

# CLEARPASS ONGUARD AGENTS

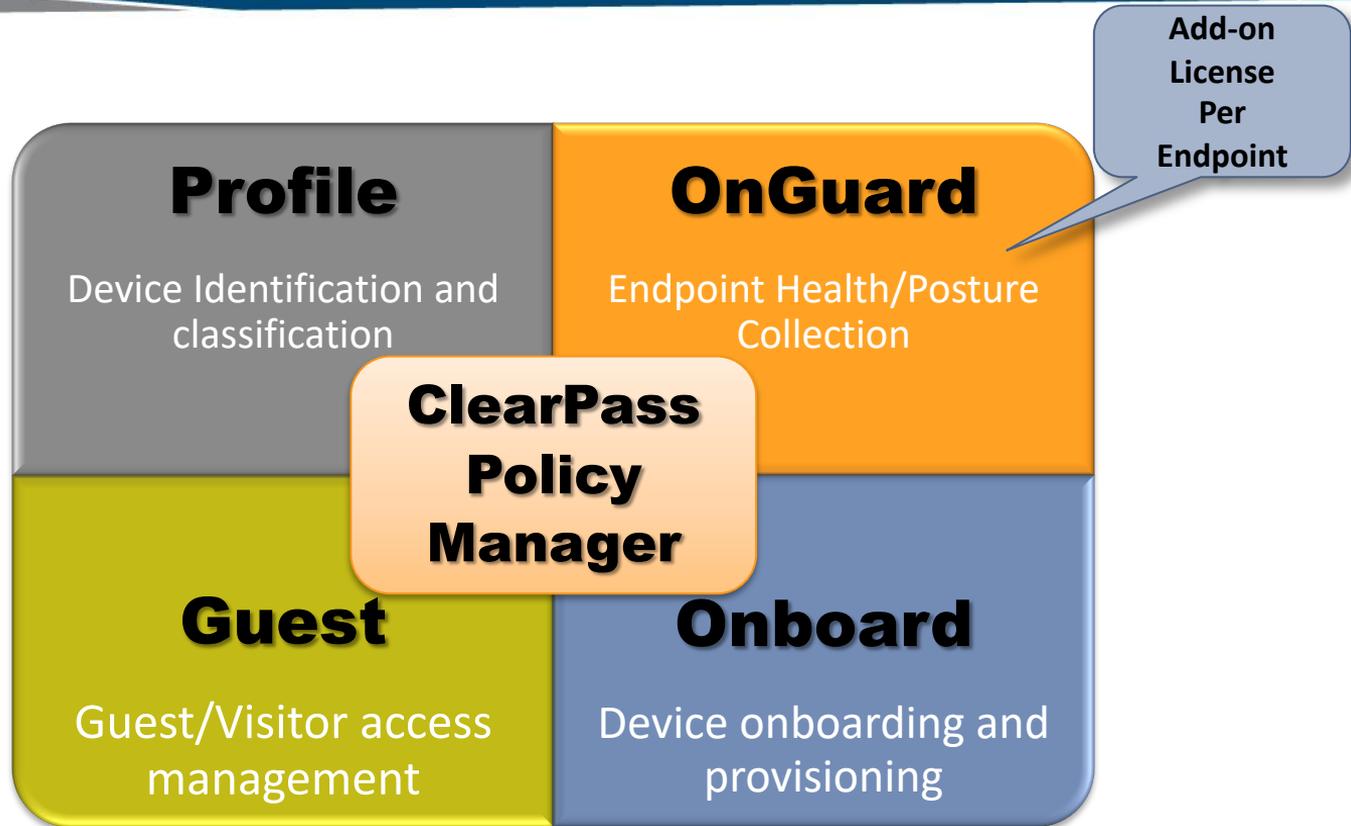
## Technical Climb Webinar

10:00 GMT | 11:00 CET | 13:00 GST  
Feb 26th, 2019

Presenter: Saravanan Rajagopal  
[saravanan.rajagopal@hpe.com](mailto:saravanan.rajagopal@hpe.com)



# WHAT IS CLEARPASS ONGUARD?



# Cont..

- ❖ **ClearPass OnGuard controls compromised devices by detecting and blocking access to unsecure or unhealthy devices.**
- ❖ **The client is denied access to network resources across wired, wireless, and remote networks when it is determined to be unsecure, which is accomplished by running an extensive posture assessment.**

# TYPES OF AGENTS

- ❖ **Persistent Agents** - The persistent agent provides nonstop monitoring and automatic remediation and control. When running persistent agents, ClearPass Policy Manager (Multi-master cache) can centrally send system-wide notification and alerts, and allow or deny network access.
- ❖ **Dissolvable agents** - The web-based dissolvable agent is ideal for personal, non IT issued devices that connect via captive portal and do not allow agents to be permanently installed. It is a one-time check at login to ensure policy compliance.

# Where can I download the agents?

Administration » Agents and Software Updates » OnGuard Settings -

## OnGuard Settings -

Use the OnGuard Settings page to configure the OnGuard agent deployment packages for Windows, macOS, and Ubuntu.

 Global Agent Settings  
 Policy Manager Zones

Settings

Installers 

Agent Installers updated at Feb 22, 2019 00:50:55 IST

 Windows	<a href="https://10.23.194.223/agent/installer/windows/ClearPassOnGuardInstall.exe">https://10.23.194.223/agent/installer/windows/ClearPassOnGuardInstall.exe</a>	(Full Install - EXE)	30MB
	<a href="https://10.23.194.223/agent/installer/windows/ClearPassOnGuardInstall.msi">https://10.23.194.223/agent/installer/windows/ClearPassOnGuardInstall.msi</a>	(Full Install - MSI)	30MB
	<a href="https://10.23.194.223/agent/installer/windows/ClearPassOnGuardLibraryUpdate.exe">https://10.23.194.223/agent/installer/windows/ClearPassOnGuardLibraryUpdate.exe</a>	(Update Only)	7MB
 macOS	<a href="https://10.23.194.223/agent/installer/mac/ClearPassOnGuardInstall.dmg">https://10.23.194.223/agent/installer/mac/ClearPassOnGuardInstall.dmg</a>	(Full Install)	22MB
	<a href="https://10.23.194.223/agent/installer/mac/ClearPassOnGuardLibraryUpdate.pkg">https://10.23.194.223/agent/installer/mac/ClearPassOnGuardLibraryUpdate.pkg</a>	(Update Only)	4MB
 Ubuntu	<a href="https://10.23.194.223/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz">https://10.23.194.223/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz</a>	(Full Install)	48MB
	<a href="https://10.23.194.223/agent/installer/ubuntu/ClearPassOnGuardLibraryUpdate.tar.gz">https://10.23.194.223/agent/installer/ubuntu/ClearPassOnGuardLibraryUpdate.tar.gz</a>	(Update Only)	19MB

### Native Dissolvable Agent Apps

 Windows	<a href="https://10.23.194.223/agent/webagent/windows/OnGuard Windows Health Checker.exe">https://10.23.194.223/agent/webagent/windows/OnGuard Windows Health Checker.exe</a>	(Full Install)	14MB
	<a href="https://10.23.194.223/agent/webagent/windows/OnGuard Windows Health Checker Library Update.exe">https://10.23.194.223/agent/webagent/windows/OnGuard Windows Health Checker Library Update.exe</a>	(Update Only)	5MB
 macOS	<a href="https://10.23.194.223/agent/webagent/mac/OnGuard Mac Health Checker.dmg">https://10.23.194.223/agent/webagent/mac/OnGuard Mac Health Checker.dmg</a>	(Full Install)	10MB
	<a href="https://10.23.194.223/agent/webagent/mac/OnGuard Mac Health Checker Library Update.pkg">https://10.23.194.223/agent/webagent/mac/OnGuard Mac Health Checker Library Update.pkg</a>	(Update Only)	4MB
 Ubuntu	<a href="https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker-x86.tar.gz">https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker-x86.tar.gz</a>	(Full Install 32-bit)	10MB
	<a href="https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker.tar.gz">https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker.tar.gz</a>	(Full Install 64-bit)	11MB
	<a href="https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker Library Update-x86.tar.gz">https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker Library Update-x86.tar.gz</a>	(Update Only 32-bit)	9MB
	<a href="https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker Library Update.tar.gz">https://10.23.194.223/agent/webagent/ubuntu/OnGuard Ubuntu Health Checker Library Update.tar.gz</a>	(Update Only 64-bit)	10MB

# OnGuard Posture Policies

Configuration » Posture » Posture Policies » Edit - Windows Posture Policies

## Posture Policies - Windows Posture Policies

**Summary** Policy Posture Plugins Rules

### Policy:

Policy Name:	Windows Posture Policies
Description:	
Posture Agent:	Web Agent
Host Operating System:	WINDOWS
Plugin Version:	2.0
Restrict by Roles:	

### Posture Plugins:

The list of selected plugins:

Plugin Name	Plugin Configuration	Status
1. ClearPass Windows Universal System Health Validator 	<a href="#">View</a>	Configured

### Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Posture Token
1. Passes all SHV checks - ClearPass Windows Universal System Health Validator	HEALTHY
2. Fails one or more SHV checks - ClearPass Windows Universal System Health Validator	QUARANTINE

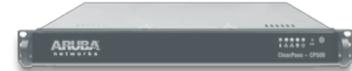
# Mapping Posture Policy To Service

Configuration » Services » Add

## Services

Service	Authentication	Roles	Posture	Enforcement	Summary
<b>Posture Policies:</b>					
Posture Policies:	Only OnGuard agent type Posture Policies are applicable for this service				
	<input type="text" value="Windows Posture Policies"/>	<input type="button" value="Remove"/>	<input type="button" value="View Details"/>	<input type="button" value="Modify"/>	
	<input type="text" value="--Select to Add--"/>				
Default Posture Token:	<input type="text" value="UNKNOWN (100)"/>				
Remediate End-Hosts:	<input checked="" type="checkbox"/> Enable auto-remediation of non-compliant end-hosts				
Remediation URL:	<input type="text"/>				

# Sample Policy Flow With Posture



User

CPPM

802.1x service

**Posture : Unknown**

**Enforcement Profile:**  
Quarantine VLAN

Web-based  
health check  
service

**Posture : Healthy**

**Enforcement Profile:**  
Terminate Session

802.1x service

**Posture : Healthy**

**Enforcement Profile:**  
Full access VLAN

# CLEARPASS ONGUARD AGENT COMPONENTS

# Cont..

- ❖ **ClearPass OnGuard agents has multiple components like Backend Service, Frontend (agent user interface), etc.**
- ❖ **Each of these components performs specific functions and it is important to understand the functions of these components for effective troubleshooting.**

**Let us Dive In!**

# 1. ClearPass OnGuard User Interface (OnGuard Frontend)

- ❖ **OnGuard Frontend** - is the main UI window of ClearPass OnGuard. It has separate UI sections for VPN and Health Checks. It allows users to start health checks, connect/disconnect VPN network, view remediation messages and results, view diagnostic logs, etc.

## Windows:

- ❖ Process Name - ClearPassOnGuard.exe
- ❖ Installation Path - “%ProgramFiles%\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard.exe”
- ❖ Log file - “%ProgramData%\Aruba Networks\ClearPassOnGuard\anuacui.txt”

# Cont..

ClearPass OnGuard 6.7.7.109065

**Health Status: Not Known**

Connection Details | Diagnostics | Settings

Health Status: Not Known

Login

Retry

ClearPass OnGuard

Enter login credentials

Username

arubatest

Password

••••••••

OK

Cancel

Send Logs

ClearPass OnGuard 6.7.7.109065

**Health Status: Healthy**

Connection Details | Diagnostics | Settings

Health Status: Healthy

Logout

Retry

INFO:Response processed

**02/23/19 03:09:32 Started new Session**

Health Log

Send Logs

ClearPass OnGuard 6.7.7.109065

**Health Status: Healthy**

Connection Details | Diagnostics | Settings

Diagnostic Type: Health Log

The health log provides the most recent sequence of events that took place after Application was launched.

[03:09:21] Ethernet: Waiting for Credentials.  
[03:09:22] Connection to ClearPass OnGuard Agent Service establis  
[03:09:33] Ethernet (WIRED) is managed by Server.  
[03:09:33] Ethernet: ClearPass Server reachable = 10.162.116.11  
[03:09:33] Ethernet: Started collecting health information.  
[03:09:58] Ethernet: Sending authentication request  
[03:10:03] Ethernet: Processing response  
[03:10:04] Ethernet: Health status - Healthy.  
[03:10:04] Ethernet: Started collecting health information.  
[03:10:05] Ethernet: Sending authentication request  
[03:10:07] Ethernet: Processing response  
[03:10:08] Ethernet: Health status - Healthy.  
[03:10:08] Ethernet: Authentication successful  
[03:10:08] Ethernet: Health status - Healthy.

# Cont..

The screenshot shows the Windows Task Manager application in the Performance tab. The 'Processes' section is expanded, displaying a list of running applications and their resource usage. A red arrow points to the 'ClearPass OnGuard' process. The table below summarizes the data shown in the screenshot.

Name	CPU	Memory	Disk	Network
<b>Apps (7)</b>				
> ClearPass OnGuard	0%	8.7 MB	0 MB/s	0 Mbps
> Google Chrome	0%	189.2 MB	0 MB/s	0 Mbps
> Notepad++ : a free (GNU) ...	0%	280.7 MB	0 MB/s	0 Mbps
> Task Manager	0%	11.0 MB	0 MB/s	0 Mbps
> TFTP server	0%	4.5 MB	0 MB/s	0 Mbps
> Windows Command Proce...	0%	0.4 MB	0 MB/s	0 Mbps
> Windows Explorer (2)	0%	95.2 MB	0 MB/s	0 Mbps
<b>Background processes (58)</b>				
> Adobe Acrobat Update Ser...	0%	1.7 MB	0 MB/s	0 Mbps
> Antimalware Service Execu...	0%	75.9 MB	0 MB/s	0 Mbps
> Aruba Networks Service	0%	1.6 MB	0 MB/s	0 Mbps
> ClearPass Agent Controller...	0%	47.7 MB	0 MB/s	0 Mbps
> ClearPass OnGuard Agent ...	0%	2.5 MB	0 MB/s	0 Mbps

At the bottom of the window, there is a 'Fewer details' button on the left and an 'End task' button on the right.

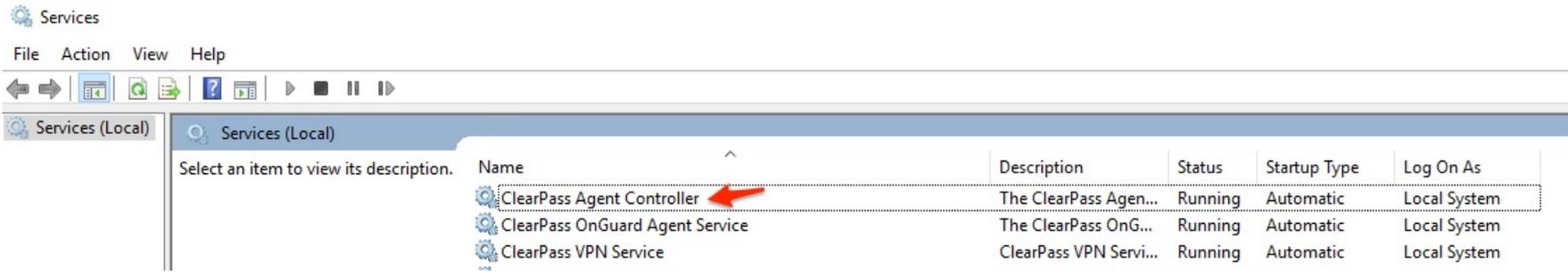
## 2. ClearPass OnGuard Backend Service (Backend Service)

- ❖ **ClearPass OnGuard Backend Service** - is installed as a Windows Service on Windows and as a Daemon on Mac OS X. It runs quietly in the background.
  
- ❖ **Some of the tasks performed by the Backend Service are:**
  - a) Monitor Health State – Backend Service collects health periodically (approx. every minute) to detect change in health state. Whenever a change in health state is detected, it informs OnGuard Plugin.
  - b) Collect Health – It also collects health whenever requested by OnGuard Plugin.
  - c) Process Health Response and Auto Remediation – It processes health check responses received from CPPM Server and also does auto remediation if required.
  - d) Bounce Network Interface – It bounces Network Interface as and when required, such as when the Agent Enforcement profile has bounce interface, when Frontend UI is closed etc.

# Cont..

## Windows:

- ❖ Service Name – ClearPass Agent Controller
- ❖ Process Name - ClearPassAgentController.exe
- ❖ Path - “%ProgramFiles%\Aruba Networks\ClearPassOnGuard\ClearPassAgentController.exe”
- ❖ Log file - “%ProgramData%\Aruba Networks\ClearPassOnGuard\winagent\_\*.log”



The screenshot shows the Windows Services console. The 'Services (Local)' window is open, displaying a list of services. The 'ClearPass Agent Controller' service is highlighted with a red arrow. The table below shows the details of the services listed.

Name	Description	Status	Startup Type	Log On As
ClearPass Agent Controller	The ClearPass Agen...	Running	Automatic	Local System
ClearPass OnGuard Agent Service	The ClearPass OnG...	Running	Automatic	Local System
ClearPass VPN Service	ClearPass VPN Servi...	Running	Automatic	Local System

### 3. ClearPass OnGuard Plugin (OnGuard Plugin)

- ❖ **OnGuard Plugin** - provides health check related functionality to OnGuard Frontend UI. It communicates with Backend Service (for collecting health, processing health responses, etc.) and CPPM Server (sends WebAuth Request, Establish Control Channel, etc).

#### **Windows:**

File Name – ClearPassOnGuardPlugin.dll

Path - %ProgramFiles%\Aruba Networks\ClearPassOnGuard\ClearPassOnGuardPlugin.dll

Log file - %AppData%\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard\_\*.log

## 4. ClearPass OnGuard Agent Service

- ❖ **ClearPass OnGuard Agent Service (from 6.6.0)** - allows OnGuard Agent on Windows running in **Service mode**. In Service Mode, OnGuard Agent will perform health checks even if User is not logged in.

### Windows:

- ❖ Service Name - ClearPass OnGuard Agent Service
- ❖ Process Name - ClearPassOnGuardAgentService.exe
- ❖ Path - “%ProgramFiles%\Aruba Networks\ClearPassOnGuard\ClearPassOnGuardAgentService.exe”
- ❖ Log file - “%ProgramData%\Aruba Networks\ClearPassOnGuard\winagent\_onguard\_service\_\*.log”

- ❖ The parameter "**Run OnGuard As**" is added in Global Agent settings to select the following agent mode,

<b>Agent</b>	Health checks are performed by the OnGuard Agent after the user logs in to the client.
<b>Service</b>	OnGuard Agent performs health checks as soon as the client boots up, that is, even before the user logs in to the client. When a user logs in to the client, the user can view the most recent health check results via the OnGuard Agent user interface. The user can perform health checks again by clicking the Retry button.
<b>Both Service and Agent</b>	When the user is not logged in to the client, the ClearPass OnGuard Agent service performs health checks. As soon as the user logs in to the client, the ClearPass OnGuard Agent service stops health checks and the OnGuard Agent user interface initiates health checks.

# Cont..

**Configure Global Agent Settings**

Name	Value	
1. Server Certificate Validation	= Required	
2. Cache Credentials Interval(in days)	= 15	
3. Enable to install VPN component	= false	
4. Run OnGuard As	= Agent	
5. Click to add...		

Agent  
Service  
BothServiceAndAgent

Save Cancel

## 5. ClearPass Universal System Health Agent Remediate (USHA Remediate)

- ❖ **ClearPass USHA Remediate** - is used by Backend Service to perform auto remediation of unhealthy health classes. Auto remediation of some of the health classes (like firewall) is done by Backend Service itself. For other health classes, USHA Remediate is used.

### Windows:

- ❖ Process Name - ClearPassUSHARemediate.exe
- ❖ Path - %ProgramFiles%\Aruba Networks\ClearPassOnGuard\ClearPassUSHARemediate.exe
- ❖ Log file - %ProgramData%\Aruba Networks\ClearPassOnGuard\winagent\_remediate\_\*.log

## 6. ClearPass Agent Helper (Agent Helper)

- ❖ **ClearPass Agent Helper** - is used by Backend Service to get information (name, status, etc.) of Virtual Machines created by current logged in user. It is also used by USHA Remediate to stop/pause Virtual Machines.

### Windows:

- ❖ Process Name - ClearPassAgentHelper.exe
- ❖ Path - %ProgramFiles%\Aruba Networks\ClearPassOnGuard\ClearPassAgentHelper.exe
- ❖ Log file - %ProgramData%\Aruba Networks\ClearPassOnGuard\winagent\_helper\_\*.log

## 7. ClearPass VPN Service (VPN Service)

- ❖ **ClearPass VPN Service** - is available only on Windows and provides VPN related features like establishing VPN Tunnel. It also downloads and installs ClearPass OnGuard Updates from Server.

### **Windows Only:**

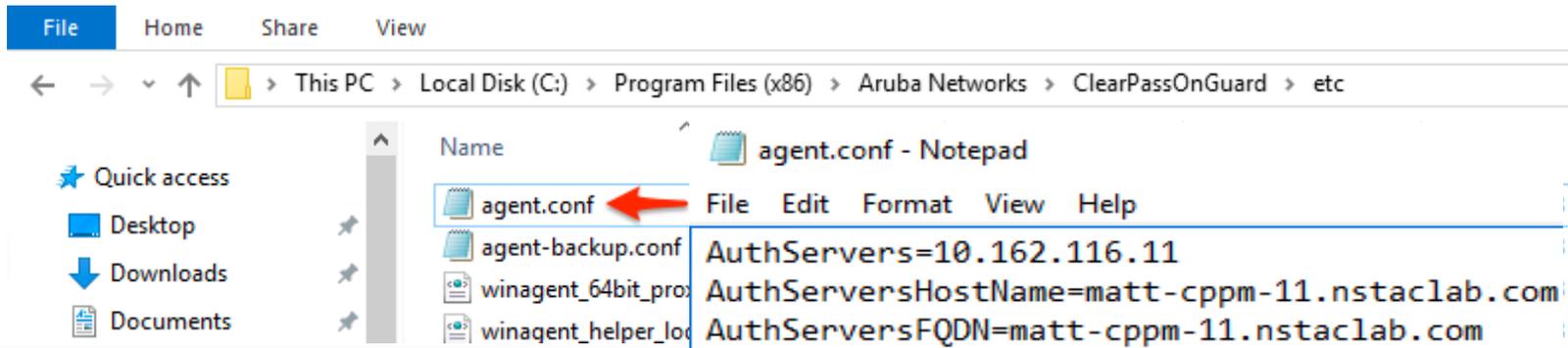
- ❖ Service Name - ClearPass VPN Service
- ❖ Process Name - arubanetsvc.exe
- ❖ Path - %ProgramFiles%\Aruba Networks\ClearPassOnGuard\arubanetsvc.exe
- ❖ Log file - %ProgramData%\Aruba Networks\ClearPassOnGuard\VIAService.txt

## 8. ClearPass OnGuard Agent Configuration (Agent Config)

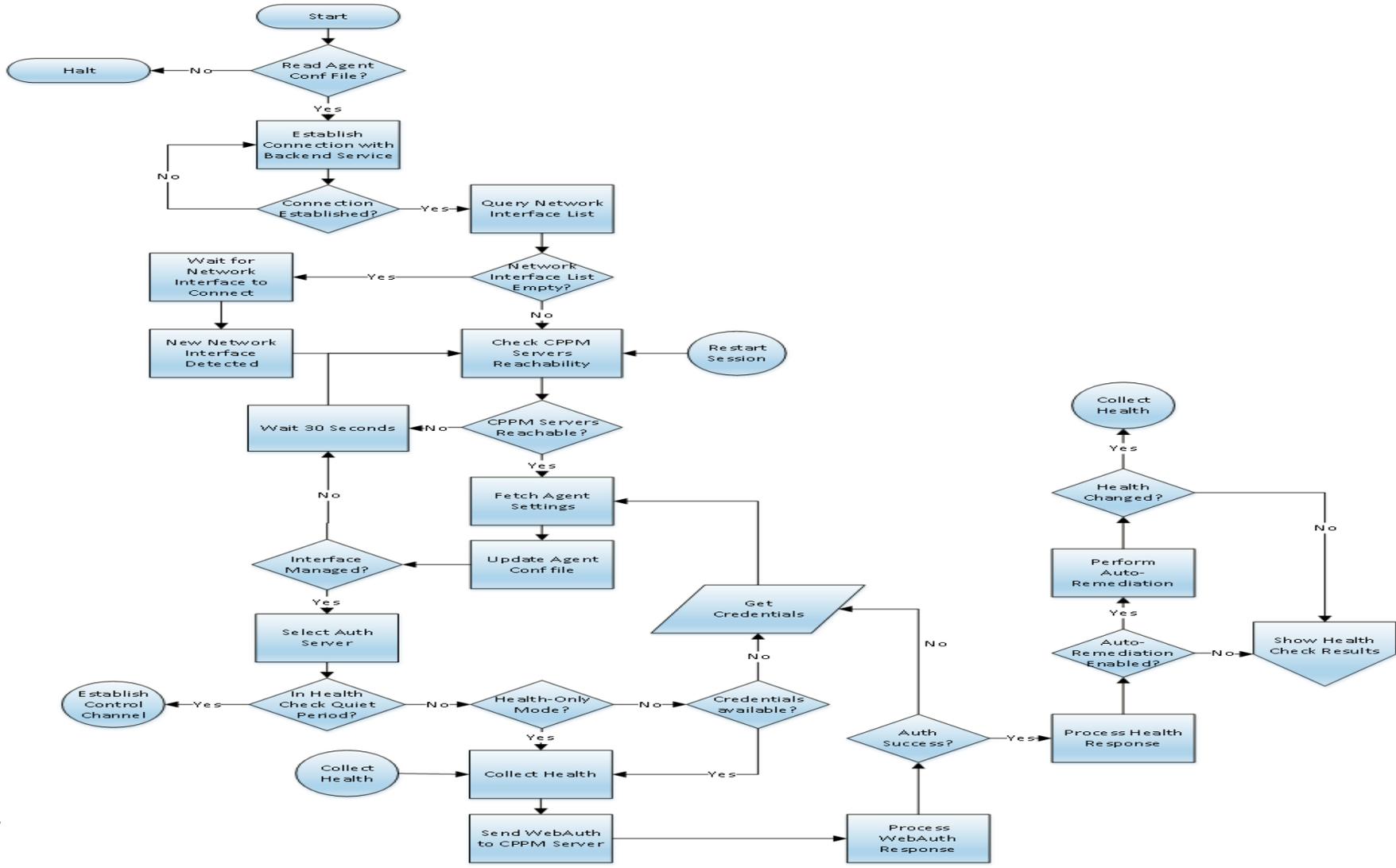
- ❖ **ClearPass OnGuard Agent Configuration (Agent Config)** - Among other information, ClearPass OnGuard Agent Configuration file contains a list of all CPPM Servers IP addresses. OnGuard Plugin uses this list to select one of the CPPM Servers.

### Windows:

- ❖ File Name - agent.conf
- ❖ Path - %ProgramFiles%\Aruba Networks\ClearPassOnGuard\etc\agent.conf



# CLEARPASS ONGUARD AGENT FLOW



# Initialize and Read CPPM Server IP Address List

**When the OnGuard Agent is launched, the first thing it does is read the list of CPPM Server IP Addresses from Agent Config (agent.conf) file.**

❖ **ClearPassOnGuard\_0.log:**

1. 2019-02-23 03:09:12,973 [Th 5324:5328] **INFO OnGuardPlugin - InitializeLogger: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard.exe**
2. 2019-02-23 03:09:12,988 [Th 5324:5328] **DEBUG OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Successfully read agent.conf file.**
3. 2019-02-23 03:09:12,988 [Th 5324:5328] **DEBUG OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: agent.conf file contains auth server list.**
4. 2019-02-23 03:09:12,988 [Th 5324:5328] **INFO OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Auth Server List - 10.162.116.11**
5. 2019-02-23 03:09:12,988 [Th 5324:5328] **ERROR OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: No auth servers fqdn in configuration**
6. 2019-02-23 03:09:12,988 [Th 5324:5328] **INFO OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Auth Server Host Name List - matt-cppm-11.nstaclab.com**

# Establish Connection with Backend Service

Once the Agent Conf file has been read, OnGuard Agent initiates connection with the Backend Service. The Backend Service listens for incoming connections from OnGuard Agents on local TCP Port #25427

❖ ClearPassOnGuard\_0.log:

1. 2019-02-23 03:09:13,503 [Th 0000f4c] **DEBUG OnGuardPlugin.BackendClient - Run: Backend Client Thread starting. Connecting to server on port=25427**
2. 2019-02-23 03:09:13,503 [Th 0000f4c] INFO OnGuardPlugin.SocketClient - Connect: BackendClient - Connecting to server=127.0.0.1 on port= 25427
3. 2019-02-23 03:09:13,503 [Th 0000f4c] **DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect to 127.0.0.1 at port - 25427**
4. 2019-02-23 03:09:13,550 [Th 0000f4c] **DEBUG OnGuardPlugin.ConnectionConnector - Connect: Successfully connected to DESKTOP-EQ59U8I. Server IP = 127.0.0.1, Port = 25427**
5. 2019-02-23 03:09:13,550 [Th 0000f4c] INFO OnGuardPlugin.SocketClient - Connect: BackendClient - Successfully connected to server. Registering the connection.

## Backend Service Logs (Connection Successful):

### ❖ winagent\_0.log:

1. 2019-02-23 03:08:59,965 [Th 000002F8] **DEBUG** WinAgent.ConnectionAcceptor - CWinAgentConnectionAcceptor::handle\_input()handle=00000328
2. 2019-02-23 03:08:59,965 [Th 000002F8] **INFO** WinAgent.ConnectionAcceptor - CWinAgentConnectionAcceptor::handle\_input() Accept Success: Client IP = 127.0.0.1, Port = 52923
3. 2019-02-23 03:08:59,965 [Th 00000cc4 Evt 0226F3B8] **INFO** WinAgent.WinAgentConnEvHandler - Registration of ReadHandler succeeded

# CPPM Server Reachability Check

For each active Network Interface, the OnGuard Agent checks reachability of all the CPPM Servers by the following reachability “Check” URL - “https://<CPPM Server IP Address>/images/index.html”.

## ❖ ClearPassOnGuard\_0.log:

1. 2019-02-23 03:09:15,506 [Th 000010c8] INFO OnGuardPlugin.AgentResourceHolder - GetAuthServerList: Auth Server List for " - [10.162.116.11]
2. 2019-02-23 03:09:15,506 [Th 000010c8] INFO OnGuardPlugin.StateMonitor - FetchAgentSettings: Auth Server List: 10.162.116.11
3. 2019-02-23 03:09:15,506 [Th 000010c8] DEBUG OnGuardPlugin.StateMonitor - IsServerReachable: called
4. 2019-02-23 03:09:15,506 [Th 000010c8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.23.172.231 Remote IP: 10.162.116.11, url: https://10.162.116.11/agent/index.html
5. 2019-02-23 03:09:16,507 [Th 000010c8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200

# Read/Fetch Agent Settings and Select Auth Server

**From the list of Reachable CPPM Servers, the OnGuard Agent has to select one CPPM Server.**

**For selecting CPPM Server, OnGuard Agent needs to know the Policy Manager Zone settings and to which Zone it belongs. To get Policy Manager Zone settings, OnGuard Agent reads Agent Settings from the first CPPM Server in the list**

Agent Settings URL - “https://<CPPM Server IP Address>/agent/settings”

# Cont..

## ❖ ClearPassOnGuard\_0.log:

2019-02-23 03:09:16,507 [Th 000010c8] **INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.23.172.231 Remote IP: 10.162.116.11, url: https://10.162.116.11/agent/settings**

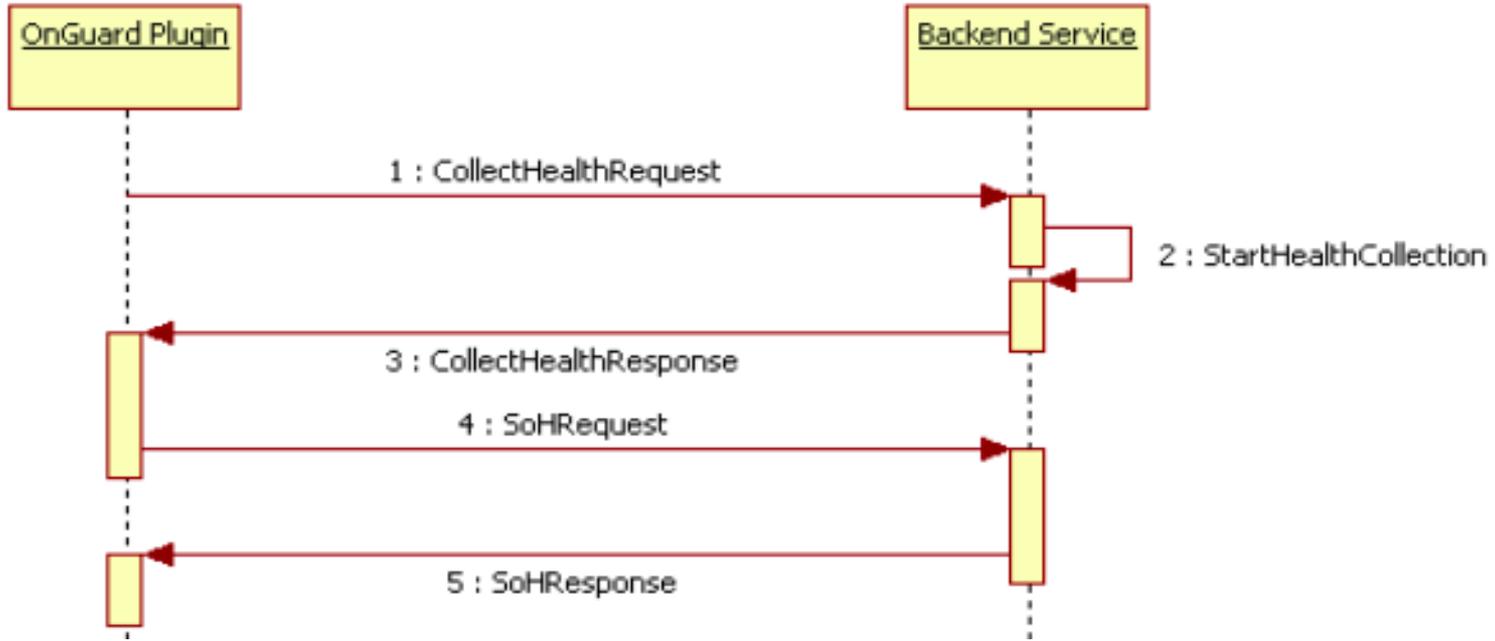
2019-02-23 03:09:17,380 [Th 000010c8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200

2019-02-23 03:09:17,380 [Th 000010c8] INFO OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: " - Parsing JSON = {"nodeDetails":[{"10.162.116.11":{"hostName":"matt-cppm-11.nstaclab.com","fqdn":""}}],"formType":"authApplet","**interfaces":"wired,wireless,vpn"**,"domainNodes":{},"nodeIp":["10.162.116.11"],"extraParams":{"customRemediationUIConfig":{"configured":false}},"usernameLabel":"Username","upgradeAction":"DoNothing","passwordLabel":"Password","mode":"both","webagent\_interfaces":"wired,wireless","nodes":**["default":["10.162.116.11"]]**,"agentLibraryVersion":"1.0.7.109065","CacheCredentialsForDays":"15",**domain":"default"**,"agentVersion":"6.7.7.109065","fieldSubmit":"Submit"}

2019-02-23 03:09:19,124 [Th 000010c8] **INFO OnGuardPlugin.InterfaceHelper - PickAuthServer: Picking Auth Server for Ethernet from Auth Server List : 10.162.116.11**

# Health Collection

Health Collection is done by the Backend Service. Whenever the OnGuard Plugin needs health information, it informs Backend Service. Backend Service collects health and sends Statement of Health (SoH) to OnGuard Plugin. Interaction between OnGuard Plugin and Backend Service for Health Collection is as shown below:



# Sample Health Check Results

ClearPass OnGuard 6.7.7.109065

**Health Status: Healthy**

Connection Details | Diagnostics | Settings

 Health Status: Healthy

INFO:Response processed

02/23/19 05:01:47 Started new Session  
[Show Old Sessions](#)

ClearPass OnGuard 6.7.7.109065

**Health Status: Quarantined**

Connection Details | Diagnostics | Settings

 Health Status: Quarantined

INFO:Response processed

 **ClearPass Windows SHV:**  
This Client or Operating System is not allowed by policy.

02/23/19 11:54:03 Started new Session  
[Show Old Sessions](#)

# Establish Control Channel

**After performing Agent Enforcement Actions, the OnGuard Agent establishes a Control Channel with the CPPM Server (Port #6658). This Control Channel is required to perform the following actions:**

- a) Showing Online/Offline status on 'OnGuard Activity' Page.
- b) Broadcasting Messages from CPPM Server to all Online clients.
- c) Bouncing clients from CPPM Server (OnGuard Activity or Access Tracker → Change Status).

**The OnGuard Agent periodically sends heart-beat (Keep-Alive) message to the CPPM Server over this Control Channel. This period is defined by “Keep-alive Interval (in seconds)” parameter in the Global Agent Settings.**

**Note: If the OnGuard Agent fails to establish a Control Channel, it assumes that the CPPM Server is Unreachable and closes current session and starts a new session.**

# Monitor Health State & Soft Re-Auth

**In AUTH\_COMPLETE state, the OnGuard Agent (Backend Service) monitors a client's health state. If the Backend Service detects any change in the status of any health class, it informs the OnGuard Plugin. The OnGuard Plugin does a Soft Re-Auth to checks if client's overall health state has really changed or not i.e. changed from Healthy to Unhealthy or vice-versa.**

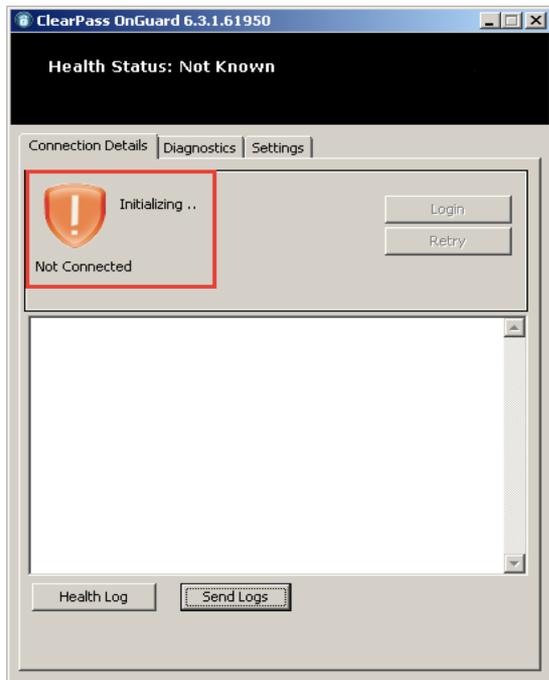
## **Differences between Soft Re-Auth and Full WebAuth:**

- ❖ Soft Re-Auth Requests are not shown in Access Tracker.
- ❖ Enforcement Policies are not applied to Soft Re-Auth Request, i.e. it will not change client's VLAN/Role, etc.
- ❖ Soft Re-Auth performs only Health Evaluation, not User Authentication.

# TROUBLESHOOTING COMMON ISSUES

# 1. ClearPass OnGuard Agent does not start health checks automatically

**This is a very common issue where OnGuard Agent shows “Initializing... / Not Connected” and does not start health checks automatically after it is launched.**



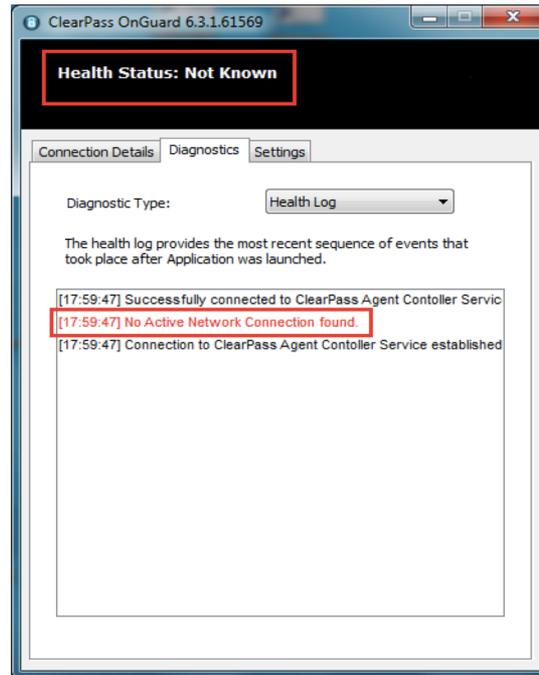
# Cont..

**This issue can be caused by a number of reasons as explained below, and Health Log view should be checked first for errors.**

- ❖ **No Network Connectivity**
- ❖ **CPPM Server is not reachable**
- ❖ **Network Interface is not managed by CPPM Server**
- ❖ **OnGuard Frontend/Plugin is not able to communicate with the Backend Service**
- ❖ **CPPM Server IP is changed**
- ❖ **Agent Configuration file is corrupt**

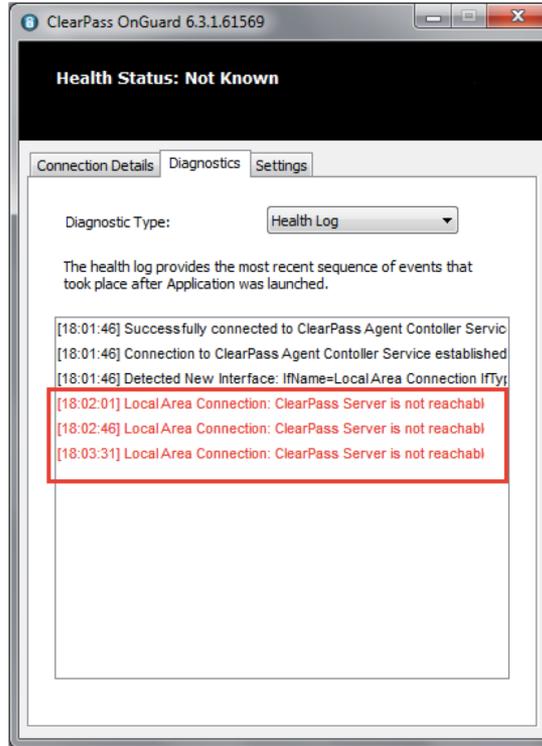
# Cont.. (No Network Connectivity)

- ❖ **No Network Connectivity** - Client is not connected to Network. OnGuard needs at least one active Network Connection.



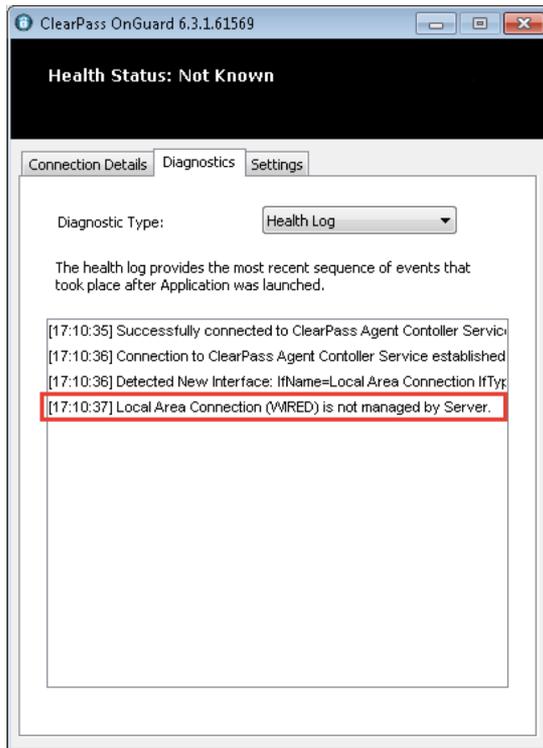
# Cont.. (CPPM Server is not reachable)

- ❖ **CPPM Server is not reachable** - CPPM Server is not reachable from any of the connected Network Interfaces.



# Cont.. (Network Interface is not managed by CPPM Server)

- ❖ **Network Interface is not managed by CPPM Server** - Current Network Interface is not Managed by the CPPM Server.



## OnGuard Settings -

 Global Agent Settings  
 Policy Manager Zones

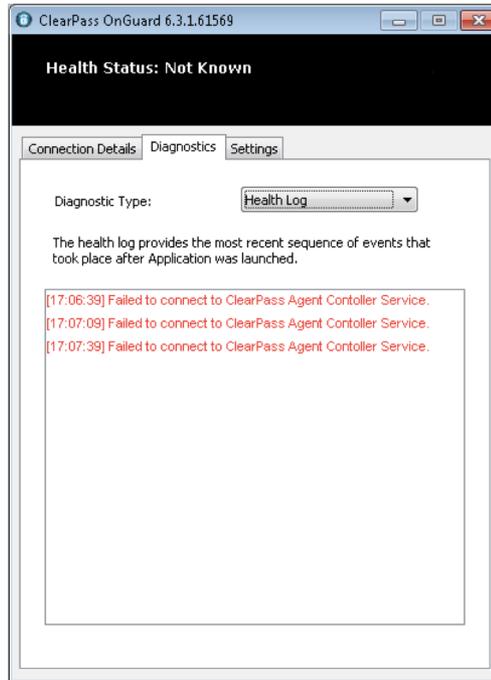
Use the OnGuard Settings page to configure the OnGuard agent deployment packages for Windows, macOS, and Ubuntu.

Settings	Installers
Agent Version:	6.7.7.109065
Agent Library Version:	1.0.7.109065
Installer Mode:	<p>Do not install/enable Aruba VIA component </p> <p>Agent will be used only to authenticate/perform health checks for client machines. This setting will not install the Aruba VIA component. If already installed, then the VIA component will be disabled on the client machine.</p> <p><b>Note: This WILL remove any existing/installed Aruba VIA client</b></p>
<b>Agent Customization</b>	
Managed Interfaces:	<input checked="" type="checkbox"/> Wired <input checked="" type="checkbox"/> Wireless <input checked="" type="checkbox"/> VPN <input type="checkbox"/> Other
Mode:	<p>Authenticate with health checks </p> <p>Authentication type: <input type="text" value="Username &amp; Password"/> </p> <p>Username Text: <input type="text" value="Username"/></p> <p>Password Text: <input type="text" value="Password"/></p>
Agent action when an update is available:	<input type="text" value="Ignore"/> 
<b>Agent Remediation User Interface Customization</b>	
Custom User Interface:	<input type="checkbox"/> Configure
<b>Native Dissolvable Agent Customization</b>	

## Cont.. (OnGuard Frontend is not able to communicate with the Backend Service )

- ❖ **OnGuard Frontend is not able to communicate with the Backend Service** - The Backend Service is running but the communication between the OnGuard Frontend and Backend may be blocked.



## This can happen because of the following reasons:

- ❖ Port #25427 is being used by another application. Use TCPView (Windows) or the netstat command (Mac OS X) to see the open ports and the applications that are using them.
- ❖ AntiVirus/Firewall is blocking the local TCP Communication between the Frontend and the Backend. Check the AntiVirus/Firewall logs to see if they are blocking **ClearPassAgentController.exe**, **ClearPassOnGuard.exe**, or the ClearPass OnGuard ServiceDaemon processes.

## Resolutions:

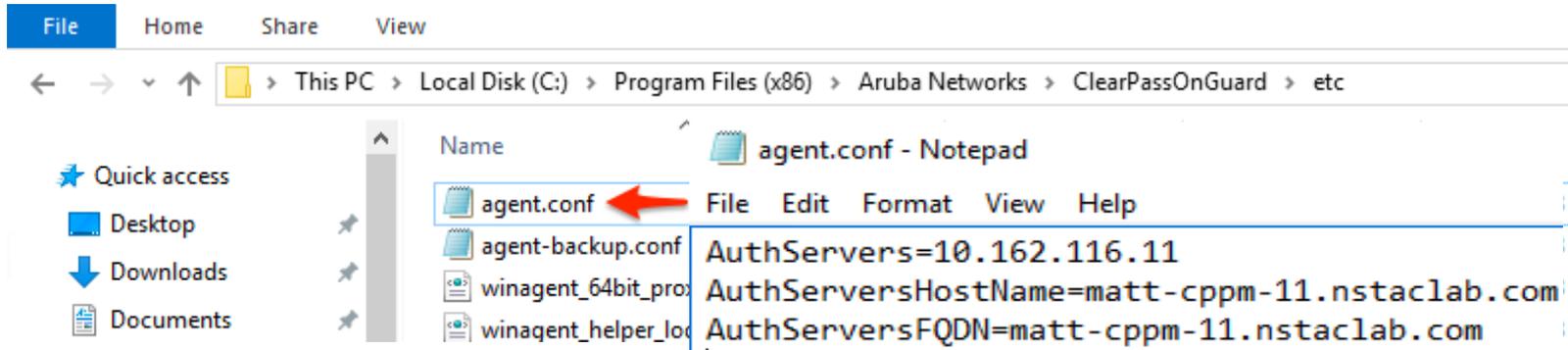
- ❖ Uninstall the application using Port #25427, and restart the client.
- ❖ Close the application using Port #25427, and restart the Backend Service.
- ❖ Whitelist the OnGuard Processes or add them to the Exclude list of any AntiVirus/Firewall application installed.

# Cont.. (CPPM Server IP is changed)

- ❖ **CPPM Server IP is changed** - OnGuard Agent will not work if the CPPM Server's IP has changed. OnGuard Agent will continue to try to connect to the old IP Address.

## Resolution - This issue can be fixed by:

- ❖ Reinstalling the OnGuard Agent downloaded from the CPPM Server with the new IP Address.
- ❖ Changing the IP Address in the Agent Configuration file.



## Cont.. (Agent Configuration file is corrupt)

- ❖ **Agent Configuration file is corrupt** - Sometimes the Agent Configuration file gets corrupted when the client machine is shut down abruptly. If the Agent Configuration file is corrupt, the OnGuard Agent will not have the CPPM Server's IP Address.

### **Resolution:**

- ❖ Reinstall the OnGuard Agent.
- ❖ Copy the Agent Configuration file from a working client machine.

## 2. ClearPass OnGuard Agent bounces the Network Interface

**ClearPass OnGuard Agent uses Port #6685 to establish the Control Channel with the CPPM Server.**

If Port #6658 is not allowed then the OnGuard Agent fails to establish the Control Channel with CPPM. OnGuard Agent will try to establish the Control Channel multiple times. If it is not able to establish the Control Channel within 150 seconds, it treats it as an Interface Down or CPPM Server is unreachable and starts the health checks again. This whole sequence takes approx. 3 minutes; and in Access Tracker, a WebAuth request is seen after every ~3 minutes.

**Resolution - Add Port #6658 to the allowed Ports list.**

### 3. ClearPass OnGuard Agent shows Healthy WebAuth Request is seen in Access Tracker

- ❖ From 6.3.0, a new option 'Health Check Interval' was added in the Global Agent Settings. **Note: The same option is also available in the Agent Enforcement Profile.**
- ❖ If the 'Health Check Interval' is set and client is healthy, then the OnGuard Agent will not perform Health Checks and no WebAuth request is sent to the CPPM Server.
- ❖ This behaviour is as per design and not an issue.

**Verify** - Verify on the CPPM Server that the Health Check Interval is enabled or not.



Name	Value
1. OnGuard Health Check Interval (in hours)	= 6
2. Cache Credentials Interval(in days)	= 15
3. <i>Click to add...</i>	

Configuration » Enforcement » Profiles » Add Enforcement Profile

#### Enforcement Profiles



Profile	Attributes	Summary
Attribute Name		Attrib
1. Bounce Client	=	false
2. Health Check Interval (in hours)	=	6
3. <i>Click to add...</i>		

# Cont..

- ❖ Use session timeout in the Agent Enforcement profile, if you need the agent to perform health check after certain interval.

Configuration » Enforcement » Profiles » Add Enforcement Profile

## Enforcement Profiles

Profile   **Attributes**   Summary

	Attribute Name		Attribute Value
1.	Bounce Client	=	false
2.	Session Timeout (in seconds)	=	10800 
3.	<i>Click to add...</i>		

## 4. Auto-Remediation does not work and the client remains Unhealthy

- ❖ **Sometimes the OnGuard Agent does not perform the auto-remediation and asks the user to perform the auto-remediation tasks manually.**

**Verify** - Auto-Remediation is enabled on the CPPM Server.

On the CPPM Server, there are 2 flags, which control the auto-remediation of health classes:

- Global Remediation Flag** - This flag is present in the Service Configuration and controls auto-remediation at the Service Level. If this flag is FALSE, then the OnGuard Agent will not perform the auto-remediation for any of the health classes.
- Health Class Level Remediation Flag** – In Posture Policy, there is a remediation flag for each health class. This flag is used to control the remediation of individual health classes, as highlighted below.

# Cont..

- ❖ If auto-remediation flags are configured properly, then check in Third-Party Support Charts that OnGuard Agent supports auto-remediation for that product.

To Access Third-Party support chart – Navigate to ClearPass Policy Manager → Administration → Support → Documentation → OnGuard Agent Support Charts.

<b>OnGuard Agent Library Version - 1.0.7.109065</b>					
Created On - Tue Oct 9 14:16:17 2018			SDK Version - 4.3.344.0		
Product Name	Tested Points	GetAgentState	GetMissingPatches	InstallMissingPatches	SetAgentState
<b>Microsoft Corporation</b>					
Microsoft Intune Client	5.0.5182.0	X	X	X	X
System Center Configuration Manager Client	5.0.7859.1000	V	V	V	V
System Center Configuration Manager Client	4.00.6487.2157	V	V	V	V
System Center Configuration Manager Client	4.00.6487.2000	V	V	V	V
System Center Configuration Manager Client	5.00.8634.1000	V	V	V	V
Windows Update Agent	7.6.7600.256	V	V	V	V
Windows Update Agent	10.0.10240.16384	V	V	V	V

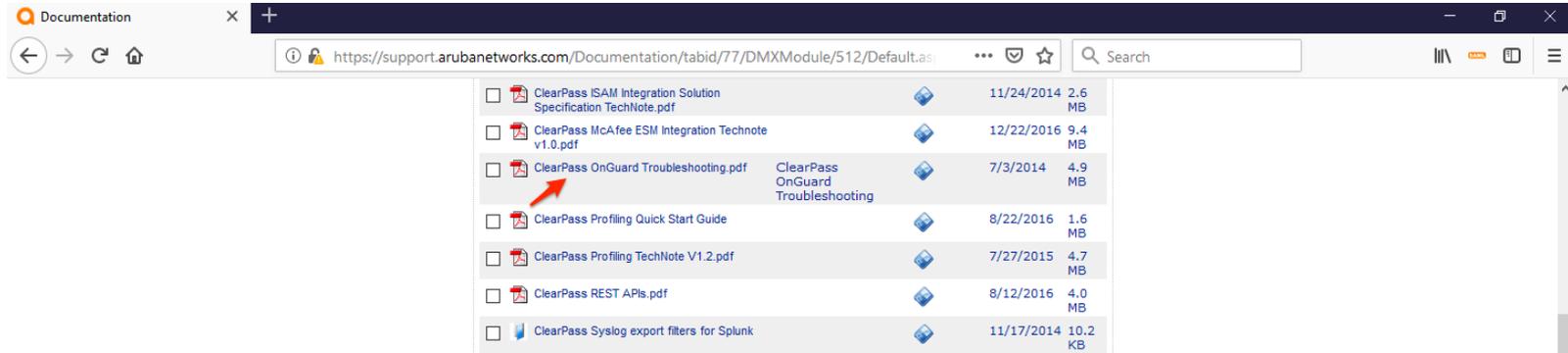
# Troubleshooting Guide

## ClearPass OnGuard Troubleshooting Guide:

Reference Link -

<https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=33093>

Navigation: Support → Documentation → Software User & Reference Guides → ClearPass → Policy Manager → Tech Notes → “ClearPass OnGuard Troubleshooting.pdf”.



QUESTIONS?

THANK YOU!