

# 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.

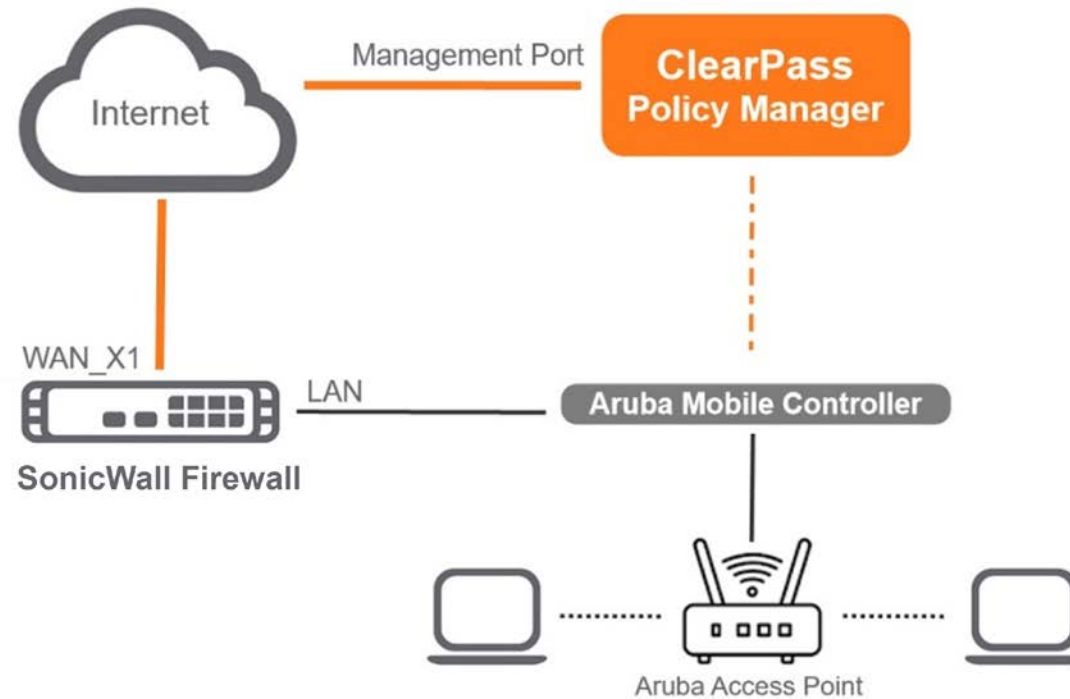
Aruba ClearPass can profile devices connecting to the network, identifying their type, operating system and other attributes. Posture assessment ensures that devices meet predefined security standards before being granted access, reducing the risk of compromised or non-compliant devices.

## 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.

# 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:

The screenshot shows the ClearPass Policy Manager interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'Local Users' and displays a table of users. A modal dialog box titled 'Add Local User' is open, allowing the user to create a new user with the following fields:

- User ID: Jack
- Name: Jack
- Password: [Redacted]
- Verify Password: [Redacted]
- Enable User:  (Check to enable user)
- Change Password:  (Check to force change password on next TACACS+ login)
- Role: Super Administrator

Below the form is an 'Attributes' section with a table:

Attribute	Value
1. Click to add...	

The background table shows existing users with columns for #, User ID, Name, Role, and Status. The first user is 'auto' with role '[Employee]' and status 'Enabled'. Other users have roles like 'Super Administrator' and 'Employee'.

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.

aruba ClearPass Guest Menu

Home > Administration > API Services > API Clients

API Clients

- Create API client
- Revoke all access tokens
- API Explorer
- API sample code on GitHub

The API clients you have defined are listed below.

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

Back to API services

Back to administration

Back to main

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**.

The screenshot displays the Aruba ClearPass Guest web interface for creating a new API client. The page title is "ClearPass Guest" and the breadcrumb trail is "Home » Administration » API Services » API Clients". The main heading is "Create API Client" with a sub-note: "Use this form to create a new API client." The form includes the following fields:

- \* 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.)

Buttons at the bottom of the form are "Create API Client" and "Cancel". A legend indicates that an asterisk (\*) denotes a required field. Navigation links at the bottom include "Back to API clients", "Back to API services", "Back to administration", and "Back to main".

© 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**.

The screenshot shows the Aruba ClearPass Guest web interface. The left sidebar contains navigation options: Guest, Devices, Onboard, Configuration, and Administration. Under Administration, there are sub-menus for API Services (API Clients, API Explorer, SOAP Web Services), Aruba Integrations, Check Security, Data Retention, Extensions, Import Configuration, Operator Logins, Plugin Manager, and Support. The main content area is titled 'Create API Client' and includes a breadcrumb trail: Home » Administration » API Services » API Clients. Below the title is a subtitle: 'Use this form to create a new API client.' The form itself is titled 'Create API Client' and contains the following fields:

- \* Client ID: FW000001 (with a tooltip: 'The unique string identifying this API client. Use this value in the OAuth2 "client\_id" parameter.')
- Description: For SonicWall Firewall (with a tooltip: '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 (with a tooltip: 'Select the purpose of this API client.')
- \* Operator Profile: (Select an operator profile) (with a tooltip: 'Select the purpose of this API client.')
- \* Grant Type: (Select an operator profile)

The 'Operator Profile' dropdown menu is open, showing a list of profiles with their respective permissions:

- (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

At the bottom of the page, there is a copyright notice: '© Copyright 2023 Hewlett Packard Enterprise Development LP' and a version string: '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.

The screenshot displays the Aruba ClearPass Guest administration console. The left sidebar shows the navigation menu with 'Administration' expanded to 'API Services' and 'API Clients'. The main content area is titled 'Create API Client' and includes a breadcrumb trail: Home » Administration » API Services » API Clients. Below the title is a subtitle: 'Use this form to create a new API client.' The form itself is titled 'Create API Client' and contains several fields:

- \* 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) - This dropdown menu is open, showing three options: '(Select an OAuth2 grant type)', 'Client credentials (grant\_type=client\_credentials)', and 'Username and password credentials (grant\_type=password)'. The third option is highlighted in blue.

At the bottom of the form, there is a legend for required fields and four back navigation links: 'Back to API clients', 'Back to API services', 'Back to administration', and 'Back to main'. The footer of the page contains the copyright information: '© Copyright 2023 Hewlett Packard Enterprise Development LP' and the version information: 'ClearPass Guest 6.10.0.180076 on C3 ABV 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.

The screenshot displays the 'Create API Client' form in the Aruba ClearPass Guest administration interface. The form is titled 'Create API Client' and includes the following fields and options:

- \* 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.)

The 'Access Token Lifetime' and 'Refresh Token Lifetime' fields are highlighted with an orange box. Below the form, there are buttons for 'Create API Client' and 'Cancel', and a legend for '\* required field'. Navigation links for 'Back to API clients', 'Back to API services', and 'Back to administration' are also present.

© 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.

The screenshot shows the Aruba ClearPass Guest Administration interface. The left sidebar contains navigation options: Guest, Devices, Onboard, Configuration, and Administration. The Administration menu is expanded, showing API Services, API Clients, API Explorer, and SOAP Web Services. The main content area is titled 'API Clients' and shows a breadcrumb trail: Home » Administration » API Services » API Clients. A 'Filter:' input field is present above the table. The table lists several API clients, with the first one, 'FW000001' (For SonicWall Firewall), highlighted by an orange border. Below the table are links to 'Back to API services', 'Back to administration', and 'Back to main'. On the right side, there are action buttons: 'Create API client', 'Revoke all access tokens', 'API Explorer', and 'API sample code on GitHub'. The footer contains copyright information for Hewlett Packard Enterprise Development LP and the version 'ClearPass Guest 6.10.0.180076 on CLABV platform'.

Client ID	Operating Mode	Grant Types	Access Token	Operator Profile
FW000001 For SonicWall Firewall	ClearPass REST API	password refresh_token	180 days	Super Administrator
snwl1	ClearPass REST API	password refresh_token	20 weeks	Super Administrator
snwl2	ClearPass REST API	password refresh_token	20 weeks	Super Administrator
snwl3	ClearPass REST API	password refresh_token	10 weeks	Super Administrator
snwl4	ClearPass REST API	password refresh_token	8 weeks	Super Administrator
Sonicwall	ClearPass REST API	password refresh_token	10 weeks	Super Administrator

## 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**.

The screenshot shows the SonicWall management interface for device 2CB8EDA2CA9C. The breadcrumb path is Device / Network Access Control / Settings. The 'Clearpass' tab is selected, and the 'CLEARPASS SETTINGS' section is visible. The 'Enable Clearpass' toggle is turned on. Below it, the 'Query User Role Interval(hours)' is set to 1. The 'Last Query Status' is 'Success', 'Last Query at' is '01/11/2024 18:44:06.000', and 'Number of Roles' is 26. There are 'Query Now', 'Cancel', and 'Accept' buttons.

Query User Role Interval(hours)	1	Query Now
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.

2CB8ED6CA968 / Device / Network Access Control / Settings

Clearpass

Clearpass Settings   **Json Web Token**   Clearpass Servers

JSON WEB TOKEN

Token Expires in (Days)

Generate Token Name

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1Ym91IjoiaWYWRtaW4ifQ.mpQjkxzdSIWPTocYVTtmebk  
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.

Action	Header	Content	Attributes
Specify the key-value pairs to be included in the HTTP Header -			
#	Header Name	Header Value	
1.	Authorization =	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1IjoiYWRtaW4ifQ.1yEUn_e5	
2.	<i>Click to add...</i>		

### 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:	<input type="text" value="test"/>
Name:	<input type="text" value="test"/>
Password:	<input type="password" value="....."/>
Verify Password:	<input type="password" value="....."/>
Enable User:	<input checked="" type="checkbox"/> (Check to enable user)
Change Password:	<input type="checkbox"/> (Check to force change password on next TACACS+ login)
Role:	<input type="text" value="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

**Summary** Profile Attributes

#### 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

Filter: Name contains  +   Show 20 records

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

The screenshot displays the SonicWall management interface. The breadcrumb navigation at the top reads: FW000001 / Device / Network Access Control / Settings. The left sidebar shows the 'Network Access Control' menu expanded to 'Settings'. The main content area has three tabs: 'Clearpass Settings', 'JSON Web Token', and 'Clearpass Servers', with the latter being selected. Below the tabs, there are '+ Add', 'Delete', and 'Refresh' buttons. A table with the following columns is shown: NAME, PORT, CLIENT ID, and USER NAME. The table is empty, with the text 'Total: 0 item(s)' below it. An orange callout box at the bottom of the image contains the text: 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**.

The screenshot displays the SonicWall management console interface. The top navigation bar includes the SonicWall logo, device information (TZ 670), and various system icons. The left sidebar lists configuration categories: FIREWALL (Settings, High Availability, Users, AppFlow, Network Access Control, Sessions, Log, Diagnostics) and EXTERNAL CONTROLLERS (Switch Network, Access Points, WWAN). The main content area shows the 'Clearpass' settings for device FW000001, with the 'Clearpass Servers' tab selected. A modal dialog titled 'Add Server' is open, containing the following fields:

NAME	PORT	CLIENT ID	USER NAME
No Data			
Total: 0 item(s)			

Server Name or IP address	10.8.152.67
Server Port	443
Client ID	FW000001
User Name	Jack
Password	*****

At the bottom of the dialog are 'Close' and 'Add' buttons. The dialog is highlighted with an orange border.

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

The screenshot displays the SonicWall management console interface. The top navigation bar includes the SonicWall logo, a breadcrumb trail (TZ 670 / HOME / MONITOR / DEVICE / NETWORK / OBJECT / POLICY), and utility icons. The left sidebar lists various configuration categories: FIREWALL (Settings, High Availability, Users, AppFlow, Network Access Control, Log, Diagnostics) and EXTERNAL CONTROLLERS (Switch Network, Access Points, WWAN). The main content area is titled 'FW000001 / Device / Network Access Control / Settings' and features a 'Clearpass' tab. Under this tab, there are three sub-sections: 'Clearpass Settings', 'JSON Web Token', and 'Clearpass Servers', with the latter being the active section. A table lists the configured ClearPass servers, with one entry highlighted by an orange border:

<input type="checkbox"/>	NAME	PORT	CLIENT ID	USER NAME
<input type="checkbox"/>	10.8.152.67	443	FW000001	Jack

At the bottom of the table area, it indicates 'Total: 1 Item(s)'. The interface also includes '+ Add', 'Delete', and 'Refresh' actions for the table.

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.

The screenshot displays the SonicWall configuration interface for Access Rules. The breadcrumb path is **FW000001 / Policy / Rules and Policies / Access Rules**. The interface shows a list of rules with columns for GENERAL, ZONE, ADDRESS, SERVICE, USER, and SCHEDULE. One rule is highlighted with an orange box:

GENERAL	ZONE	ADDRESS	SERVICE	USER	SCHEDULE
<input type="checkbox"/> 1 (A) 0 Network Access Control Default Policy_402	Any	Threat_Default_SrcIP_Group	Any	All	Always

An orange callout box at the bottom of the screenshot contains the text **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.

The screenshot shows the SonicWall NGFW interface. The breadcrumb navigation is **FW000001 / Object / Match Objects / Addresses**. The **Address Groups** tab is selected. The table below lists 17 address groups:

#	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	

A blue banner at the bottom of the table area contains the text **ClearPass Objects**. The status bar at the bottom left indicates **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.

The screenshot shows the SonicWall management console interface. The top navigation bar includes 'TZ 670', 'HOME', 'MONITOR', 'DEVICE', 'NETWORK', 'OBJECT', and 'POLICY'. The breadcrumb path is 'FW000001 / Object / Match Objects / Addresses'. The left sidebar contains a menu with 'Match Objects' selected, and sub-items like 'Zones', 'Addresses', 'Services', 'URI Lists', 'Reputation', 'Match Objects', 'Schedules', 'Dynamic Group', 'Email Addresses', 'Device Profiles', 'Profile Objects', and 'Action Objects'. The main content area shows a search for 'Threat\_' and a table of 14 objects. The table has columns for 'GROUP NAME', 'TYPE', 'IP VERSION', 'ZONE', 'CLASS', and 'REFERENCES'. The objects are numbered 1 through 14 and include names like 'Threat\_Mac\_Quarantine', 'Threat\_Mac\_Healthy', 'Threat\_SrcIp\_Unknown', etc. The table is highlighted with an orange border.

#	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_SrcIp_Unknown	-	Group	ipv4	-	Default	
4	Threat_SrcIp_Transient	-	Group	ipv4	-	Default	
5	Threat_SrcIp_Quarantine	-	Group	ipv4	-	Default	
6	Threat_SrcIp_Infected	-	Group	ipv4	-	Default	
7	Threat_SrcIp_Healthy	-	Group	ipv4	-	Default	
8	Threat_SrcIp_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_SrcIp_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](http://www.sonicwall.com)

SONICWALL®

© 2024 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. 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.