are no restrictions on network access.
- **Checkup** - Client is compliant, but there is an update available. This can be used to proactively remediate to a healthy state.
- **Transient** - Client evaluation is in progress. This is typically associated with auditing a client. The network access granted is interim.
- **Quarantine** - Client is out of compliance. Restrict network access so the client only has access to the remediation servers.
- **Infected** - Client is infected and is a threat to other systems in the network. Network access should be denied or severely restricted.
- **Unknown** - The posture token of the client is unknown.



Threat_

Applied Column Filters SEARCH Threat_ ×

#	GROUP NAME	DETAILS	TYPE	IP VERSION	ZONE	CLASS	REFERENCES
1	Threat_Mac_Quarantine	-	Group	mixed	-	Default	🗎
2	Threat_Mac_Healthy	-	Group	mixed	-	Default	🗎
3	Threat_Srclp_Unknown	-	Group	ipv4	-	Default	🗎
4	Threat_Srclp_Transient	-	Group	ipv4	-	Default	🗎
5	Threat_Srclp_Quarantine	-	Group	ipv4	-	Default	🗎
6	Threat_Srclp_Infected	-	Group	ipv4	-	Default	🗎
7	Threat_Srclp_Healthy	-	Group	ipv4	-	Default	🗎
8	Threat_Srclp_Checkup	-	Group	ipv4	-	Default	🗎
9	Threat_Mac_Unknown	-	Group	ipv4	-	Default	🗎
10	Threat_Mac_Transient	-	Group	ipv4	-	Default	🗎
11	Threat_Mac_Infected	-	Group	ipv4	-	Default	🗎
12	Threat_Mac_Checkup	-	Group	ipv4	-	Default	🗎
13	Threat_Default_Srclp_Group	-	Group	ipv4	-	Default	🗎
14	Threat_Default_Mac_Group	-	Group	ipv4	-	Default	🗎

Total: 14 item(s)

Conclusion

Aruba ClearPass in conjunction with SonicWall can provide administrators with full context and visibility about the users and devices on the network to deliver end-to-end safe application enablement.

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.