

# ClearPass

# **OnGuard Troubleshooting**

	<u>Date</u>	Modified By	Comments
0.1	March 11 <sup>th</sup> , 2014	Deepak Jain	Initial Draft Version
0.2	May, 20 <sup>th</sup> , 2014	Deepak Jain	Updated document based on review comments
0.9	June 8 <sup>th</sup> 2014	Danny Jump	Edits and updates for Draft Release
1.0	July 3 <sup>rd</sup> 2014	Danny Jump	Full V1 Release

# **Table of Contents**

Overview4
Introduction4
ClearPass OnGuard Agent Components4
Communication between ClearPass OnGuard Agent Components and CPPM Server7
ClearPass OnGuard Agent Installation8
Language Selection
Post Installation9
Launching OnGuard Agent9
Health Monitoring and Auto-Remediation10
Health Collection Interval for Each Health Class10
Health Checks and Auto-Remediation11
Troubleshooting ClearPass OnGuard13
OnGuard Health Log View
Troubleshooting Common Issues15
ClearPass OnGuard Agent does not start health checks automatically
ClearPass OnGuard Agent bounces the Network Interface and performs health checks every 3 minutes
ClearPass OnGuard Agent shows Healthy and connects to the Network but no WebAuth Request is seen in Access Tracker
Network Interface is bounced a few minutes after OnGuard Agent is closed
Auto-Remediation does not work and the client remains Unhealthy
ClearPass OnGuard Agent Flow
Read CPPM Server IP Address List
Establish Connection with Backend Service30
Active Network Interface List

Auth Server Discovery	37
CPPM Server Reachability Check	37
Select Auth Server	40
Wait For Credentials	44
Collect Health	47
Send WebAuth to CPPM Server	50
Process WebAuth Response	51
Agent Enforcement Actions	61
Establish Control Channel	64
Monitor Health State & Soft Re-Auth	66
Automatic Remediation	69
Retry	71
Logout	75
Quit	82
Third-Party Application Logs	84
Appendix A – Tools and Utilities	
Appendix B – References	

# **Overview**

The following guidance has been produced to aid customers and partners to troubleshoot and fix common ClearPass **OnGuard Agent** issues. This guide covers troubleshooting of Windows and Mac OS X OnGuard Persistent Agent but does not cover troubleshooting of OnGuard Dissolvable.

# Introduction

# **ClearPass OnGuard Agent Components**

ClearPass OnGuard<sup>™</sup> agent has multiple components like **Backend Service**, User Interface (will be referred as Frontend), etc. Each of these components perform specific functions. It is important to understand what these components are, what are their main functions are, and the log files created by these component in order to effectively troubleshoot issues.

ClearPass **OnGuard Agent** has the following main components:

 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 provides the ability to users to start health checks, connect/disconnect VPN Connection, 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"

🔋 ClearPass OnGuard 6.3.1.61950		ClearPass OnGuard 6.3.1.61950	- 🗆 🗡	🔋 ClearPass OnGuard 6.3.1.61950
Network category Not Determined Connection Status Authenticating Health Status: Not Known		Network category Not Determined Connection Status Authenticating Health Status: Not Known		Network category Not Determined Connection Status Authenticating Health Status: Not Known
Summary Details Diagnostics Settings		Summary Details Diagnostics Settings		Summary Details Diagnostics Settings
Connection Status: VPN: Trusted Network: Not K	Not Connected	Change Detail Type Health Checks		Change Detail Type Connection Cetails
Local Network : Wire Details IP Details IP Ac Mask Gate	d Idress : 10.20.23.123 : 255.255.255.0 way : 10.20.23.254	INFO:Response processed		Remote Server:         Not Available         Download           Assigned IP / Mask:         Not Available         Packet Traffic:         0 / 0
Health		12:33:45 Test Authentication failed	1	Connected time / Max session time: 00:00:00 / 00:00:00 Network Details
Health Status: Not I	Known	12:30:52 Started new Session		Connected Network: Wired
Details				Signal: / 100 Mbps Local IP / Mask: 10.20.23.123 / 255.255.255.0
Send Logs		Health Log Send Logs	×	Connection Log Send Logs

**Figure 1 - Windows GUI Summary** 

### Mac OS X:

- Process Name ClearPassOnGuard
- Installation Path /Applications/ClearPassOnGuard.app
- Log file ~/Library/Logs/ClearPassOnGuard/ClearPassOnGuard\_\*.log

⊖ ○ ClearPass OnGuard	⊖ ○ ClearPass OnGuard
Please download the profile from preferences VPN	Please download the profile from preferences VPN
Not Connected     Connect       Not Connected     Connect       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences       Image: Connect and the prome from preferences     Image: Connect and the prome from preferences	Not Connected       Connect         Not Connected       Connect         Image: Connect and the prome from preferences       Image: Connect and the prome from preferences         Image: Connect and the prome from preferences       Image: Connect and the prome from preferences         Image: Connect and the prome from preferences       Image: Connect and the prome from preferences         Image: Connect and the prome from preferences       Image: Connect and the prome from preferences         Image: Connect and the prome from preferences       Image: Connect and the prome from preferences         Image: Connect and the prome from preferences       Image: Connect and the prome from preferences         Image: Connect and the prome from prom prome from prome from prome from prome from prom prome from prom
Send Logs	Send Logs

Figure 2 - OSX GUI Summary

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.

### 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"

### Mac OS X:

- Daemon Name com.arubanetworks.servicedaemon
- Process Name ServiceDaemon
- Daemon Path /Library/LaunchDaemons/com.arubanetworks.servicedaemon.plist
- Binary Path /Applications/ClearPassOnGuard.app/Contents/PlugIns/ OnGuard.bundle/Contents/MacOS/ServiceDaemon
- Log file /Library/Logs/ClearPassOnGuard/macagent\_backend \_\*.log

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

### Mac OS X:

- File Name OnGuard.bundle
- Path /Applications/ClearPassOnGuard.app/Contents/PlugIns/OnGuard.bundle
- Log file ~/Library/Logs/ClearPassOnGuard/ClearPassOnGuard\_\*.log
- 4. ClearPass Universal Sytem 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

## Mac OS X:

On Mac OS X, there is no separate process for USHA Remediate. ServiceDaemon performs autoremediation also.

- Process Name ServiceDaemon
- Path /Applications/ClearPassOnGuard.app/Contents/PlugIns/ OnGuard.bundle/Contents/MacOS/ServiceDaemon
- Log file /Library/Logs/ClearPassOnGuard/macagent\_remediate \_\*.log
- 5. **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

### Mac OS X:

- Process Name ClearPassAgentHelper
- Path /Applications/ClearPassOnGuard.app/Contents/PlugIns/ OnGuard.bundle/Contents/MacOS/ClearPassAgentHelper
- Log file /Library/Logs/ClearPassOnGuard/ClearPassAgentHelper\_\*.log

6. **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
- 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

# Mac OS X:

- File Name agent.conf
- Path /Library/Application\ Support/ClearPassOnGuard/agent.conf

# Communication between ClearPass OnGuard Agent Components and CPPM Server

The **OnGuard Plugin** connects to **Backend Service** on TCP Port #25427, the **OnGuard Plugin** uses https (Port #443) to send WebAuth Request to CPPM Server. In turn, CPPM Server replies WebAuth Response, which contains health evaluation results.

Note: OnGuard Plugin also uses CPPM Server's Port #6658 to establish Control Channel.

# **ClearPass OnGuard Agent Installation**

ClearPass **OnGuard Agent** Installers for Windows and Mac OS X can be downloaded from CPPM Server **(Administration -> Agents and Software Updates -> OnGuard Settings)**. For Windows, both EXE and MSI Installers are available. For Mac OS X, it's a DMG file.

As part of the installation, these installers create Agent Config (agent.conf) file, which contains CPPM Server IP Addresses. If CPPM Servers are in a cluster, then this list has IP Addresses of all the nodes in the cluster. If it's a stand-alone Server then this list contains the IP Address of the CPPM Server from which installer was downloaded.

The Installer starts the **Backend Service**, on both Windows and Mac OS X, after installation is over.

# Language Selection

ClearPass **OnGuard Agent** supports English and Japanese Languages as of the CPPM 6.3.x release.

# Windows:

Windows Installer presents a dialog to the user to select Language.



Figure 3 - Language installation selection

# Mac OS X:

On Mac OS X, there is no option in Installer to select Language. OnGuard uses current user's Language to select either English or Japanese Language.

OnGuard uses English for all the languages other than Japanese.

# **Post Installation**

OnGuard Installer installs all the required services (**Backend Service**/Daemon, VPN Service, etc.) and starts them. Post Installation, all these services are expected to be in a running state.

# Launching OnGuard Agent

## Windows:

On Windows, the User is shown an option to launch **OnGuard Frontend** after Installation is complete.



Windows Shortcuts are added on the Desktop and "**All Programs -> Aruba Networks -> ClearPass OnGuard**" to launch **OnGuard Agent** manually.

Also, **OnGuard Agent** is added in Startup item so that it is started automatically when the User logs in.

## Mac OS X:

On Mac OS X, **OnGuard Frontend** is launched automatically, after the installation is completed.

ClearPass **OnGuard Agent** is added to 'Applications' and also added as a Startup Agent for starting OnGuard automatically.

# **Health Monitoring and Auto-Remediation**

The **OnGuard Agent** continuously monitors the client health state. Whenever a change in health state is detected, OnGuard starts the health check (Refer to section '<u>Monitor Health State & Soft Re-Auth'</u> for more details).

The **Backend Service** caches the health of each health class for a predefined time (non-configurable). When the cached health of a health class expires, it collects health again.

# **Health Collection Interval for Each Health Class**

The period after which **Backend Service** collects the health status of each health class is given in table below:

Health Class Name	Health Cache Duration
Services	30 Seconds
Firewall	1 Minute
AntiVirus	1 Minute
AntiSpyware	1 Minute
P2P	1 Minute
Processes	30 Seconds
Registry Keys	30 Seconds
Patch Management	1 Minute (Status)
	1 Hour (Missing Patches)
Windows Hotfixes	1 Minute
USB Devices	30 Seconds
Virtual Machines	1 Minute
Network Connections	30 Seconds
Disk Encryption	5 Minutes
Installed Applications	5 Minutes
Windows Security - Firewall	1 Minute

Windows Security - AntiVirus	1 Minute
Windows Security - AntiSpyware	1 Minute
Windows Security - Automatic Updates	30 Seconds
Windows Security – Security Updates	1 Hour

# Health Checks and Auto-Remediation

Following table shows which application (**Backend Service** or **USHA Remediate**) handles autoremediation of which health check/health class:

Health Class Name	Health Check	Auto-Remediation Done By
Services	Start/Stop Services	Backend Service
Firewall	Change Status	Backend Service
AntiVirus	Set RTP Status, Dat File Update, Full System Scan	USHA Remediate Application
AntiSpyware	Set RTP Status, Dat File Update, Full System Scan	USHA Remediate Application
P2P	Terminate Application	Backend Service
Processes	Start/Stop Processes	Backend Service
Registry Keys	Create/Delete Registry Keys	Backend Service
Patch Management	Change Status	Backend Service
5	Install Missing Patches	USHA Remediate Application
Windows Hotfixes	Install Missing Hotfixes	USHA Remediate Application
USB Devices	Disable/Eject USB Device	USHA Remediate Application
Virtual Machines	Stop Guest VM, Pause Guest VM	USHA Remediate Application (uses Agent Helper application)
Network Connections	Disable Network Connection, Disable ICS, Stop Hosted Wireless Network, Disconnect Adhoc Wireless Network	USHA Remediate Application

Disk Encryption	-	Auto-Remediation Not Supported
Installed Applications	-	Auto-Remediation Not Supported
Windows Security - Firewall	Enable Firewall	Backend Service
Windows Security - AntiVirus	Enable/Update	USHA Remediate Application
Windows Security - AntiSpyware	Enable/Update	USHA Remediate Application
Windows Security - Automatic Updates	Enable	Backend Service
Windows Security –	Enable	Backend Service
Security Updates	Install Security Updates	USHA Remediate Application

This information is required to know whether we should look in **Backend Service** Logs or USHA Application Logs for auto-remediation.

**Note:** OnGuard does not support Auto-Remediation of following health checks/health classes:

- a) Installed Application Health Class
- b) Disk Encryption Health Class
- c) Install Product Product is not installed
- d) Upgrade Product Product Version does not match



# **Troubleshooting ClearPass OnGuard**

This section covers basic troubleshooting steps to debug some of the common OnGuard related issues. Please take special notice of the new Health Log information as noted below.

# **OnGuard Health Log View**

**Note:** In **6.3.1**, a new diagnostic view 'Health Log' was added to **OnGuard Agent**. This view displays OnGuard related logs. For easy differentiation between error, warning and normal messages, following color coding is used:

Error Messages – Red color Warning Messages – Orange color Normal Messages – Black color

Below are snap-shots of Windows and Mac **OnGuard Agent**'s Health Log View:

🔞 ClearPass OnGuard 6.3.1.61569 💼 📼	🖸 ClearPass OnGuard 6.3.1.61569 📃 📼 💌
Health Status: Healthy	Health Status: Healthy
Connection Details Diagnostics Settings	Connection Details Diagnostics Settings
Health Status: Healthy Logout INFO:Response processed	Diagnostic Type: Health Log  The health log provides the most recent sequence of events that took place after Application was launched.
17:28:45 You are connected to network!	<ul> <li>[17:25:27] Connection to ClearPass Agent Contoller Service establist</li> <li>[17:25:27] Detected New Interface: IfName=Local Area Connection I</li> <li>[17:25:28] Local Area Connection (WIRED) is managed by Server.</li> <li>[17:25:28] Local Area Connection: ClearPass Server reachable = 10</li> <li>[17:25:28] Local Area Connection: Started collecting health information</li> <li>[17:25:47] Local Area Connection: Processing response</li> <li>[17:25:52] Local Area Connection: Health status - Healthy.</li> <li>[17:25:52] Local Area Connection: Started collecting health information</li> </ul>
Health Log Send Logs	[17:25:54] Local Area Connection: Health status - Healthy. [17:25:54] Local Area Connection: Authentication successful [17:25:54] Local Area Connection: Health status - Healthy.

#### Figure 4 Windows OnGuard - Health Logs

⊖ ○ ClearPass OnGuard			
Authentication failed Remediation Messages	OnGuard Login Retry v Health Logs		
7:16:02 J eno: watting for Credentials. 7:16:11 ] en0 (WIRED) is managed by Ser 7:16:11 ] en0: ClearPass Server reachable 7:16:11 ] en0: Started collecting health ir 7:16:12 ] en0: Sending authentication red 7:16:13 ] en0: Processing response 7:16:13 ] en0: Processing health respons 7:16:13 ] en0: Authentication failed	ver. e = 10.17.4.199 nformation quest e failed		
	Send Logs		

Figure 5 Mac OnGuard – Health Logs

Many common issues like CPPM Server is not reachable, **Backend Service** is not running, etc. can be identified using the Health Logs view.

# **Troubleshooting Common Issues**

For troubleshooting OnGuard issues, Health Logs should be checked first to rule out the basic common issues like Network Connectivity, etc.

Some of the common OnGuard issues and troubleshooting tips are covered below.

# **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.

🔞 ClearPass OnGuard 6.3.1.61950	
Health Status: Not Known	
Connection Details Diagnostics Settings	
Initializing Not Connected	Login Retry
	4
Health Log	

Figure 6 OnGuard stuck at Initializing

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

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

ClearPass OnGuard 6.3.1.61569
Health Status: Not Known
Connection Details Diagnostics Settings
Diagnostic Type:
The health log provides the most recent sequence of events that took place after Application was launched.
[17:59:47] Successfully connected to ClearPass Agent Contoller Servic [17:59:47] No Active Network Connection found. [17:59:47] Connection to ClearPass Agent Contoller Service established

Figure 7 OnGuard - No Active Network Connection

**Resolution** – Connect client to Wired/Wireless Network. Once the client is connected, the **OnGuard Agent** should start communicating with the CPPM Server.

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

O ClearPass OnGuard 6.3.1.61569
Health Status: Not Known
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.
[18:01:46] Successfully connected to ClearPass Agent Contoller Servic
[18:01:46] Connection to ClearPass Agent Contoller Service established
[18:02:01] Local Area Connection: ClearPass Server is not reachabl
[18:02:46] Local Area Connection: ClearPass Server is not reachabl
[18:03:31] Local Area Connection: ClearPass Server is not reachabl

Figure 8 OnGuard - CPPM Server Not Reachable

**Resolution** – Connect the client to the correct network/VLAN which has connectivity to the CPPM Server. Verify that the client is able to ping the CPPM Server. Also verify that the CPPM Server is not down.

3. **Network Interface is not managed by CPPM Server** – Current Network Interface is not managed by the CPPM Server.

🛈 ClearPass OnGuard 6.3.1.61569 📃 🔲 🗾
Health Status: Not Known
Connection Details Diagnostics Settings
Diagnostic Type:
The health log provides the most recent sequence of events that took place after Application was launched.
[17:10:35] Successfully connected to ClearPass Agent Contoller Service
[17:10:36] Connection to ClearPass Agent Contoller Service established
[17:10:36] Detected New Interface: IfName=Local Area Connection IfTyk
[17:10:37] Local Area Connection (WIRED) is not managed by Server.

Figure 9 OnGuard - Unmanaged Network Interface

**Resolution** – Change the CPPM Server configuration to allow Network Interface type or connect client via allowed Network Interface Type.

dministration » Agents a	and Software Updat	es » OnGuard Settings –				
OnGuard Setting	js -		📴 Global Age 📴 Policy Mar	ent Settings Jager Zones		
Agent Version:	6.2.6.62196					
Agent Installers						
Agent Installers update	ed at May 21, 2014 :	18:15:22 IST				
Installer Mode:	Do not install/e	nable Aruba VIA component 👻				
	Agent will be u Aruba VIA com Note - This W	ised only to authenticate / perform health checks for client ma ponent. If already installed, then the VIA component will be dis ILL remove any existing/installed Aruba VIA client	chines. This setting will no sabled on the client machi	ot install the ne.		
🎥 Windows	http://10.17.4	.199/agent/installer/windows/ClearPassOnGuardInstall.exe	(Full Install - EXE)	16MB		
	http://10.17.4	.199/agent/installer/windows/ClearPassOnGuardInstall.msi	(Full Install - MSI)	17MB		
🧉 Mac OS X	http://10.17.4	.199/agent/installer/mac/ClearPassOnGuardInstall.dmg	(Full Install)	9MB		
Agent Customization						
Managed Interfaces:		🕅 Wired 🗹 Wireless 🗹 VPN 📄 Other				
Mode:		Check health - no authentication				
Client Certificate Check	k:	Enable to use a certificate from User keystore during auther	ntication			
Agent action when an	update is available:	Ignore				
External Captive Port	al Support					
Enter the URL of a web device that is configure	page that can be a ed for captive porta	accessed only after a successful authentication (e.g., http://w -based authentication redirects requests to this URL to an auth	ww.arubanetworks.com). hentication page.	A network		
-						

**Figure 10 CPPM - Managed Interfaces** 

4. Backend Service is not running/stopped – OnGuard Backend service is stopped.



Figure 11 OnGuard - Backend Service Not Running

**Resolution** – Start **Backend Service** manually. On Windows OS, use Windows Service Manager. For Mac OS X, refer point 5 of <u>Appendix A</u>.

Another option is to restart the client (**Backend Service** starts automatically when the client is started).

5. **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 is blocked.

🛈 ClearPass OnGuard 6.3.1.61569 📃 📼 💌
Health Status: Not Known
Connection Details Diagnostics Settings
Diagnostic Type:
The health log provides the most recent sequence of events that took place after Application was launched.
[17:06:39] Failed to connect to ClearPass Agent Contoller Service.
[17:07:09] Failed to connect to ClearPass Agent Contoller Service.

Figure 12 OnGuard - Backend Service Not Running

This can happen because of the following reasons:

- a. 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.
- b. 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 ClearPassOnGuard ServiceDaemon processes.

### **Resolution** -

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

6. **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:

- a. Reinstalling the **OnGuard Agent** downloaded from the CPPM Server with the new IP Address.
- b. Changing the IP Address in the Agent Configuration file. Refer to the section <u>ClearPass</u> <u>OnGuard Agent Components</u> for the Agent Configuration file paths.
- 7. **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** -

- c. Reinstall the **OnGuard Agent**
- d. Copy the Agent Configuration file from a working client machine. Refer to the section <u>ClearPass OnGuard Agent Components</u> for the Agent Configuration file paths.

# **ClearPass OnGuard Agent bounces the Network Interface and performs health checks every 3 minutes**

ClearPass **OnGuard Agent** uses Port #6685 to establish the Control Channel with the CPPM Server. Refer to the section <u>Establish Control Channel</u> for details.

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.

# ClearPass OnGuard Agent shows Healthy and connects to the Network but no WebAuth Request is seen in Access Tracker

In 6.3.0, a new option 'Health Check Interval' was added in the Global Agent Settings; and the same option was added in the Agent Enforcement Profile in 6.3.1.

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 behavior is as per design and not an issue.

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

# Network Interface is bounced a few minutes after OnGuard Agent is closed

Refer <u>Quit</u> section for the **OnGuard Agent**'s behavior post quit.

# 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.

🔞 ClearPass OnGuard 6.3.1.61950	
Health Status: Quarantined	
Connection Details Diagnostics Settings	1
Health Status: Quarantined INFO:Response processed	Logout Retry
Firewall Check: Enable Microsoft Windows Firewall 16:00:59 Started new Session Show Old Sessions	
Health Log Send Logs	~

Figure 13 OnGuard - Auto-Remediation failed

**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:
- a) **Global Remediation Flag** This flag is present in the Service Configuration and controls autoremediation 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.

Configuration »	Services » E	dit - health	i-only		
Services -	health-o	only			
Summary	Service	Roles	Posture	Enforcement	
Posture Polic	ies:				
Posture Policie	:5:	Only On( windows mac -Select	Guard agent t	ype posture polici	cies are applicable for this service       Remove     Add new Posture Poli       View Details     Modify
Default Postur	e Token:	QUARA	NTINE (20)	•	
Remediate Enc	l-Hosts:	🗵 Enable	e auto-remed	ation of non-comp	npliant end-hosts
Remediation U	RL:				
Posture Serv	ers:				
Posture Serve	rs:	-Select	to Add–		Remove     Add new Posture Server       View Details     Modify
< Back to S	ervices				Disable Copy Save Cance

Figure 14 WebAuth Service - Remediation Flag

b) 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.

ClearPass Windows Univers	al System Health Validator			8
Windows Server 2003 🛛 👩	Enable checks for Window	vs 7		
Windows XP 📀				
Windows Vista 🛛 👩	Remediation checks	Auto Remediation	Vser Notification	
Windows 7	Product-specific checks	(Uncheck to allow any product)		
A Services				Add
Brasses	Firewall Product Name		Product Ver	rsion 💼
Processes	Microsoft Windows Firewall		no check	<u> </u>
C Registry Keys				
Ω AntiVirus				
🗘 AntiSpyware				
🔅 Firewall				
🛱 Peer To Peer				
🛱 Patch Management				
🛱 Windows Hotfixes				
💭 USB Devices				
🛱 Virtual Machines				
🛱 Network Connections				
Disk Encryption				
Windows Server 2008 🛛 👩				
Windows 8 🛛 🕔				
Quarantine Message				
Reset			Save	Cancel

Figure 15 Firewall Health Class - Remediation Flag

The **OnGuard Agent** performs auto-remediation for a health class only if both Global and Health class Remediation Flags are TRUE.

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

To open Third-party Support Charts - In CPPM go to *Administration > Agents and Software Updates > OnGuard Settings*, click the Help link, and then click the *OnGuard Agent Support Charts* link (Refer [7] in <u>Appendix B - References</u> on how to read/interpret Support Charts for auto-remediation).

For example, in below snap-shot, we can see that *SetRTP* and *FullSystemScan* are not supported for "avast! Free AntiVirus 2014.x".

Product Name	Version	GetDataFileTime	GetDataFileVers	EngineVersion	Check RTP	LiveUpdate	Sync/Async Update	Set RTP	LastScanTime	FullSystemScar	GetVirusDefServ	IsFullScanInProg
avast! Endpoint Protection Suite Plus	7.x	V	V	0	V	V	V	V	V	х	۷	V
avast! Endpoint Protection Suite Plus	8.x	V	V	0	V	V	V	V	х	х	V	V
avast! File Server Security	7.X	V	V	0	х	V	V	х	V	х	٧	V
avast! Free Antivirus	2014.x	۷	۷	Х	۷	х	Х	Х	۷	х	х	X
avast! Free Antivirus	5.x	V	V	х	V	V	V	х	х	V	V	Х
avast! Free Antivirus	6.x	V	V	х	V	V	V	V	х	V	۷	Х
avast! Free Antivirus	7.x	V	V	0	V	V	V	V	V	X	٧	V
avast! Free Antivirus	8.x	۷	۷	Х	۷	V	۷	Х	V	Х	Х	х

Figure 16 AntiVirus Support Chart

If auto-remediation is not supported or supported but **OnGuard Agent** is not able to perform autoremediation then contact Aruba TAC Support with **OnGuard Agent** logs to analyze the issue.

Also refer section <u>Auto-Remediation</u> for more information.

# **ClearPass OnGuard Agent Flow**

This section explains **OnGuard Agent** Flow from the moment it is launched, till the health checks are over and after that how it monitors client's health state going forward.





# **Read CPPM Server IP Address List**

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

## OnGuard Plugin Logs (Read CPPM Server List Successful):

2014-03-12 11:02:22,356 [Th 1988:3360] INFO OnGuardPlugin.AgentResourceHolder - <mark>LoadAuthServerList: Auth Server List -</mark> <mark>10.17.4.198</mark>

ClearPassOnGuard_0.log (20.7 KB) - BareTail	
Elle Edit View Preferences Help	
😂 Open 🤌 Highlighting 🔽 Follow Tail ANSI 🔄 C:\Users\Deepak\AppData\Roaming\Anba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (20.7 KB)	
ClearPassOnGuard_0.0g V whagert_0.0g V	< > X
02014-03-12 12:24:51,629 [Th 5616:5620] INFO OnGuardPlugin - InitializeLogger: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard.exe	
02014-03-12 12:24:51,629 [Th 5616:5620] INFO OnGuardPlugin.OnGuardPlugin - COnGuardPlugin: Constructor called	
o 2014-03-12 12:24:51,629 [Th 5616:5620] INFO OnGuardPlugin.OnGuardPlugin - AddRef: m lRefCount - 1	
o 2014-03-12 12:24:51,634 [Th 5616:5620] INFO OnGuardPlugin.OnGuardPlugin - Initialize: called	
02014-03-12 12:24:51,635 [Th 5616:5620] DEBUG Common.TextStore - LoadResourceManager: Resource Manager DLL Loaded Succesfully	
2014-03-12 12:24:51,636 [Th 5616:5620] INFO OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Auth Server List - 10.17.4.234	
2014-03-12 12:24:51,636 [Th 5616:5620] INFO OnGuardPlugin.AgentResourceHolder - SetAuthServerList: AuthServerList size - 1	
02014-03-12 12:24:51,636 [Th 5616:5620] INFO OnGuardPlugin.AgentResourceHolder - LoadUserSettings: User Settings file - C:\Users\Deepak\AppData\Roamin	ig\On(
02014-03-12 12:24:51,637 [Th 5616:5620] INFO OnGuardPlugin.AgentResourceHolder - LoadHealthStateInfoData: Health State Info file - C:\Users\Deepak\App	Data\
02014-03-12 12:24:51,637 [Th 5616:5620] ERROR OnGuardPlugin.AgentResourceHolder - LoadHealthStateInfoData: Cannot open Health State Info file - C:\User	:s\Dee
02014-03-12 12:24:51,637 [Th 5616:5620] INFO OnGuardPlugin.AgentThread - Start: AgentController Thread created successfully.	
02014-03-12 12:24:51,637 [Th 5616:5620] DEBUG OnGuardPlugin.AgentController - Start: Controller Thread created	<b>T</b>

The Agent Configuration file is created by **OnGuard Agent** Installer and then updated by **Backend Service** periodically.

For Agent Config file paths, refer point #7 in <u>ClassPass OnGuard Agent Components</u> section.

If the **OnGuard Agent** fails to read the CPPM Server IP List from Agent Config file then it will **not** start the health checking functionality and OnGuard UI will show 'Initializing...".

## OnGuard Plugin Logs (Read CPPM Server List Failed):

2014-03-12 11:27:22,221 [Th 2956:164] ERROR OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Execption - Cannot open property file C:\Program Files\Aruba Networks\ClearPassOnGuard\etc\agent.conf 2014-03-12 11:27:22,222 [Th 2956:164] ERROR OnGuardPlugin.AgentResourceHolder - Init: LoadAuthServerList failed 2014-03-12 11:27:22,222 [Th 2956:164] ERROR OnGuardPlugin.AgentResourceHolder - Init: LoadAuthServerList threw exception 2014-03-12 11:27:22,222 [Th 2956:164] ERROR OnGuardPlugin.OnGuardPlugin - Initialize: Exception caught while Intializing Agent Plugin.

🚺 Clea	irPa	ssOnG	uard_0	.log (1.1	KB) - B	areTail			- O ×
<u>File</u>	dit	⊻iew	Preferer	nces <u>H</u> el	р				
😂 Оре	m	🌽 Hig	hlighting	🔽 Folk	<u>w</u> Tail	ANSI	-	:/Users/Deepak/AppData/Roaming/Aruba Networks/ClearPassOnGuard/ClearPassOnGuard_O.log (1.1 KB)	
ClearP	ass	OnGua	rd_0.loį	<b>] ● [</b> w	inagent_	0.log 🔻			X
0 201	4-0	3-12	12:2	2:00,6	72 [1	h 5056:5	5060] IN	OnGuardPlugin - InitializeLogger: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard.exe	-
0 201	4-0 4-0	13-12 13-12	12:2	2:00,6 2:00,6	72 [] 72 []	n 5056:5 h 5056:5	5060] IN 5060] IN	) OnGuardPlugin.OnGuardPlugin - COnGuardPlugin: Constructor called ) OnGuardPlugin.OnGuardPlugin - AddRef: m_lRefCount - 1	
0 201	4-0 4-0	3-12	12:2	2:00,6 2:00 6	75 []	h 5056:5	5060] IN: 5060] DE:	) OnGuardPlugin.OnGuardPlugin - Initialize: called 16 Common TextStore - LoadBesourceMenager: Besource Menager DLL Loaded Succesfully	
<ul> <li>201</li> </ul>	4-0	3-12	12:2	2:00,6	77 []	h 5056:5	5060] ER	DR OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Execption - Cannot open property file C:\Program	File:
	4-0 <mark>4-0</mark>	3-12 3-12	12:2	2:00,6 2:00,6	77 [] 77 []	h 5056:5 h 5056:5	5060] ER 5060] ER	DR OnGuardPlugin.AgentResourceHolder - Init: LoadAuthServerList failed DR OnGuardPlugin.AgentResourceHolder - Init: LoadAuthServerList threw exception	
♦ <mark>201</mark>	4-0	3-12	12:2	2:00,6	78 [1	<mark>h 5056:5</mark>	5060] ER	DR OnGuardPlugin.OnGuardPlugin - Initialize: Exception caught while Intializing Agent Plugin.	
		_							-
<u> </u>		1							

ClearPass OnGuard 6.3.1.61950	
Health Status: Not Known	
Connection Details Diagnostics Settings	1
Initializing	Login
	Retry
Not Connected	
	A
	<b>*</b>
Health Log Send Logs	

Reading of Agent Config file may fail in the following cases:

- 1. Agent Config file is missing May happen because of failed/incomplete installation.
- 2. Agent Config file is corrupted May happen if machine is shut down abruptly.

<u>Note</u> - The first log (InitializeLogger) written by **OnGuard Agent** to ClearPassOnGuard\_0.log file indicates that Agent was just launched.

<mark>2014-03-12 11:02:22,</mark>277 [Th 1988:3360] INFO\_OnGuardPlugin - InitializeLogger: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard.exe

This is helpful in case we want to know when the **OnGuard Agent** was launched.

🕻 ClearPassOnGuard_O.log (12.7 KB) - BareTail									
Elle Edit View Preferences Help									
😕 Opeg 🧈 Highlighting 🗖 Follow Tail 🗚 SI 🔽 C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (12.7 KB)									
ClearPassOnGuard_0.log 💙 winagert_0.log 🗙									
	-03-12	11:02:22,277	[Th	1988:3360]	INFO	OnGuardPlugin - InitializeLogger: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard.	exe		
0 2014-	-03-12	11:02:22,278	[Th	1988:3360]	INFO	OnGuardPlugin.OnGuardPlugin - COnGuardPlugin: Constructor called			
0 2014-	-03-12	11:02:22,278	[Th	1988:3360]	INFO	OnGuardPlugin.OnGuardPlugin - AddRef: m_lRefCount - 1			
0 2014-	-03-12	11:02:22,284	[Th	1988:3360]	INFO	OnGuardPlugin.OnGuardPlugin - Initialize: called			
0 2014-	-03-12	11:02:22,350	[Th	1988:3360]	DEBUG	Common.TextStore - LoadResourceManager: Resource Manager DLL Loaded Succesfully			
0 2014	-03-12	11:02:22,356	[Th	1988:3360]	INFO	OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Auth Server List - 10.17.4.198			
0 2014	-03-12	11:02:22,357	[Th	1988:3360]	INFO	OnGuardPlugin.AgentResourceHolder - SetAuthServerList: AuthServerList size - 1			
0 2014-	-03-12	11:02:22,358	[Th	1988:3360]	INFO	OnGuardPlugin.AgentResourceHolder - LoadUserSettings: User Settings file - C:\Users\Deepak\AppData\F	Roamin	ç	
0 2014-	-03-12	11:02:22,360	[Th	1988:3360]	INFO	OnGuardPlugin.AgentResourceHolder - LoadHealthStateInfoData: Health State Info file - C:\Users\Deepe	ak∖App	I	
0 2014-	-03-12	11:02:22,361	[Th	1988:3360]	ERROR	OnGuardPlugin.AgentResourceHolder - LoadHealthStateInfoData: Cannot open Health State Info file - C:	\User	2	
0 2014-	-03-12	11:02:22,361	[Th	1988:3360]	INFO	OnGuardPlugin.AgentThread - Start: AgentController Thread created successfully.			

# **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 Agent**s on local TCP Port #25427.

### **OnGuard Plugin Logs (Connection Successful):**

2014-03-12 13:30:34,312 [Th 00000f24] DEBUG OnGuardPlugin.BackendClient - Run: Backend Client Thread starting. Connecting to server on port=25427 2014-03-12 13:30:34,312 [Th 00000f24] INFO OnGuardPlugin.SocketClient - Connect: BackendClient - Connecting to server=127.0.0.1 on port= 25427

2014-03-12 13:30:34,312 [Th 00000f24] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect to 127.0.0.1 at port - 25427

2014-03-12 13:30:34,322 [Th 00000f24] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Successfully connected to Deepak-PC. Server IP = 127.0.0.1, Port = 25427

2014-03-12 13:30:34,322 [Th 00000f24] INFO\_OnGuardPlugin.SocketClient - Connect: BackendClient - Successfully connected to server. Registring the connection.

2014-03-12 13:30:34,323 [Th 00000f24] DEBUG OnGuardPlugin.BackendClient - Run: Connection to Agent Backend established

2014-03-12 13:30:34,323 [Th 00000f24] DEBUG OnGuardPlugin.AgentController - ConnectionEstablished: Connection to Agent Backend established

😫 ClearPassOnGuard_0.log (42.2 KB) - BareTail	
Eile Edit View Preferences Help	
😂 Open 🤌 Highlighting 🗐 Follow Tail 🛛 ANSI 💿 🔽 C:\Users\Deepak\AppData\Roaming\Aruba Ne	stworks\ClearPassOnGuard\ClearPassOnGuard_0.log (42.2 KB)
ClearPassOnGuard_0.log  winagent_0.log	
0-12 12:28:25,749 [Th 3048:3876] INFO OnGuardPlugin.AgentThread - Star	t: AgentController Thread created successfully.
o -12 12:28:25,749 [Th 3048:3876] DEBUG OnGuardPlugin.AgentController - :	Start: Controller Thread created
o-12 12:28:25,769 [Th 000001bc] INFO OnGuardPlugin.AgentController - R	un: Agent Controller Thread starting
o-12 12:28:26,270 [Th 000001bc] INFO OnGuardPlugin.AgentThread - Start	: BackendClient Thread created successfully.
o-12 12:28:26,270 [Th 000001bc] DEBUG OnGuardPlugin.SocketClient - Star	t: BackendClient Client Thread created
o -12 12:28:26,270 [Th 000001bc] DEBUG OnGuardPlugin.AgentController - I:	nit: Backend not active. Waiting 2 seconds before retry
o -12 12:28:26,270 [Th 000001f0] DEBUG OnGuardPlugin.BackendClient - Run	: Backend Client Thread starting. Connecting to server on port=25427
o-12 12:28:26,270 [Th 000001f0] INFO OnGuardPlugin.SocketClient - Conn	ect: BackendClient - Connecting to server=127.0.0.1 on port= 25427
o-12 12:28:26,271 [Th 000001f0] DEBUG OnGuardPlugin.ConnectionConnector	- Connect: Trying to connect to 127.0.0.1 at port - 25427
c-12 12:28:26,276 [Th 000001f0] DEBUG OnGuardPlugin.ConnectionConnector	- Connect: Successfully connected to Deepak-PC. Server IP = 127.0.0.1, Port = 25427
o-12 12:28:26,276 [Th 000001f0] INFO OnGuardPlugin.SocketClient - Conn.	ect: BackendClient - Successfully connected to server. Registring the connection.
o-12 12:28:26,276 [Th 000001f0] DEBUG OnGuardPlugin.SocketClient - Regi	sterConnection: BackendClient - Registering the connection, ConnId=1
0-12 12:28:26,276 [Th 000001f0] DEBUG OnGuardPlugin.ConnectionReader -	CAgentConnectionReader::get_handle: handle =00000710
o-12 12:28:26,276 [Th 000001f0] DEBUG OnGuardPlugin.SocketClient - Regi	sterHandler: BackendClient - Registering ACE event handler=00000710
0-12 12:28:26,276 [Th 000001f0] DEBUG OnGuardPlugin.ConnectionReader -	CAgentConnectionReader::get_handle: handle =00000710
o -12 12:28:26,277 [Th 000001f0] DEBUG OnGuardPlugin.SocketClient - Regi	sterConnection: BackendClient - Adding ConnectionReader into map for ConnId=1
o-12 12:28:26,277 [Th 000001f0] DEBUG OnGuardPlugin.BackendClient - Run	: Connection to Agent Backend established
0-12 12:28:26,277 [Th 000001f0] DEBUG OnGuardPlugin.AgentController - Control	onnectionEstablished: Connection to Agent Backend established
o-12 12:28:26,277 [Th 000001f0] DEBUG OnGuardPlugin.AgentController - E	nqueue: Adding action to queue: BACKEND_UP (12)
0-12 12:28:26,277 [Th 000001f0] INFO OnGuardPlugin.ActionQueue - Enque	ue: Inserted event 029109D8 type BACKEND_UP (12) into Queue 028F4418, QueueSize=1
0-12 12:28:26.297 [Th 000001f0] DEBUG OnGuardPlugin.ConnectionReader -	ChgentConnectionReader::handle input: handle =00000710

## **Backend Service Logs (Connection Successful):**

2014-03-12 13:30:34,314 [Th 0000021C] DEBUG WinAgent.ConnectionAcceptor - CWinAgentConnectionAcceptor::handle_input()handle=00000244
2014-03-12 13:30:34,314 [Th 0000021C] DEBUG WinAgent.ConnectionAcceptor - Creating new connection for ConnId=1
2014-03-12 13:30:34,314 [Th 0000021C] INFO_WinAgent.ConnectionAcceptor - CWinAgentConnectionAcceptor::handle_input() Accept Success: Client IP = 127.0.0.1, Port = 50218
2014-03-12 13:30:34,316 [Th 000010a8 Evt 04F3BEE0] INFO WinAgent.WinAgentConnEvHandler - Registration of ReadHandler succeeded

Aruba Networks

🐉 winagent_0.log (690.1 KB) - BareTail	
Eile Edit View Preferences Help	
😰 Open 🤣 Highlighting 🗂 Follow Tail 🗛 NSI 🤍 🔍 C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (690.1 KB)	
	< > ×
04-03-12 13:30:34,314 [Th 0000021C] DEBUG Winkgent.ConnectionAcceptor - CWinkgentConnectionAcceptor::handle_input()handle=00000244	
04-03-12 13:30:34,314 [Th 0000021C] DEBUG Winkgent.ConnectionAcceptor - Creating new connection for ConnId=1	
c4-03-12 13:30:34,314 [Th 0000021C] DEBUG WinAgent.ConnectionAcceptor - Posting ConnectionEvent with Id=101	
04-03-12 13:30:34,314 [Th 0000021C] INFO Common.EventProcessor - PostEvent: Posting Event 04F3BEE0 (101) into Queue 006D8178 of Thread 00747CA0	
04-03-12 13:30:34,314 [Th 0000021C] INFO Common.EventQueue - Enqueue: Inserted event 04F3BEE0 type (101) into Queue 006D8178, QueueSize=1	_
04-03-12 13:30:34,314 [Th 0000021C] INFO Winkgent.ConnectionAcceptor - CWinkgentConnectionAcceptor::handle input() Accept Success: Client IP = 127.0.0	0.1, I
0 4-03-12 13:30:34,314 [Th 000010a8] INFO Common.EventOueue - Dequeue: Removed event 04F3BEED type (101) from Oueue 006D8178, OueueSize=0	
04-03-12 13:30:34,315 [Th 000010a8] INFO Common.EventProcessor - EventThreadHandler: Processing Event 04F3BEE0 (101) from Event0 006D8178 started	
04-03-12 13:30:34.315 [Th 000010a8 Ext 04F3BEE0] DEBUG Winlgent.WinlgentEventProcessor - CWinlgentEventProcess::ProcessEvent(), processing event callbu	ack
04-03-12 13:30:34.315 [Th 00001088 Evt 04F3EEE0] DEBUG Winkgent Winkgent Found EventHandler for the EventId=101	
4-03-12 13:30:34 315 [Th 00001088 Fyr 04F3FF0] DEBUG Windgert WindgertConnEvMandler - Processing WindgertConnEvent	
4.03.12 13:30:43.43.5 [Th 0000106 For 0.153EF0] DEBUG Windgent WindgentWasardBandler - Degistering the connection _ Consider	
4.03.12 13:00:43.15 [IN DODTION For ONTSPIC] PERO MINIGENT WINDOW WEST WAS A	
4 02 12 12:00:04 215 [10 00001080 Eve OffSEE0] DEBUG Winkgent Winkgent Workssagehauter - Addite Ing we event hauter - ooboord	
4 03 13 13:00.34,016 [II b 0001040 EVE OFFSELD] DEDO WINKERLE WINKERSAGENAUTE - Auting ConnectionReader Into Map 10 Connect	
4.00-12 13:50:54,516 [In boolides Evel of Shell] INFO Winkgent Win	
04-03-12 13:30:34,316 [In 000010as Evt 04F36EE0] DEB0G winkgent.winkgentEventhandler - Encoded message = 99:("Content":("OS":"windows","Server":"Clear	ass I
0	
04-03-12 13:30:34,316 [Th 000010a8 Evt 04F3BEE0] DEBUG Winkgent.WinkgentEventHandler - Done sending the data. Size - 103	
04-03-12 13:30:34,316 [Th 000010a8 Evt 04F3BEE0] INFO Common.EventProcessor - EventThreadHandler: Processing Event (101) from EventQ 006D8178 finished	1
04-03-12 13:30:34,316 [Th 000010a8] INFO Common.EventQueue - Dequeue: No pending events in the queue 006D8178	
04-03-12 13:30:36.512 [Th 0000021C] DEBUG WinAgent.ConnectionReader - handle input: handle =00000464	<u> </u>

If the **OnGuard Plugin** fails to connect with the **Backend Service** then the **OnGuard Agent** UI will show "Initializing..." and **OnGuard Plugin** will keep on trying to connect with the **Backend Service**.

# OnGuard Plugin Logs (Connection with Backend Service Failed):

2014-03-12 14:09:26,299 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry
2014-03-12 14:09:26,299 [Th 00000678] DEBUG OnGuardPlugin.BackendClient - Run: Backend Client Thread starting. Connecting to server on port=25427
2014-03-12 14:09:26,300 [Th 00000678] INFO_OnGuardPlugin.SocketClient - Connect: BackendClient - Connecting to server=127.0.0.1 on port= 25427
2014-03-12 14:09:26,300 [Th 00000678] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect to 127.0.0.1 at port - 25427
2014-03-12 14:09:27,335 [Th 00000678] ERROR OnGuardPlugin.ConnectionConnector - Connect: Failed to connect to Remote Server. Error - 10061 (No connection could be made because the target machine actively refused it.)
2014-03-12 14:09:27,336 [Th 00000678] ERROR OnGuardPlugin.SocketClient - Connect: BackendClient - Failed to connect. Returned value = -1
2014-03-12 14:09:27,336 [Th 00000678] ERROR OnGuardPlugin.BackendClient - Run: Backend connection failed. Will retry after 5 seconds
2014-03-12 14:09:28,299 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry
2014-03-12 14:09:30,299 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry
2014-03-12 14:09:32,303 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry
2014-03-12 14:09:32,337 [Th 00000678] INFO_OnGuardPlugin.SocketClient - Connect: BackendClient - Connecting to server=127.0.0.1 on port= 25427
2014-03-12 14:09:32,337 [Th 00000678] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect to 127.0.0.1 at port - 25427
2014-03-12 14:09:33,373 [Th 00000678] ERROR OnGuardPlugin.ConnectionConnector - Connect: Failed to connect to Remote Server. Error - 10061 (No connection could be made because the target machine actively refused it.)
2014-03-12 14:09:33,373 [Th 00000678] ERROR OnGuardPlugin.SocketClient - Connect: BackendClient - Failed to connect. Returned value = -1
2014-03-12 14·09·33 374 [Th 00000678] ERROR OnGuardPluain BackendClient - Run <sup>.</sup> Backend connection failed Will retry after 5 seconds

🚺 Clear	PassOnG	iuard_0.log	(10.7 KB	s) - Ba	reTail				
<u>File E</u> dit	⊻iew	Preferences	Help						
൙ Open	i 🥔 Hig	hlighting 🗖	Follo <u>w</u> Ta	AA lie	ISI	• C	C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (10.7 KB)		
ClearPas	sonGua	rd_0.log 🔻	winage	ent_0.k	og 🗙			( )	×
02014-	-03-12	14:09:2	5,777	[Th	5560:5100	] INFO	O OnGuardPlugin.AgentThread - Start: AgentController Thread created successfully.		
02014-	-03-12	14:09:2	.5,777	[Th	5560:5100	] DEBU	3UG OnGuardPlugin.AgentController - Start: Controller Thread created		
02014-	-03-12	14:09:2	5,792	[Th	00001590]	INFO	) OnGuardPlugin.AgentController - Run: Agent Controller Thread starting		
02014-	-03-12	14:09:2	.6,299	[Th	00001590]	INFO	) OnGuardPlugin.AgentThread - Start: BackendClient Thread created successfully.		
02014-	-03-12	14:09:2	6,299	[Th	00001590]	DEBUG	JG OnGuardPlugin.SocketClient - Start: BackendClient Client Thread created		
02014-	-03-12	14:09:2	.6,299	[Th	00001590]	DEBUG	JG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry		_ 11
0 2014-	-03-12	14:09:2	6,299	[Th	00000678]	DEBUG	JG OnGuardPlugin.BackendClient - Run: Backend Client Thread starting. Connecting to server on port=25427		
◇ 2014-	-03-12	14:09:2	6,300	[Th	00000678]	INFO	) OnGuardPlugin.SocketClient - Connect: BackendClient - Connecting to server=127.0.0.1 on port= 25427		
	-03-12	14:09:2	6,300	[Th	00000678]	DEBUG	JG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect to 127.0.0.1 at port - 25427		
♦ 2014-	-03-12	14:09:2	7,335	[Th	00000678]	ERROR	JR OnGuardPlugin.ConnectionConnector - Connect: Failed to connect to Remote Server. Error - 10061 (No connect	lection	C
02014-	-03-12	14:09:2	7,336	[Th	00000678]	ERROR	<pre>/R OnGuardPlugin.SocketClient - Connect: BackendClient - Failed to connect. Returned value = -1</pre>		
0 <mark>2014-</mark>	-03-12	14:09:z	7,336	[Th	000006781	ERROR	JR OnGuardPlugin.BackendClient - Run: Backend connection failed. ⊎ill retry after 5 seconds		
02014-	-03-12	14:09:2	8,299	[Th	00001590]	DEBUG	JG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry		
0 2014-	-03-12	14:09:3	0,299	[Tn	00001590]	DEBUG	JG OnGuardFlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry		
02014-	-03-12	14:09:3	2,302	['1n	00001590]	DEBUG	JG Common.lextStore - GetFormattedPextFromResource: vswprintr result - 55	21 D	
02014-	-03-12	14:09:3	2,302	lin	00001590]	INFO	) OnGuardPlugin.AgentController - SendblagnosticLogMessage: Level - 2 Log message - Failed to connect to	ClearP	a
02014-	-03-12	14:09:3	2,303	[In	000015903	DEBUG	JG OnGuardFlugin.AgentController - Init: Backend not active. Waiting 2 seconds perore retry		_
02014-	-03-12	14:09:3	2,337	[In	000006783	INFO	) OnGuardFlugin.SocketClient - Connect: BackendClient - Connecting to Server=127.0.0.1 on port= 25427		
0 2014-	-03-12	14:09:3	2,357	[ In	000006783	PEBOG	JG OnGuardFlugin.ConnectionConnector - Connect: Ifying to connect to 127.0.0.1 at port - 25427		
02014-	-03-12	14:09:3	3,373	[ In	000006781	ERROR	JR OnGuardFlugin.ConnectionConnector - Connect: Failed to connect to Remote Server. From - 10051 (No connect) Providence and the connect Providence and the	lection	· •
02014	02 12	14:09:3	3,373	(Th	000006781	ERROR	R UnduardFlugin.SocketClient - Connect: Backendclient - Faired Co Connect, Returned Value		
2014	-02-12	14:05.3	0,017	[III [Th	00000070	DERUG	JK OnGuardFlugin.Backendclient - Kun: Backend Connection faired, will fetty after 5 becomes		-
2014.	-03-12	14:09.3	4,303	[ III	000015901	DEBUG	16 OnGuardFlugin.Agenconfolier - Init: Backend not active. Waiting 2 seconds before retry		
0 2014.	-03-12	14:09.3	8 303	[ Th	00001390]	DEBUG	No ondular dring in Agenconformer - Init: Backend not active Watchny 2 seconds before retry		
2014	-03-12	14.09.3	8 374	[Th	000013333	INFO	A one detailing in Agencion (for the converted active converting to servers 127.0.0.1 on ports 25427.		_
2014	-03-12	14.09.3	8 374	(Th	000006781	DEBUG	G OnGuardFlugin, Sobreccitence - Connect, Trying to connect to 127 0.0.1 at nort - 25427		
0 2014	-03-12	14:09:3	9.410	[Th	000006781	ERROR	N on warder ungin connection connector - connect reging to connect to Remote Server, Error - 19061 (No con	ection	
2014	-03-12	14.09.3	9 410	(Th	000006781	FRROR	A constant agrin connect lient $-$ connect. Backend(lient $-$ Failed to connect Deturned value $= -1$	leccion	
2014-	-03-12	14:09:3	9.410	[Th	000006781	FRROR	N onclardPlustin Backend(lient - Dun Backend connection failed Will retry after 5 seconds		
A2014-	-03-12	14.00.4	10 203	(Th	0000000000	DERIIG	A Gongley Main Agent Controller - Thit: Berband not extine . Weiting ? earonds hefore retru		<u> </u>
•									• //

# **Active Network Interface List**

After establishing a connection with **Backend Service**, **OnGuard Plugin** gets the list of Active Network Interfaces from the **Backend Service**.

### **OnGuard Plugin Logs (Network Interface List Successful):**

2014-03-12 14:24:55,689 [Th 000013f0] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 46:{"id":0,"name":"**NetworkInterfaceListRequest**"} 2014-03-12 14:24:55,692 [Th 000013f0] DEBUG OnGuardPlugin.MessageReguestDispatcher - SendMessage: Done sending the data. Size - 50 Result - 50 2014-03-12 14:24:55,704 [Th 00001408] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 215:{"content":{"ifList":{{"ifList":{{"isplayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"}]},"id":0,"name":"NetworkInterfaceListResponse"} 2014-03-12 14:24:55,705 [Th 00001408] DEBUG JsonWrapper.AgentJSONTransformer - Read message name NetworkInterfaceListResponse 2014-03-12 14:24:55,705 [Th 00001408] DEBUG OnGuardPlugin.MessageHandler - ProcessMessage: Network message parsed successfully. Message Name = NetworkInterfaceListResponse, Id = 0 2014-03-12 14:24:55,705 [Th 00001408] INFO OnGuardPlugin.BackendClientMessageHandler - ProcessResponse: Message Name = NetworkInterfaceListResponse Id = 02014-03-12 14:24:55,705 [Th 000013f0] DEBUG [sonWrapper.NetworkInterfaceListResponse - Interface List contents size = 1 2014-03-12 14:24:55,706 [Th 000013f0] DEBUG |sonWrapper.NetworkInterfaceListResponse - NetworkInterface::displayName=Local Area Connection 2014-03-12 14:24:55,706 [Th 000013f0] DEBUG |sonWrapper.NetworkInterfaceListResponse - NetworkInterface::ifName=Local Area Connection 2014-03-12 14:24:55,706 [Th 000013f0] DEBUG |sonWrapper.NetworkInterfaceListResponse - NetworkInterface::ifType=**WIRED** 2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::ipAddress=10.20.23.123 2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::macAddress=**001d09cca2bc** 

2014-03-12 14:24:55,706 [Th 000013f0] DEBUG OnGuardPlugin.BackendClientInfoCollector - GetNetworkInterfaceList: Network Interface List size=1

🛃 Clear	PassOnG	uard_0.log (`	79.7 KB)	) - Ba	reTail		
<u>File E</u> di	t <u>V</u> iew	Preferences	Help				
൙ Oper	) 🧳 Hig	hlighting 🔲 F	ollo <u>w</u> Tai	AN I	4SI	▼ C:	\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log [79.7 KB]
ClearPa	ssOnGua		winage	, nt N I	00 🔽		4 b X
	00.10		coo.			DEDUC	
2014	-03-12	14:24:55	,669	liu	00001310]	DEBUG	OnGuardPlugIn.hessagekequestPlspatcher - Senamessage:Encoded message = 46:("14":0,"hame":"WetWorkInterlaceList
02014	-03-12	14:24:55	. 692	ГTh	000013f01	DEBUG	OnGuardPlugin,MessageReguestDispatcher - SendMessage: Done sending the data, Size - 50 Result - 50
♦ 2014	-03-12	14:24:55	,692	[Th	000013f0]	DEBUG	OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=NetworkInterfaceListRet
♦ 2014	-03-12	14:24:55	,703	[Th	00001408]	DEBUG	OnGuardPlugin.ConnectionReader - C&gentConnectionReader::handle_input: handle =00000710
0 2014	-03-12	14:24:55	,703	[Th	00001408]	DEBUG	OnGuardPlugin.Connection - Outer sock->recv() returned 220
	-03-12	14:24:55	,703	[Th	00001408]	DEBUG	OnGuardPlugin.Connection - Inner sock->recv() returned -1
	-03-12	14:24:55	,704	[Th	00001408]	DEBUG	OnGuardPlugin.ConnectionReader - Read Data = 215:("content":("ifList":[("displayName":"Local Area Connection",'
¢ ,	00.10	14.04.55	704	c (11).	000014001	THE	
2014	-03-12	14:24:55	,704	lιυ	00001408]	INFO	UnduardFlugin.Hessagehandler - Frocesshessage: Got message=215:("Content":("libist":[("displayMame":"Local Are
2014	-03-12	14:24:55	.704	[Th	000014081	DEBUG	JaonWrapper.Netstrings - Extracted Netstrings message = {"content":{"ifList":[{"displayName":"Local &rea Connet
٥,							
02014	-03-12	14:24:55	,704	[Th	00001408]	DEBUG	JsonWrapper.JSONUtils - Key=id is INT
02014	-03-12	14:24:55	,704	[Th	00001408]	DEBUG	JsonWrapper.JSONUtils - Inserting Key=id Value=0
02014	-03-12	14:24:55	,704	[Th	00001408]	DEBUG	JsonWrapper.JSONUtils - Key=name is STRING
	-03-12	14:24:55	,704	[Th	00001408]	DEBUG	JsonWrapper.JSONUtils - Inserting Key=name Value=NetworkInterfaceListResponse
0 2014	-03-12	14:24:55	,704	[Th	00001408]	DEBUG	JsonWrapper.JSONUtils - Key=content is OBJECT
<ul> <li>≥ 2014</li> </ul>	-03-12	14:24:55	,705	[Th	00001408]	DEBUG	JsonWrapper.AgentJSONTransformer - Read message name NetworkInterfaceListResponse
	-03-12	14:24:55	,705	[Th	00001408]	DEBUG	OnGuardPlugin. MessageHandler - ProcessMessage: Network message parsed successfully. Message Name = NetworkInter
02014	-03-12	14:24:55	,705	[In	00001408]	DEDUC	UnduardPlugin.BackendUlientHessagenandler - Processkesponse: Message Name = NetworkInterfaceListkesponse in = (
0 2014	-03-12	14:24:55	705	[ I D	00001310]	DEBUG	Onduardriugh.nessagekequestbishatcher - walfforkesponse: walf for response over, kesponse event occurred
2014	-03-12	14.24.55	705	[Th	00001310]	DEBUG	OnGuardringht.nessagerequestDispatcher - NaitForDernorse. Removing message u - 0
0 2014	-03-12	14:24:55	,705	[Th	000013101	DEBUG	JaonWaner, Neuer Kinterfacelijst Besnonse - In Chetwork Interfacelijst Besnonse: Deserialize()
02014	-03-12	14:24:55	705	[Th	000013f01	DEBUG	JaonWrapper.NetworkInterfaceListResponse - Interface List contents size = 1
0 2014	-03-12	14:24:55	,706	[Th	000013f0]	DEBUG	JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::displayName=Local Area Connection
0 2014	-03-12	14:24:55	,706	[Th	000013f0]	DEBUG	JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::ifName=Local Area Connection
0 2014	-03-12	14:24:55	,706	[Th	000013f0]	DEBUG	JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::ifType=WIRED
	-03-12	14:24:55	,706	[Th	000013f0]	DEBUG	JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::ipAddress=10.20.23.123
2014	-03-12	14:24:55	,706	[Th	000013f0]	DEBUG	JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::macAddress=001d09cca2bc
♦ 2014	-03-12	14:24:55	,706	[Th	000013f0]	DEBUG	OnGuardPlugin.BackendClientInfoCollector - GetNetworkInterfaceList: Network Interface List size=1
02014	-03-12	14:24:55	,706	[ Th	000013f0]	DEBUG	OnGuardPlugin.AgentController - Enqueue: Adding action to queue: IF_UP (3)
02014	-03-12	14:24:55	,707	[Th	000013f0]	INFO	OnGuardPlugin.ActionQueue - Enqueue: Inserted event 0386F810 type IF_UP (3) into Queue 03865430, QueueSize=2
02014	-03-12	14:24:55	,712	lTh	UU0013f0]	INFO	OnGuardFlugin.ActionQueue - Dequeue: Removed event 03880AF8 type BACKEND_UP (12) from Queue 03865430, QueueSize
<u> </u>							

# Backend Service Logs (Network Interface List Successful):

2014-03-12 14:24:55,693 [Th 000016b4 Evt 050C5468] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 46:{"id":0,"name":" <b>NetworkInterfaceListRequest</b> "}
2014-03-12 14:24:55,693 [Th 000016b4 Evt 050C5468] DEBUG WinAgent.WinAgentMessageDriver - Message buffer is empty
2014-03-12 14:24:55,693 [Th 000016b4 Evt 050C5468] INFO WinAgent.WinAgentMessageDriver - Processing the network message = {"id":0,"name":"NetworkInterfaceListRequest"}
2014-03-12 14:24:55,694 [Th 000016b4 Evt 050C5468] DEBUG JsonWrapper.AgentJSONTransformer - Read message name NetworkInterfaceListRequest
2014-03-12 14:24:55,694 [Th 000016b4 Evt 050C5468] DEBUG WinAgent.NetworkInterfaceListMessageHandler - Inside NetworkInterfaceListMessageHandler()
2014-03-12 14:24:55,702 [Th 000016b4 Evt 050C5468] INFO_Common.NetworkIfHelper - GetNetworkInterfacesWindows: Add IfName={4228529A-5C50- 4DE6-8B87-7F8B7BBA2F6A} Adapter Index=10 Display Name=Broadcom 440x 10/100 Integrated Controller Type=WIRED MAC Address=00:1d:09:cc:a2:bc IP=10.20.23.123
I contraction of the second
2014-03-12 14:24:55,703 [Th 000016b4 Evt 050C5468] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message=NetworkInterfaceListRequest
2014-03-12 14:24:55,703 [Th 000016b4 Evt 050C5468] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 215:{"content":{"ifList":[{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"}]},"id":0,"name":"NetworkInterfaceListResponse"}
2014-03-12 14:24:55,703 [Th 000016b4 Evt 050C5468] DEBUG WinAgent.WinAgentEventHandler - Done sending the data. Size - 220

	vinagenl	t_0.log (204.9 KB) - BareTail
Eile	<u>E</u> dit <u>V</u>	Jew <u>Preferences</u> Help
2	Ope <u>n</u> 🚄	😕 Highlighting 🗖 Follow Tail 🖉 C.VProgram Data-Varuba Networks/ClearPassDnGuard/winagent_0.log (204.9 KB)
Cle	earPassO	nGuard_0.log 🔍 winagent_0.log 🔍
•	DEBUG	WinAgent.WinAGentReadEvHandler - Read data = 46:("id":0,"name":"NetworkInterfaceListRequest")
•		
•	DEBUG	Winlgent.WinlgentMessageDriver - Message buffer is empty
•	DEBUG	JsonWrapper.Netstrings - Extracted Netstrings message = ("id":0,"name":"NetworkInterfaceListRequest")
•		
•	INFO	WinAgent.WinAgentMessageDriver - Processing the network message = {"id":0, "name":"NetworkInterfaceListRequest"}
<b>°</b>		
	DEBUG	Jsonwrapper, Jsowuchis – keymia is ini Januaren Jsowuchis – keymia is ini
L.	DEBUG	Jacebranez Jowitila Company a STDING
	DEBUG	UsenWranper.JoSWichis - Krymame is Sikiwo JaenWranper.JoSWichis - Krymame is Sikiwo
Ň	MARN	Janutraner.JSONICIE - Indereing wey make varie wegerinderidenistede
Ň	DEBUG	Januiraner, Jonnitaner i Angelianer - Read message name NetworkInterfaceListRequest
	DEBUG	WinAgent.WinAgentMessageFactory - Inserting messageId=0 into message cache
•	DEBUG	Winkgent.NetworkInterfaceListMessageHandler - Inside NetworkInterfaceListMessageHandler()
•	INFO	Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (63884050-B59A-4346-89B9-CC2016A7B114) Desc: Microsoft Virtual WiFi Miniport Ada
•	INFO	Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (B553619B-BDB0-4F7C-9BAD-4DF6CDBE3F2E) Desc: Dell Wireless 1395 WLAN Mini-Card
•	INFO	Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (4228529A-5C50-4DE6-8B87-7F8B7BBA2F6A) Desc: Broadcom 440x 10/100 Integrated Com
•	INFO	Common.NetworkIfHelper - GetNetworkInterfacesWindows: Add IfName=(4228529A-5C50-4DE6-8B87-7F8B7BBA2F6A) Adapter Index=10 Display Name=Broadcom 440x
•	INFO	Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (988DF315-1000-4597-8080-4CFC5117FAF5) Desc: VirtualBox Host-Only Ethernet Adapt
•	DEBUG	Winkgent.WinkGentReadEvHandler - Successfully processed the message=NetworkInterfaceListRequest
•	DEBUG	WinAgent.WinAgentEventHandler - Encoded message = 215:("content":("ifList":[("displayName":"Local Area Connection","ifName":"Local Area Connection",
•		
Ŷ	DEBUG	Winagent.WinagentzventHandler - Done sending the data. Size - 220
l°.	TNEO	Winagent.Winagenthessageractory - Deleting messagela-0 from message cache
Ľ.	Event(	Common. Eventor to Cost - Eventor in Learnand tet. Frocessing Event (102) from EventQ 000001/0 finished
1		

If none of the Network Interface is active/connected then the OnGuard UI will show as "Initializing..." because OnGuard needs at-least 1 active Network Interface to communicate with the CPPM Server.

# **OnGuard Plugin Logs (Empty Network Interface List):**

2014-03-12 14:37:26,283 [Th 00000ab8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 46:{"id":0,"name":"**NetworkInterfaceListRequest**"}

2014-03-12 14:37:26,295 [Th 0000085c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 73:{"content":{"ifList":null},"id":0,"name":"NetworkInterfaceListResponse"}

2014-03-12 14:37:26,299 [Th 00000ab8] DEBUG JsonWrapper.NetworkInterfaceListResponse - In CNetworkInterfaceListResponse::Deserialize()

2014-03-12 14:37:26,299 [Th 00000ab8] WARN JsonWrapper.NetworkInterfaceListResponse - Interface list is empty

2014-03-12 14:37:26,299 [Th 00000ab8] DEBUG OnGuardPlugin.BackendClientInfoCollector - GetNetworkInterfaceList: Network Interface List size=0

2014-03-12 14:37:26,299 [Th 00000ab8] ERROR OnGuardPlugin.AgentController - Init: Network Interface List is empty.

ClearPa	issOnGi	uard 0.log (19	).4 KB) - Ba	areTail		×
File Edit	View F	Preferences He	elp			_
🗃 Open	Hiak	oliabtina 🗆 Eol	Iow Tail 🗛	NSI	CVUsers/Deepak/dopData/Boamin/douba Networks/ClearPassOnGuard/ClearPa	
						~
ClearPass	Unguar	a_v.iog 🗸 🔽	vinagent_u	log V	<u> </u>	<u> </u>
0 2014-0	03-12	14:37:26,	283 [Th	00000ab8]	DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 46:("id":0,"name":"NetworkInterfaceList	
2014	12 12	14.27.26	204 57%	00000-101	DEBUG On Guard Diverse Descent Discount State Sand Management Date sending the date Size 50 Decult 50	
2014-0	13-12 13-12	14:37:26,	284 [Th 284 [Th	00000ab8j	DEBUG UNUdaturlugin.messagerequestDispatcher - Senanessage: Durb Senaing the data. Size - So Result - So Debug DFRNG Unguard Playin MessagerequestDispatcher - WaitForDespanse: Wait for results for results NetworkInterfaceListDe	.
02014-0	03-12	14:37:26.	295 [Th	0000085c1	DEBUG OnGuardPlugin.ConnectionReader - ClarentConnectionReader::handle input: handle =0000070C	
0 2014-0	03-12	14:37:26,	295 [Th	0000085c]	DEBUG OnGuardPlugin.Connection - Outer sock->recv() returned 77	
0 2014-0	03-12	14:37:26,	295 [Th	0000085c]	DEBUG OnGuardPlugin.Connection - Inner sock->recv() returned -1	
0 2014-0	03-12	14:37:26,	295 [Th	0000085c]	DEBUG OnGuardPlugin.ConnectionReader - Read Data = 73:("content":("ifList":null),"id":0,"name":"NetworkInterfaceList	1
۰,						
	03-12	14:37:26,	295 [Th	0000085c]	INFO OnGuardPlugin.MessageHandler - ProcessMessage: Got message=73:("content":("ifList":null),"id":0,"name":"Networ	1
0, ,		14.07.05		0000005-1		
02014-0	J3-12	14:37:26,	295 [Th	000008563	DEBUG JSonWrapper.Netstrings - Extracted Netstrings message = {"content":("ifList":null),"id":U,"name":"NetworkInter	
2014-0	13-12	14.37.26	296 ГТЪ	0000085~1	DERIG JeonWrenner JSONUtile - Verzid is INT	
2014-0	13-12	14.37.26	296 [Th	0000085c1	DEBIG Southanner JSONTitis – Inserting Keysid Value=0	
0 2014-0	13-12	14:37:26.	296 [Th	0000085c1	DEBUG JonnWrapper, JSONUtils - Kevename is STRING	
0 2014-0	03-12	14:37:26,	296 [Th	0000085c1	DEBUG JsonWrapper.JSONUtils - Inserting Kev=name Value=NetworkInterfaceListResponse	
02014-0	03-12	14:37:26,	296 [Th	0000085c]	DEBUG JsonWrapper.JSONUtils - Key=content is OBJECT	•
♦ 2014-0	03-12	14:37:26,	296 [Th	0000085c]	DEBUG JsonWrapper.AgentJSONTransformer - Read message name NetworkInterfaceListResponse	
0 2014-0	03-12	14:37:26,	296 [Th	0000085c]	DEBUG OnGuardPlugin.MessageHandler - ProcessMessage: Network message parsed successfully. Message Name = NetworkInte	1
◇ 2014-0	03-12	14:37:26,	296 [Th	0000085c]	INFO OnGuardPlugin.BackendClientMessageHandler - ProcessResponse: Message Name = NetworkInterfaceListResponse Id =	<u>(</u>
0 2014-0	03-12	14:37:26,	299 [Th	00000ab8]	DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response over. Response event occurred	
0 2014-0	03-12	14:37:26,	299 [Th	00000ab8]	DEBUG OnGuardPlugin.MessageRequestDispatcher - RemovePendingResponse: Removing message id - O	
02014-0	J3-12	14:37:26,	299 [Th	00000ab8]	DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForkesponse: Response after Wait=U285C140	.
0 2014-0	J3-12 12-12	14:37:26,	299 [IN 200 [Th	00000ab8j	DEBUG JSONWTAPPET.NEtWORKINTETTACELISTKESPONSE - IN CHETWORKINTETTACELISTKESPONSE::DESETIALIZE()	
2014-0	13-12	14:37:26,	299 [IN 200 [Th	00000ab8j	waxw osonwizapper,weeworkinderizaebistkesponse - interizae iist is empty DFBNG (onGraphDurgin RackardChientInfoCollactor - CatNaturcEInterfacelist, NaturrE Interface list size=0	
0 2014-0	13-12	14:37:26.	299 [Th 299 [Th	00000ab81	FREE On Grandburgin Architection of the control of	
0 2014-0	03-12	14:37:26.	299 [Th	00000ab81	INFO OnGuardPlugin.AgentController - SendDiagnosticLogMessage: Level - 2 Log Message - No Active Network Connection	
0 2014-0	03-12	14:37:26,	312 [Th	00000ab8]	INFO OnGuardPlugin.ActionQueue - Dequeue: Removed event 02880AF8 type BACKEND UP (12) from Queue 02865430, QueueSiz	ε
0 2014-0	03-12	14:37:26,	312 [Th	00000ab8]	DEBUG OnGuardPlugin.AgentController - Run: Removed action from queue: BACKEND UP (12)	
02014-0	03-12	14:37:26,	312 [Th	00000ab8]	DEBUG OnGuardPlugin.AgentController - HandleAction: Handling action=BACKEND_UP (12) after a delay of 2.248 seconds	
<ul> <li>2014–0</li> </ul>	03-12	14:37:26,	312 [Th	00000ab8]	DEBUG OnGuardPlugin.AgentController - HandleConnectionEstablished: Connection with Backend established	
0 2014-0	03-12	14:37:26,	312 [Th	00000ab8]	INFO OnGuardPlugin.AgentController - HandleConnectionEstablished: Number of Managed Interfaces - O	
02014-0	03-12	14:37:26,	313 [Th	00000ab8]	DEBUG Common.TextStore - GetFormattedTextFromResource: vswprintf result - 60	النے
•						1/1

## **Backend Service Logs (Empty Network Interface List):**



🕽 winagent_0.log (148.2 KB) - BareTail										
Elle Edit View Preferences Help										
😂 Open 🥔 Highlighting 🗖 Follow Tail 🔼 ANSI 🗾 🔽 C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (148.2.KB)										
ClearPassOnGuard filing @ winanent filing @	♦ ¥									
Construction of the second sec	Permant (1)									
ouddoed Evt 04200920] DEb00 WInkgent.WInkGentReadEvManuler - Read data - 46:("Id":0,"Name":"NetWorkInterladeList	skequest")									
0000009ec Evt. 04E809281 DEBUG Winlgent.WinlgentMessageDriver - Message buffer is emnty										
0 000009ec Evt 04E60928] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message = {"id":0, "name": "NetworkInter	rfaceListRequest")									
000009ec Evt 04E80928] INFO Winkgent.WinkgentMessageDriver - Processing the network message = ("id":0,"name":"Net	etworkInterfaceListRequest")									
o 000009ec Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Key=id is INT										
000009ec Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Inserting Key=id Value=0										
000009cc Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Key=name is STRING										
00000925 EVE 04E80528] DEBUG JSONWEAPPER.JSONWEATS - Inserting key-name/value=NetworkInteriaceListkequest										
o bobolec ivi offoosioj ekki osonerappel.osonorija - key-content is Nobb nononger ivi offoosioj (kaj jenki osoner appel.osonorijantijenter - Bed mesege neme NetvorkinterfereljetBergest										
0000009cr Evt 04F800203 DEBUG Winkert Winkert WessareFactory - Inserting message Id=0 into message cache										
0 000009cc Evt 04E809281 DEBUG Winkgent.NetworkInterfaceListMessaceHandler - Inside NetworkInterfaceListMessaceHand	dler()									
000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: {63884050-B59A-4	4346-8989-CC2016A78114} Desc: Microsoft V:									
0 000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: {B553619B-BDB0-4	4F7C-9BAD-4DF6CDBE3F2E} Desc: Dell Wireles									
000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: {4228529A-5C50-4	4DE6-8B87-7F8B7BBA2F6A} Desc: Broadcom 44(									
000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (9B8DF315-1000-4	4597-80B0-4CFC5117FAF5} Desc: VirtualBox I									
000009ec Evt 04E80928] DEBUG Winkgent.WinkGentReadEvHandler - Successfully processed the message=NetWorkInterface	eListRequest									
000009ec Evt 04E80928] DEBUG Winkgent.WinkgentEventHandler - Encoded message = 73:("content":("ifList":null),"id"	":0,"name":"NetworkInterfaceListResponse"}									
000009cc Evt 04E80928] DEBUG Winkgent.WinkgentEventHandler - Done sending the data. Size - 77										
DUDUDUSED IV UTLOUSAD DEDUS WINNEHL. WINNEHL WEINAGENE TOTY - Deleting messagela-U from message cache	ol70 dinished									
Internet and internet into compare and proven and a compare and the provesting from the present the provided of the present the pr										

The OnGuard Agent maintains internal state of each Network Interface.

Initially all the Network Interfaces are in DOWN state.

After receiving Network Interface List from **Backend Service**, all the active Network Interfaces are moved from **DOWN** to **AUTH\_SERVER\_DISCOVERY** state.

### **OnGuard Plugin Logs (Moving Network Interface from DOWN to AUTH\_SERVER\_DISCOVERY):**

2014-03-12 15:51:39,697 [Th 000009e8] DEBUG OnGuardPlugin.AgentController - HandleIfUp: New Interface Up = IfName=Local Area Connection IfType=WIRED DisplayName=Local Area Connection MAC=001d09cca2bc IP=10.20.23.123

2014-03-12 15:51:39,697 [Th 000009e8] INFO\_OnGuardPlugin.AgentController - GetOrCreateInterfaceManager: Creating interface manager for Local Area Connection

2014-03-12 15:51:39,697 [Th 000009e8] INFO OnGuardPlugin.UIManager - NewInterface: Creating UI for interface=Local Area Connection

2014-03-12 15:51:39,699 [Th 000009e8] INFO OnGuardPlugin.InterfaceManager - HandleIfUp: Got IfUp in state=**DOWN** (0)

2014-03-12 15:51:39,699 [Th 000009e8] DEBUG OnGuardPlugin.InterfaceManager - UpdatelfInfo: Update interface info: IfName=Local Area Connection IfType=WIRED DisplayName=Local Area Connection MAC=001d09cca2bc IP=10.20.23.123

2014-03-12 15:51:39,700 [Th 000009e8] INFO OnGuardPlugin.HttpAuthChannel - SetLocalAddr: New local IP: 10.20.23.123

2014-03-12 15:51:39,700 [Th 000009e8] INFO\_OnGuardPlugin.InterfaceManager - SetState: Moving from DOWN (0) to AUTH\_SERVER\_DISCOVERY (1) after 0 seconds
# **Auth Server Discovery**

For each active Network Interface, the **OnGuard Agent** needs to select one CPPM Server from the list of CPPM Servers. The **OnGuard Agent** will send WebAuth Request to this selected CPPM Server. The list of CPPM Servers is read from the Agent Config file.

Selection of the CPPM Server is done in 2 steps:

- 1. Perform Reachability Check for all the CPPM Servers and creates a list of reachable CPPM Servers for each Network Interface.
- 2. Select one CPPM Server from the list of Reachable CPPM Servers.

### **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 - "<u>https://<CPPM Server IP Address>/images/index.html</u>".

Then the **OnGuard Agent** opens Reachability Check URL by binding the HTTPS Request to the Network Interface so that a HTTPS Request is sent to CPPM Server using that Network Interface. This is done to ensure that CPPM Server Reachability Check is performed using that particular Network Interface only.

### **OnGuard Plugin Logs (CPPM Server Reachability Check Passed):**

2014-03-12 15:27:43,978 [Th 000014c4] DEBUG OnGuardPlugin.AuthServerQueryComponent - FindAuthServer: Starting Auth server query for interface=Local Area Connection
I
2014-03-12 15:27:43,979 [Th 000012d8] INFO OnGuardPlugin.InterfaceQuery - Execute: Starting Query for - Local Area Connection
2014-03-12 15:27:43,980 [Th 000014dc] INFO OnGuardPlugin.AuthServerQuery - operator: Executing auth server query thread for - Local Area Connection
2014-03-12 15:27:43,980 [Th 000014dc] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950
2014-03-12 15:27:43,980 [Th 000014dc] INFO OnGuardPlugin.HttpAuthChannel - SetLocalAddr: New local IP: 10.20.23.123
2014-03-12 15:27:43,980 [Th 000014dc] INFO_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: <b>10.20.23.123</b> Remote IP: 10.17.4.234, url: https://10.17.4.234/images/index.html
2014-03-12 15:27:45,139 [Th 000014dc] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
2014-03-12 15:27:45,139 [Th 000014dc] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 214
2014-03-12 15:27:45,150 [Th 000014dc] INFO_OnGuardPlugin.AuthServerQuery - Execute: Reachability Status for Local Area Connection to server 10.17.4.234 - 1
2014-03-12 15:27:45,151 [Th 000012d8] INFO OnGuardPlugin.InterfaceQuery - GetActiveServers: Auth server= <b>10.17.4.234</b> is active for Local Area Connection

2014-03-12 15:27:45,152 [Th 000012d8] INFO OnGuardPlugin.InterfaceQuery - QueryActiveAuthServers: Active servers for interface Local Area Connection : 10.17.4.234

	ClearP	assOnGuard	_0.loc	<b>j (39.0 KB) - B</b> a	areTail	, and the second se	_ 0	x
Ei	e <u>E</u> dit	<u>V</u> iew <u>P</u> refer	ences	Help				
1	Open	🌽 Highlighti	ng E	Follow Tail A	NSI	C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (39.0 KB)		
ſci	earPas	sOnGuard_0.	og 🥆	vinagent_0.	log 🔻		• •	×
•	15:2	7:43,978	[Th	000014c4]	DEBUG	OnGuardPlugin.AuthServerQueryComponent - FindAuthServer: Starting Auth server query for interface=Local Area Connecti	ion	
•	15:2	7:43,978	[Th	000014c4]	INFO	OnGuardPlugin.ThreadGroup - AddThread: Adding thread to map with supplied key - Local Area Connection		
•	15:2	7:43,979	[Th	000014c4]	INFO	OnGuardPlugin.ThreadGroup - AddThread: Thead Group Size - 1 Map Size - 1		
۰	15:2	7:43,979	[Th	000014c4]	INFO	OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.		
•	15:2	7:43,979	[Th	000012d8]	INFO	OnGuardPlugin.InterfaceQuery - Execute: Starting Query for - Local &rea Connection		
٥	15:2	7:43,979	[Th	000012d8]	INFO	OnGuardPlugin.ThreadGroup - AddThread: Adding thread with key (id) - 14dc		
•	15:2	7:43,979	[Th	000012d8]	INFO	OnGuardPlugin.ThreadGroup - AddThread: Adding thread to map with supplied key - 14dc		
۰	15:2	7:43,979	[Th	000012d8]	INFO	OnGuardPlugin.ThreadGroup - AddThread: Thead Group Size - 1 Map Size - 1		_
۰	15:2	7:43,980	[Th	000014dc]	INFO	OnGuardPlugin.AuthServerQuery - operator: Executing auth server query thread for - Local Area Connection		
۰	15:2	7:43,980	[Th	000014dc]	INFO	OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950		_
۰	15:2	7:43,980	[Th	000014dc]	INFO	OnGuardPlugin.Http&uthChannel - SetLocal&ddr: New local IP: 10.20.23.123		
٥	15:2	7:43,980	[Th	000014dc]	INFO	OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.	.234/	1
۰	15:2	7:45,139	[Th	000014dc]	INFO	OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200		
۰	15:2	7:45,139	[Th	000014dc]	DEBUG	OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 214		
۰	15:2	7:45,150	[Th	000014dc]	INFO	OnGuardPlugin.AuthServerQuery - Execute: Reachability Status for Local Area Connection to server 10.17.4.234 - 1		1
•	15:2	7:45,151	[Th	000012d8]	INFO	OnGuardPlugin.InterfaceQuery - GetActiveServers: Auth server=10.17.4.234 is active for Local Area Connection		
۰	15:2	7:45,151	[Th	000012d8]	INFO	OnGuardPlugin.ThreadGroup - RemoveAllThreads: Removing thread from map with key - 14dc		
•	15:2	7:45,151	[Th	000012d8]	INFO	OnGuardPlugin.ThreadGroup - RemoveAllThreads: Thead Group Size - 0 Map Size - 0		
۰	15:2	7:45,152	[Th	000012d8]	INFO	OnGuardPlugin.InterfaceQuery - QueryActiveAuthServers: Active servers for interface Local Area Connection : 10.17.4.2	234	1
•	15:2	7:45,152	[Th	000012d8]	DEBUG	OnGuardPlugin.AgentController - Enqueue: Adding action to queue: AUTH_SERVERS (2)		
0	15:2	7:45,152	[Th	000012d8]	INFO	OnGuardPlugin.ActionQueue - Enqueue: Inserted event 042A80D0 type AUTH_SERVERS (2) into Queue 04285430, QueueSize=1		
•	15:2	7:45,153	[Th	000014c4]	INFO	OnGuardPlugin.ActionQueue - Dequeue: Removed event 042A80D0 type AUTH SERVERS (2) from Queue 04285430, QueueSize=0		2
1							•	1

If none of the CPPM Servers are reachable from a Network Interface, then **OnGuard Agent** keeps rechecking the CPPM Servers Reachability for that Network Interface every 30 seconds.

### **OnGuard Plugin Logs (CPPM Server Reachability Check Failed)**:



🚺 Clear	PassOnGuard_0.log (	47.1 KB) - BareTail	
<u>File</u> <u>E</u> di	: <u>V</u> iew <u>P</u> references	Help	
൙ Ope <u>n</u>	🥔 Highlighting 🔲 F	Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (47.1 KB)	
ClearPa	ss0nGuard_0.log 🔻	winagert_0.0g 🔽	×
♦ DEBU	G OnGuardPlugin	A.AuthServerQueryComponent - FindAuthServer: Starting Auth server query for interface=Local Area Connection 2	
♦ INFO	OnGuardPlugin	a.ThreadGroup - AddThread: Adding thread to map with supplied key - Local Area Connection 2	
<ul> <li>INFO</li> </ul>	OnGuardPlugin	ı.ThreadGroup - AddThread: Thead Group Size - 1 Map Size - 1	
♦ INFO	OnGuardPlugin	1.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.	
♦ INFO	OnGuardPlugin	1.InterfaceQuery - Execute: Starting Query for - Local Area Connection 2	
♦ INFO	OnGuardPlugin	1.ThreadGroup - AddThread: Adding thread with key (id) - 15e8	
♦ INFO	OnGuardPlugin	ı.ThreadGroup - AddThread: Adding thread to map with supplied key - 15e8	
♦ INFO	OnGuardPlugin	۱.ThreadGroup - AddThread: Thead Group Size - 1 Map Size - 1	
♦ INFO	OnGuardPlugin	h.AuthServerQuery - operator: Executing auth server query thread for - Local Area Connection 2	
♦ INFO	OnGuardPlugin	1.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950	
♦ INFO	OnGuardPlugin	1.HttpluthChannel - SetLocallddr: New local IP: 192.168.1.10	
♦ INFO	OnGuardPlugin	1.HttpClientWrapper - ExecuteMethod: Local IP: 192.168.1.10 Remote IP: 10.17.4.234, url: https://10.17.4.234/images/index.html	
♦ ERRO	R OnGuardPlugin	1.HttpClientWrapper - ExecuteMethod: Send Request failed from Local IP: 192.168.1.10 to Remote IP: 10.17.4.234.Error - 7(Couldn'	t
♦ ERRO	R OnGuardPlugin	i.HttpClientWrapper - DoSubmit: ExecuteMethod failed for Local IP: 192.168.1.10 Remote IP: 10.17.4.234.	
♦ ERRO	R OnGuardPlugin	1.HttpAuthChannel - IsAuthServerReachable: Echo to 10.17.4.234 failed from Local IP: 192.168.1.10.	
◊ INFO	OnGuardPlugin	1.AuthServerQuery - Execute: Reachability Status for Local Area Connection 2 to server 10.17.4.234 - O	
♦ WARN	OnGuardPlugin	).InterfaceQuery - GetActiveServers: Auth server=10.17.4.234 is not active/available on interface Local Area Connection 2	
♦ INFO	OnGuardPlugin	1.ThreadGroup - RemoveAllThreads: Removing thread from map with key - 15e8	
♦ INFO	OnGuardPlugin	1.ThreadGroup - RemoveAllThreads: Thead Group Size - 0 Map Size - 0	
♦ INFO	OnGuardPlugin	a.InterfaceQuery - QueryActiveAuthServers: Active servers for interface Local Area Connection 2 :	
♦ DEBU	G OnGuardPlugin	1.AgentController - Enqueue: Adding action to queue: AUTH_SERVERS (2)	
○ INFO	OnGuardPlugin	1.ActionQueue - Enqueue: Inserted event 041D80E0 type AUTH_SERVERS (2) into Queue 041B5430, QueueSize=1	
♦ INFO	OnGuardPlugin	1.InterfaceQuery - Execute: Finished Query for - Local Area Connection 2	
♦ INFO	OnGuardPlugin	1.ActionQueue - Dequeue: Removed event 041D80E0 type AUTH_SERVERS (2) from Queue 041B5430, QueueSize=0	
♦ DEBU	G OnGuardPlugin	1.AgentController - Run: Removed action from queue: AUTH_SERVERS (2)	
♦ DEBU	G OnGuardPlugin	1.AgentController - HandleAction: Handling action=AUTH_SERVERS (2) after a delay of 0.0 seconds	
♦ DEBU	G OnGuardPlugin	a.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Connection 2	
♦ INFO	OnGuardPlugin	1.InterfaceManager - PickAuthServer: Local Area Connection 2 Managed state: UNKNOWN_STATE	
♦ DEBU	G OnGuardPlugin	.InterfaceManager - PickAuthServer: No auth servers active for Local Area Connection 2	
♦ INFO	OnGuardPlugin	i.InterfaceManager - DoAuthServerDiscovery: No auth server for this interface Local Area Connection 2	
○ DEBU	G Common.TextSt	;ore - GetFormattedTextFromResource: vswprintf result - 59	<b>_</b>
			<u>)</u> //

### **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"

(Agent Settings can be viewed in Brower by opening Agent Settings URL.)

After reading the Agent Settings, **OnGuard Agent** also updates Agent Config file with latest information.

Refer '<u>ClearPass OnGuard in a Cluster</u>" Tech Note [1] to know how **OnGuard Agent** selects CPPM Server from the list of CPPM Servers. It also has detailed description of Agent Settings Parameters.

### OnGuard Plugin Logs (Select Auth Server Successful):

2014-03-12 15:51:40,774 [Th 000009e8] DEBUG OnGuardPlugin.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Connection
2014-03-12 15:51:40,774 [Th 000009e8] INFO_OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection Managed state: UNKNOWN_STATE
2014-03-12 15:51:40,774 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950
2014-03-12 15:51:40,774 [Th 000009e8] INFO_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/agent/settings
2014-03-12 15:51:40,775 [Th 00001248] INFO OnGuardPlugin.InterfaceQuery - Execute: Finished Query for - Local Area Connection
2014-03-12 15:51:40,791 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
2014-03-12 15:51:40,792 [Th 000009e8] INFO_OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = {"InstallVPNComponent":"false","fieldSubmit":"Submit","nodelp":["10.17.4.234"],"formType":"authApplet","CacheCredentialsForDays":"15","pass wordLabel":"Password","mode":"both","upgradeAction":"DoNothing","nodes":{"India":["10.17.4.234"]},"interfaces":"wired,wireless,vpn","domain" :"default","usernameLabel":"Username","agentVersion":"6.3.0.61264","trapUrl":""}
2014-03-12 15:51:40,792 [Th 000009e8] DEBUG OnGuardPlugin.AgentAppHttpClient - UpdateGlobalAgentSettings: Domain servers: Non-domain servers: 10.17.4.234 Load Balance:
2014-03-12 15:51:40,795 [Th 000009e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=UpdateAgentConfRequest Timeout value (ms) - 180000
2014-03-12 15:51:40,804 [Th 000009e8] DEBUG OnGuardPlugin.BackendClientInfoCollector - UpdateAgentConf: Update Agent Conf Response Status =1
2014-03-12 15:51:40,805 [Th 000009e8] INFO OnGuardPlugin.InterfaceManager - PickAuthServer: First init or client has moved domains. Old= New=default
2014-03-12 15:51:40,805 [Th 000009e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Node 10.17.4.234 is not part of domain default. Try and pick another one

Aruba Networks

2014-03-12 15:51:40,805 [Th 000009e8] INFO_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/agent/settings
2014-03-12 15:51:40,824 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
2014-03-12 15:51:40,824 [Th 000009e8] INFO_OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = {"InstallVPNComponent":"false","fieldSubmit":"Submit","nodeIp":["10.17.4.234"],"formType":"authApplet","CacheCredentialsForDays":"15","pass wordLabel":"Password","mode":"both","upgradeAction":"DoNothing","nodes":{"India":["10.17.4.234"]},"interfaces":"wired,wireless,vpn","domain" :"default","usernameLabel":"Username","agentVersion":"6.3.0.61264","trapUrl":""}
2014-03-12 15:51:40,824 [Th 000009e8] DEBUG OnGuardPlugin.AgentAppHttpClient - UpdateGlobalAgentSettings: Domain servers: Non-domain servers: 10.17.4.234 Load Balance:
2014-03-12 15:51:40,836 [Th 000009e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
2014-03-12 15:51:40,836 [Th 000009e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 97:{"content":{"ifName":"Local Area Connection","status":true},"id":6,"name":"AuthServerReachable"}
2014-03-12 15:51:40,838 [Th 000009e8] INFO_OnGuardPlugin.InterfaceManager - <b>DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local</b> Area Connection

2014-03-12 15:51:40,838 [Th 000009e8] INFO\_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH\_SERVER\_DISCOVERY (1) to WAIT\_FOR\_CREDENTIALS (2) after 1 seconds

😫 ClearPassOnGuard_0.log (349.5 KB) - BareTail	1×I
Elle Edit View Preferences Help	
😰 Open 🥜 Highlighting 🔲 Follow Tail 🗛 IC. VUsers/Deepak/AppData/Roaming/Aruba Networks/ClearPassOnGuard/ClearPassOnGuard_0.log (343.5 KB)	
ClearPassOnGuard_0.log Vwinagent_0.log V	X
02014-03-12 15:51:40,774 [Th 000009e8] DEBUG OnGuardPlugin.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Co	
02014-03-12 15:51:40,774 [Th 000009e8] INFO OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection Managed state: UNKNOWN_STATE	
02014-03-12 15:51:40,774 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950	
02014-03-12 15:51:40,774 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: User&gent - OnGuard 6.3.1.61950	
2014-03-12 15:51:40,774 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https	÷. Ц
2014-03-12 15:51:40,775 [Th 00001248] INFO OnGuardPlugin.InterfaceQuery - Execute: Finished Query for - Local Area Connection	1
2014-03-12 15:51:40,785 [Th 00001248] INFO OnGuardPlugin. ThreadGroup - RemoveThread: Removed thread from map with supplied key - Local Area Connection	n
2214-03-12 15:51:40,785 [Th 00001248] INFO OnGuardPlugin.ThreadGroup - RemoveThread: Thead Group Size - 0 Map Size - 0	_
0 2014-03-12 15:51:40,785 [Th 00001248] DEBUG OnGuardPlugin.AuthServerQueryComponent - RemovePendinginterface: Removing interface=Local area Connection	
a 2014-03-12 ISISII:40,791 [In 00000988] INFO UnduardPlugin.http://entwapper - Executemethod: HITP Response Code - 200	
a 2014-03-12 ISISII40, 792 [In bounded] bEbog UnduardPlugin.http://entwapper - Executemethod: Content_Length: 359	
0/2014-05-12 15:51:40,792 [In 00000983] INFO Unduardriugin.AgentAppnttplient - recongentSetting: Parsing JSUW = {"InstailyPhytomphonent": "Talser, "Tield	a
olui-05-12 15:51:40,722 [in 000009e6] bibbo Ondururiugin.kgentkprittpritent - Opuateolobaikgentsettings: Domain Servers: Non-domain Servers: 10.17.4	••
0. 0 2014-03-12 15:51:40,795 [Th 000009e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=UpdateAgentConfRequest. 0.	w
2014-03-12 15:51:40.804 (Th 000009e8) DEBUG OnGuardPlugin.BackendClientInfoCollector - UpdateAgentConf: Update Agent Conf Response Status =1	
22014-03-12 15:51:40,804 [Th 000009e8] DEBUG OnGuardPlugin.WsHttpClient - CWsHttpClient: URL=10.17.4.234	
2014-03-12 15:51:40,804 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950	
02014-03-12 15:51:40,805 [Th 000009e8] INFO OnGuardPlugin.InterfaceManager - PickkuthServer: First init or client has moved domains. Old= New=default	
02014-03-12 15:51:40,805 [Th 000009e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Node 10.17.4.234 is not part of domain default. Try and p	i,
0 2014-03-12 15:51:40,805 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https	<b>.</b>
02014-03-12 15:51:40,824 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200	
02014-03-12 15:51:40,824 [Th 000009e8] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 359	
02014-03-12 15:51:40,824 [Th 000009e8] INFO OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = {"InstallVPNComponent":"false","field	d:
02014-03-12 15:51:40,824 [Th 000009e8] DEBUG OnGuardPlugin.AgentAppHttpClient - UpdateGlobalAgentSettings: Domain servers: Non-domain servers: 10.17.4	-i
2014-03-12 15:51:40,836 [Th 000009e8] DEBUG OnGuardPlugin.WsHttpClient - CWsHttpClient: URL=10.17.4.234	
2014-03-12 15:51:40,836 [Th 000009e8] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950	
02014-03-12 15:51:40,836 [Th 000009e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234	
02014-03-12 15:51:40,836 [Th 00000985] DEBUG OnGuardFlugin. MessagekequestDispatcher - SendMessage:Encoded message = 97:("content":("ifName":"Local Area	•
	_
2014 03-12 15:51:40 000 [IN 0000090] INFO "On datur lugin, interite chanager - DOAUTASETVERDISCOVERY: USINg atth SETVER= 10.17.4.234 IOT EDGAL REG COMM	<b>;</b>
West to the local set of the second second second set of the second s	8
	-
	• //

After selecting CPPM Server, Network Interface is moved from **AUTH\_SERVER\_DISCOVERY** to **WAIT\_FOR\_CREDENTIALS** state to

# OnGuard Plugin Logs (Interface Moved from AUTH\_SERVER\_DISCOVERY to WAIT\_FOR\_CREDENTIALS state):

2014-03-12 15:51:40,838 [Th 000009e8] INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection

2014-03-12 15:51:40,838 [Th 000009e8] INFO\_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH\_SERVER\_DISCOVERY (1) to WAIT\_FOR\_CREDENTIALS (2) after 1 seconds

While selecting CPPM Server, **OnGuard Agent** also checks whether current Network Interface Type (Wired, Wireless, VPN or Other) is allowed (managed) by CPPM Server or not.

**OnGuard Agent** gets list of allowed Network Interface Type from Agent Settings. Example of Agent Settings:

```
{"InstallVPNComponent":"false","fieldSubmit":"Submit","nodeIp":["10.17.4.234"],"formType"
:"authApplet","CacheCredentialsForDays":"15","passwordLabel":"Password","mode":"both","up
gradeAction":"DoNothing","nodes":{"India":["10.17.4.234"]},"interfaces":"wired,wireless,v
pn","domain":"default","usernameLabel":"Username","agentVersion":"6.3.0.61264","trapUrl":
"","UseWindowsCredentials":"false"}
```

These agent settings also control **OnGuard Agent** behavior. For example: "**mode**" indicates whether **OnGuard Agent** should run in 'Auth-Only mode', 'Health-Only mode' or 'Auth+Health mode".

If a Network Interface Type is not allowed by CPPM Server then the **OnGuard Agent** will not change state of that Network Interface i.e. it will remain in AUTH\_SERVER\_DISCOVERY state.

#### **OnGuard Plugin Logs (Select Auth Server for Unmanaged Interface):**

2014-03-12 17:25:18,941 [Th 0000014c] DEBUG OnGuardPlugin.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Connection 2014-03-12 17:25:18,941 [Th 0000014c] INFO OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection Managed state: UNKNOWN\_STATE 2014-03-12 17:25:18,942 [Th 0000014c] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/agent/settings 2014-03-12 17:25:18,958 [Th 0000014c] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200 2014-03-12 17:25:18,959 [Th 0000014c] INFO OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = {"InstallVPNComponent":"false","fieldSubmit":"Submit","nodelp":["10.17.4.234"],"formType":"authApplet","CacheCredentialsForDays":"15","pass wordLabel":"Password","mode":"both","upgradeAction":"DoNothing","nodes":{"India":["10.17.4.234"]},"interfaces":"wireless,vpn","domain":"defa ult","usernameLabel":"Username","agentVersion":"6.3.0.61264","trapUrl":""} 2014-03-12 17:25:18,959 [Th 0000014c] DEBUG OnGuardPlugin.AgentAppHttpClient - UpdateGlobalAgentSettings: Domain servers: Non-domain servers: 10.17.4.234 Load Balance: 2014-03-12 17:25:18,970 [Th 0000014c] DEBUG OnGuardPlugin.BackendClientInfoCollector - UpdateAgentConf: Update Agent Conf Response Status =1 2014-03-12 17:25:18,970 [Th 0000014c] INFO OnGuardPlugin.InterfaceHelper - PickAuthServer: Local Area Connection not an allowed type: WIRED 2014-03-12 17:25:18,971 [Th 0000014c] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain= Auth server=10.17.4.234 2014-03-12 17:25:23,973 [Th 0000014c] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH\_SERVER\_DISCOVERY (1) (Seconds in this state=6) for Local Area Connection 2014-03-12 17:25:23,973 [Th 0000014c] DEBUG OnGuardPlugin.InterfaceManager - HandleNoOp: Not time for another auth server discovery run Local Area

Aruba Networks

Connection

2014-03-12 17:25:28,974 [Th 0000014c] INFO\_OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= AUTH\_SERVER\_DISCOVERY (1) (Seconds in this state=11) for Local Area Connection

2014-03-12 17:25:28,974 [Th 0000014c] DEBUG OnGuardPlugin.InterfaceManager - HandleNoOp: Not time for another auth server discovery run Local Area Connection

2014-03-12 17:25:33,975 [Th 0000014c] INFO\_OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= AUTH\_SERVER\_DISCOVERY (1) (Seconds in this state=16) for Local Area Connection

😋 ClearPassOnGuard_0.log (47.4 KB) - BareTail	
Elle Edit View Preferences Help	
🗃 Open 🥔 Highlighting 🗖 Follow Tail 🕼 NSI 🤍 C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPasSOnGuard\ClearPassOnGuard\ClearPasSOnGuard\ClearPassOnGuard\ClearPassOnGuard\ClearPassOnGuard\ClearPasSOnG	
ClearPassOnGuard_0.log Vwinagert_0.log V	<
o DEBUG OnGuardPlugin.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Connection	
o INFO OnGuardPlugin.InterfaceManager - PickluthServer: Local Area Connection Managed state: UNKNOWN STATE	
o INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950	
o INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950	
o INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/agent/settings	
o INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200	
NFO OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = {"InstallVPNComponent":"false","fieldSubmit":"Submit","nodeIp":["10.17	.4.23
o DEBUG OnGuardPlugin.AgentAppHttpClient - UpdateGlobalAgentSettings: Domain servers: Non-domain servers: 10.17.4.234 Load Balance:	
DEBUG OnGuardPlugin.BackendClientInfoCollector - UpdateAgentConf: Update Agent Conf Response Status =1	
DEBUG OnGuardPlugin.WsHttpClient - CWsHttpClient: URL=10.17.4.234	
NFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950	
o INFO OnGuardPlugin.InterfaceHelper - PickAuthServer: Local Area Connection not an allowed type: WIRED	
o DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain= Auth server=10.17.4.234	
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 97:("content":{"ifName":"Local Area Connection","status":true),"id":4	, "nam
o DEBUG OnGuardPlugin. MessageRequestDispatcher - SendMessage: Done sending the data. Size - 101 Result - 101	
o DEBUG OnGuardPlugin. MessageRequestDispatcher - SendRequest: No response expected for message: AuthServerReachable	
o DEBUG Common. TextStore - GetFormattedTextFromResource: vswprintf result - 55	
o INFO onGuardFlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.	
o INFO OnGuardFlugin.ActionQueue - Dequeue: No pending events in the queue U42C5430	
O LIVE UNCUARATATIUGIN.INTERIGEMANAGET - MANALENOUP: NOUP MANAIING IN STATE=AUIM SERVER DISCOVERY (1) (Seconds in this state=b) for Local Area Connec	stion
Bubbuc Unguardriugin. Interiacemanager - Handlewoop: Not time for another auth server discovery run Local Area Connection	
o INFO Oncuardriugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.	
Ginyo onguardriugin, actionquede - pequede: no pending vents in the queue 04205450	
DEPER OCCURRENTIQUE IN INCLASSE AND A AND	SCCIO
THEO OCCURRENT MINING INTERFERENCE AND A DEPENDENT OF A DEPENDENT AND A DEPEND	
a INFO Chordina Lagan, accordence. Dequete: No pending events in the quete, waiting for 3000 Ms.	
A INTO ONCOUNTED INFINITE For Marca - Pequete, No pending the state of 200300 DISCOMPDY (1) (Seconds in this state 16) for Local irea Conv	ortio
A DEFIC AGGinard Light interface Manager - Handraley nov maining in Sector Acid Sector Discover (1) (Sections in this sector is been acid to be a sector in the sector discover (1) (Sections in this sector is a	
o INFO Conducted Light institutionaget - Dequeues into the events in the queue. Waiting for 5000 ms.	
and should regimine the provide the provide regime in the queue, which give the second regime r	

## **Wait For Credentials**

In WAIT\_FOR\_CREDENTIALS state, the **OnGuard Agent** waits until it get credentials (username/password) to proceed further. The credentials **OnGuard Agent**s uses depends on following:

1. Value of 'mode' (auth, health-only or auth+health) in Agent Settings – **OnGuard Agent** shows Credentials dialog to the User to provide Credentials for 'auth' and 'auth+health' modes.

ClearPass OnGuard	×
Enter login credentials	
Username	
Password	
OK Cancel	

For 'health-only' mode, **OnGuard Agent** uses **Mac Address** of Network Interface as both username and password (no dialog is shown to user).

- User's selection for 'Save Credentials' If 'Save Credentials' option is selected and once provided credentials are authenticated by CPPM Server then **OnGuard Agent** saves user's credentials. Next time onwards, **OnGuard Agent** uses saved credentials automatically (no dialog is shown to user). Applicable to 'auth' and 'auth+health' modes.
- 3. Value of 'UseWindowsCredential' in Agent Settings If 'UseWindowsCredentials' option is enabled on the CPPM Server then **OnGuard Agent** uses current User's Windows Credential (no dialog is shown to user). **This option is not available on Mac OS X**.

Once the **OnGuard Agent** has the credentials, the Network Interface is moved back to into an AUTH\_SERVER\_DISCOVERY state, this time in an AUTH\_SERVER\_DISCOVERY state **OnGuard Agent** has credentials so it will start collecting health. The Network Interface will remain in the AUTH\_SERVER\_DISCOVERY state until it finishes its health checks.

# OnGuard Plugin Logs (Start Health Collection for Health-Only Mode after AUTH\_SERVER\_DISCOVERY):

 2014-03-12 18:08:12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection

 2014-03-12 18:08:12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH\_SERVER\_DISCOVERY (1) to WAIT\_FOR\_CREDENTIALS (2) after 1 seconds

 2014-03-12 18:08:12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - DoWaitForAuthCredentials: Only health checks required for Local Area Connection

 2014-03-12 18:08:12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - DoWaitForAuthCredentials: Only health checks required for Local Area Connection

 2014-03-12 18:08:12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - GetNetworkInterfaceList: Network interfaces list size for Local Area Connection : 1

 2014-03-12 18:08:12,837 [Th 000008f4] DEBUG OnGuardPlugin.AuthSession - Authenticate: Not In HealthCheckQuietPeriod. Performing full Auth with health checks

2014-03-12 18:08:12,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 43:{"id":8,"name":" <b>CollectHealthDataRequest</b> "}
2014-03-12 18:08:12,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 47 Result - 47
2014-03-12 18:08:12,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>CollectHealthDataRequest</b> Timeout value (ms) - 1200000
ClearPassOnGuard_0.log (90.2 KB) - BareTail  Ele Edit View Preferences Help  Chlisers\Deenak\\donData\Boamin(\donba Networks\DeePassOnGuard\DeePasSOnGuard\DeePasSOnGuard\DeePasSOnGuard\
ClearPasonGward_Blog Wmagent_Dig V ClearPasonGward_Blog Wmagent_Dig V 12,814 [Th 000006f4] INFO OnGwardPlugin.InterfaceManager = DoWaitForkuthGreentais: Only Mealth Check Party Top_CREPENTIALS (2) after 1 seconds 12,814 [Th 000006f4] INFO OnGwardPlugin.InterfaceManager = DoWaitForkuthGreentais: Only Mealth Check Peruited for Local Area Connection 12,814 [Th 000006f4] INFO OnGwardPlugin.InterfaceManager = DoWaitForkuthGreentais: Only Mealth Checks Peruited For Local Area Connection 12,814 [Th 000006f4] INFO OnGwardPlugin.InterfaceManager = DoWaitForkuthGreentais: Only Mealth Checks Peruited For Local Area Connection 12,815 [Th 000006f4] DENG OnGwardPlugin.AuthSession = InHealthCheckQuitePeriod: PeriodInable(4) returned false for Local Area Connectic 12,835 [Th 000006f4] DEBUG OnGwardPlugin.AuthSession = InHealthCheckQuitePeriod: Personble cause = InterfaceType=VPN   Mode!=HealthOnly   HealthCheckQuite 12,837 [Th 000006f4] DEBUG OnGwardPlugin.AuthSession = InHealthCheckQuitePeriod: Personble Cause = InterfaceType=VPN   Mode!=HealthOnly   HealthCheckQuite 12,837 [Th 000006f4] DEBUG OnGwardPlugin.MuthSession = InHealthCheckQuitePeriod: Performing full Auth with health Check 12,837 [Th 000006f4] DEBUG OnGwardPlugin.MuthSession = Authenticate: To In HealthCheckQuitePeriod.Performing full Auth with health Check 12,837 [Th 000006f4] DEBUG OnGwardPlugin.MuthSession = Authenticate: VaryInitf result = 61 12,837 [Th 000006f4] DEBUG OnGwardPlugin.MuthSessagerEncestDispatcher = AddPlugingmessage = 431("3d"18," Mame";"CollectHealthDataRequest")

o 012,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendHessage: Done sending the data. Size - 47 Result - 47 012,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout Value 043,132 [Th 000012d8] DEBUG OnGuardPlugin.ConnectionReader - C&gentConnectionReader::handle\_input: handle =00000708 043,132 [Th 000012d8] DEBUG OnGuardPlugin.Connection - Outer sock->recv() returned 74

# **OnGuard Plugin Logs (Start Health Collection in AUTH\_SERVER\_DISCOVERY for auth modes):**

2014-03-12 17:58:05,422 [Th 00000f68] INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection
2014-03-12 17:58:05,422 [Th 00000f68] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_SERVER_DISCOVERY (1) to WAIT_FOR_CREDENTIALS (2) after 1 seconds
2014-03-12 17:58:05,422 [Th 00000f68] INFO_OnGuardPlugin.InterfaceManager - DoWaitForAuthCredentials: Need user action to proceed for Local Area Connection
2014-03-12 17:58:05,510 [Th 6092:3892] INFO_OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Connection Username=dj
2014-03-12 17:58:05,510 [Th 6092:3892] DEBUG OnGuardPlugin.AgentController - Enqueue: Adding action to queue: USER_CREDENTIALS (1)
2014-03-12 17:58:05,525 [Th 00000f68] DEBUG OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Local Area Connection
2014-03-12 17:58:05,525 [Th 00000f68] INFO_OnGuardPlugin.InterfaceManager - SetState: <b>Moving from WAIT_FOR_CREDENTIALS (2) to</b> AUTH_SERVER_DISCOVERY (1) after 0 seconds
2014-03-12 17:58:05,525 [Th 00000f68] INFO_OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection Managed state: OVERRIDE_UNMANAGE
2014-03-12 17:58:05,525 [Th 00000f68] INFO_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/agent/settings
2014-03-12 17:58:05,551 [Th 00000f68] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
2014-03-12 17:58:05,565 [Th 00000f68] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
2014-03-12 17:58:05,568 [Th 00000f68] INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery <b>: Using auth server= 10.17.4.234 for Local Area</b> Connection
2014-03-12 17:58:05,569 [Th 00000f68] INFO OnGuardPlugin.InterfaceManager - GetNetworkInterfaceList: Network interfaces list size for Local Area Connection : 1

 2014-03-12 17:58:05,569 [Th 00000f68] DEBUG OnGuardPlugin.AuthSession - Authenticate: Not In HealthCheckQuietPeriod. Performing full Auth with health

 check

 ]

 2014-03-12 17:58:05,570 [Th 00000f68] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =

 44:{"id":12,"name":"CollectHealthDataRequest"}

 2014-03-12 17:58:05,570 [Th 00000f68] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 48 Result - 48

 2014-03-12 17:58:05,570 [Th 00000f68] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 48 Result - 48

 2014-03-12 17:58:05,570 [Th 00000f68] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000

🕏 ClearPassOnGuard, 0.log (110.7 KB) - BareTail	_ 🗆 × 🛛
Elle Edit View Breferences Help	
<sup>26</sup> Open <sup>20</sup> Highlighting <sup>17</sup> Follog Tail ANSI <sup>1</sup> C.Utsers/Deepak/AppData/Roaming/Aruba Networks/ClearPassOnGuard/ClearPassOnGuard_0.log (110.7 KB)	
ClearPassOnGuard_Blog 🔍 winagent_Blog 🔍	<
NFO OnGuardPlugin, InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection	
o INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH SERVER DISCOVERY (1) to WAIT FOR CREDENTIALS (2) after 1 seconds	
O INFO OnGuardPlugin.InterfaceManager - DoWaitForkuthCredentials: Need user action to proceed for Local Area Connection	
o] INFO OnGuardPlugin.NetworkInterface&ctionListener - SetUser&uthInfo: User auth info available for Local Area Connection Username=dj	
] DEBUG OnGuardPlugin.AgentController - Enqueue: Adding action to queue: USER_CREDENTIALS (1)	
o DEBUG OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Local Area Connection	
o INFO OnGuardPlugin.InterfaceManager - SetState: Moving from WAIT_FOR_CREDENTIALS (2) to AUTH_SERVER_DISCOVERY (1) after 0 seconds	
INFO OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection Managed state: OVERRIDE_UNMANAGE	
INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/agent/settings	
INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200	
INFO OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = ("InstallVPNComponent":"false","fieldSubmit":"Submit", "nodeIp":["10.17.	4.234
DEBUG UNGUARAPIUGIN.Interfacemanager - Pickauthserver: Current domain=derault auth Server=10.17.4.234	
o INFO OpCuardDlugin InterforeNewsger - DebuthServerDiggovery, Heing outh server: 10,17,4,224 for Logal Area Convection	
a INFO OnGuardright, interfacemanager - Doubleverbristerfacelist. Natural interface list are for local Area Connection - 1	
A DERIG ONGUERING MUTCHERSESSION - TWEETERSTRUCTURE TERIOLITICS INCOMPLETING THE INFORMATION FOR THE STATE ON THE STATE OF	_
DEBUG ONGUNATU TANJUN AUTOSESSION - INFERITORACIUST Period. Dossible cause - InterfaceTunes:UNI   Model=HealthObertuni   HealthObertunistPeriod == 0	
DEBIG OnGuarda Lagunational international construction international construction of the second seco	
DEBUG OnGuardPlugin.MessageReguestDisnatcher - AddPendingResnonse: Adding message id - 12	
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:("id":12."name":"CollectHealthDataRequest")	
	_
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 48 Result - 48	
DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000	<b>-</b>

# **Collect Health**

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:



<u>Note</u> – Starting with CPPM 6.3.1 onwards, the **OnGuard Agent** collects health only if the health classes are configured in Posture Policy on CPPM.

# OnGuard Plugin Logs (Health Collection):





R (FearPassOnGuard, D. Ion / 356 4 VB) - BareTail
File Edit View Preferences Help
😂 Open 🤌 Highlighting 🔽 Follow Tail ANSI 🤍 C. VUsers/Deepak/AppData/Roaming/Aruba Networks/ClearPassOnGuard/ClearPassOnGuard/0.log (356.4 KB)
ClearPassOnGuard_0.log 👻 winagert_0.log 👻
<ul> <li>(Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 43:("id":8, "name":"CollectHealthDataRequest")</li> <li>(Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms         (Th 00000e60] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 70:("content":("status":true),"id":8, "name":"CollectHealthDataResponse")</li> <li>(Th 00000e60] INFO OnGuardPlugin.MessageHandler - ProcessBessage: Got message=70:("content":("status":true),"id":8, "name":"CollectHealthDataResponse")</li> <li>(Th 00000e60] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message = ("content":("status":true),"id":8, "name":"CollectHealthDataResponse")</li> </ul>
(Th 00000ee4] DEBUG OnGuardPlugin.BackendClientInfoCollector - CollectHealthData: Collect Health Data Response Status =1 (Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 301("id":10,"mame":"SoRRequest") (Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 34 Result - 34 (Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=SoRRequest Timeout value (ms) - 180000
(Th 00000c60] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 4478:("content":("soh":[0,7,5,91,0,0,1,55,0,2,5,83,0,7,0,30,0,0,1,55,35,72,0,0,-66,24 4,0,111,0,115,0,111,0,102,0,116,0,32,0,83,0,101,0,99,0,117,0,114,0,105,0,116,0,121,0,32,0,69,0,115,0,115,0,101,0,116,0,105,0,97,0,108,0,115,0,0,1 (Th 00000ee4] DEBUG OnGuardPlugin.InterfaceSessionHelper - CollectHealthData: SoH: 0x0007055b000001370002055530007001e0000013723480000be18000094670000e

### **Backend Service Logs (Health Collection):**

2014-03-13 12:09:03,392 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 43:{"id":8,"name":" <b>CollectHealthDataRequest</b> "}
I contraction of the second
2014-03-13 12:09:03,393 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.CollectHealthDataMessageHandler - Inside CollectHealthDataMessageHandler()
2014-03-13 12:09:03,393 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentHealthProcessor - Start collecting health information
2014-03-13 12:09:06,375 [Th 000001A4] DEBUG WinSHA.VMHealthClassInfoFactory - GetGuestVMList: EnumerateVirtualMachines returned success - 0
2014-03-13 12:09:06,446 [Th 000001A4] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - VirtualMachines (14)
2014-03-13 12:09:06,446 [Th 000001A4] DEBUG WinSHA.NetConnHealthClassInfoFactory - GetHealth: Updating Network Connections Info
2014-03-13 12:09:08,101 [Th 000001A4] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - NetworkConnections (15)
l
2014-03-13 12:09:12,589 [Th 000001A4] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - DiskEncryption (16)

2014-03-13 12:09:12,589 [Th 000001A4] DEBUG WinSHA.InstalledAppHealthClassInfoFactory - GetHealth: Updating cached InstalledApp Health Class Info.
I. Construction of the second s
2014-03-13 12:09:12,705 [Th 000001A4] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - InstalledApplications (17)
2014-03-13 12:09:12,706 [Th 000001A4] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Finished collecting Health of the Client
I contraction of the second
2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.CollectHealthDataMessageHandler - Done collecting the health data
2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message= <b>CollectHealthDataRequest</b>
2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 70:{"content":{"status":true},"id":8,"name":" <b>CollectHealthDataResponse</b> "}
I and the second se
2014-03-13 12:09:18,038 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 30:{"id":10,"name":"SoHRequest"}
I contraction of the second
2014-03-13 12:09:18,039 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.SoHMessageHandler - In ProcessMessage() of SoHMessageHandler
2014-03-13 12:09:18,041 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message=SoHRequest
2014-03-13 12:09:18,042 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 4478:{"content":{"soh":[0,7,5,91,0,0,1,55,0,2,0,4,2,0]},"id":10,"name":" <b>SoHResponse</b> "}

🕽 winagent_0.log (1.5 MB) - BareTail		×
Elle Edit View Preferences Help		
😰 Open 🖉 Highlighting 🔽 Follow Tail 🗛 NST 🔍 C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (1.5 MB)		
ClearPassOnGuard_0.log • winagent_0.log •	٠ )	×
2014-03-13 12:09:03.392 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent, WinkGentReadEvHandler - Read data = 43:("id":8."name":"CollectHealthDataRequest")		
· · · · · · · · · · · · · · · · · · ·		
o 2014-03-13 12:09:03,393 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.CollectHealthDataMessageHandler - Inside CollectHealthDataMessageHandler()		
02014-03-13 12:09:03,393 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent.WinkgentHealthProcessor - Start collecting health information		
02014-03-13 12:09:06,375 [Th 000001A4] DEBUG WinSHA.VMHealthClassInfoFactory - GetGuestVMList: EnumerateVirtualMachines returned success - 0		
02014-03-13 12:09:06,376 [Th 00000114] DEBUG WinSHA.VMHealthClassInfoFactory - GetGuestVMList: Number of Guest Virtual Machines found - 2		-
2014-03-13 12:09:06,444 [Th 00000114] INFO WinSHA.VMHealthClassInfoFactory - GetHealth: Number of Guest Virtual Machine - 2		
2014-03-13 12:09:06,444 [Th 000001A4] INFO WinSHA.VMHealthClassInfoFactory - GetHealth: Adding IsHostVirtualMachine attr to Map		
·		
0 2014-03-13 12:09:06,446 [Th 000001A4] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - VirtualMachines (14)		
2214-03-13 12:09:06,446 [Th UUUUU1A4] DEBUG WINSHA.NetConnHealthClassInforactory - GetHealth: Updating Network Connections Info		
0,		
a 2014-05-13 12:09:06,101 [in 00000144] INFO winshk.healthractoryix - Gethealthrequest: kading health class into - Wetworktonnections (15)		
2014-03-13 12:09:12 589 [Th 000001141 INFO WinSH! HealthFactoryFy - GetHealthRequest: Adding Health Class Info - DiskEncryption (16)		
2014-03-13 12:19:12-589 [Th 00000114] DEBUG WinSHA Installedin HealthClassInforectory - GetHealth Indefing cached Installedin Health Class Info.		
A.		
2014-03-13 12:09:12.705 [Th 000001A4] INFO WinSHA.HealthFactorvEx - GetHealthRequest: Adding Health Class Info - InstalledApplications (17)		
0 2014-03-13 12:09:12,706 [Th 000001A4] DEBUG WinSHA HealthFactorvEx - GetHealthRequest: Finished collecting Health of the Client		
o 2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent.CollectHealthDataMessageHandler - Done collecting the health data		
o 2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent.WinkGentReadEvHandler - Successfully processed the message=CollectHealthDataRequest		
o 2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent.WinkgentEventHandler - Encoded message = 70:("content":("status":true),"id":8,"name"	:"Co	1
o 2014-03-13 12:09:18,038 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent.WinkGentReadEvHandler - Read data = 30:("id":10,"name":"SoHRequest")		
P.		
o 2014-03-13 12:09:18,039 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent.SoHMessageHandler - In ProcessMessage() of SoHMessageHandler		
o 2014-03-13 12:09:18,041 [Th 00000344 Evt 04D7EE60] DEBUG Winkgent.WinkGentReadEvHandler - Successfully processed the message=SoHRequest		
02014-03-13 12:09:18,042 [Th 00000344 Evt 04D7EE60] DEEUG Winkgent.WinkgentEventHandler - Encoded message = 4478: ("content": ("soh": [0,7,5,91,0,0,1,55,0]	1,2,5,	
3,0,8,0,1,2,0,10,0,58,77,0,105,0,99,0,114,0,111,0,115,0,111,0,102,0,116,0,32,0,83,0,101,0,99,0,117,0,114,0,105,0,116,0,121,0,32,0,69,0,115,0,115,0,10	1,0,1	4
	Þ	Č.
		1/1

### Send WebAuth to CPPM Server

After Health Collection is complete, the **OnGuard Plugin** creates WebAuth Request and sends it to the CPPM Server for evaluation.

### **OnGuard Plugin Logs (Send WebAuth):**

2014-03-13 12:09:18,119 [Th 00000ee4] INFO\_OnGuardPlugin.WsHttpClient - GetRequestXml: Request={username=001d09cca2bc, sohSize=1375, networkInterfaceInfo=(ip=10.20.23.123,mac=001d09cca2bc), , Attributes=(name=Host:FQDN,value=Deepak-PC), (name=Host:InterfaceType,value=WIRED), (name=Host:OSArch,value=i386), }

2014-03-13 12:09:18,119 [Th 00000ee4] INFO OnGuardPlugin.WsHttpClient - SubmitWebAuth: Posting request to URL=/v2/PostureCheck/OnGuard

2014-03-13 12:09:18,119 [Th 00000ee4] INFO OnGuardPlugin.HttpClientWrapper - SetRequestEntity: Mime Type - text/xml Post Data Size - 3534

2014-03-13 12:09:18,119 [Th 00000ee4] INFO\_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/networkservices/webauthservice/v2/PostureCheck/OnGuard

2014-03-13 12:09:18,674 [Th 00000ee4] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200

2014-03-13 12:09:18,675 [Th 00000ee4] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 1957

2014-03-13 12:09:18,676 [Th 00000ee4] INFO\_OnGuardPlugin.AuthSession - ProcessResponse: Response={status=0, statusMsg=, sohrSize=703, opaqueAuthState=wcy1DvZOW8g3h3VKkjyUkg+XB5CeT5CVZzdQPpz3bXgcs3EVeU0VrPldJKOCzrBT3yZnG3hTNcxXHLlbh5oa0AgpRGYgt9OvfP3QLJEuVQA=, attributes=[{N=BounceClient V=false}, {N=HealthCheckQuietPeriod V=0}, {N=Message V=Test}, ]}

ClearPassDnGuard_0.log (356.5 KB) - BareTail	
Eile Edit View Preferences Help	
😰 Open 🤣 Highlighting 🔽 Follow Tail 🗚 SI 📃 C. Ubsers/Deepak/AppData/Roaming/Aruba Networks/ClearPassDnGuard/ClearPassDnG	
ClearPassOnGuard_0.log  winagert_0.log	< > X
2014-03-13 12:09:18,119 [Th 00000ee4] INFO OnGuardPlugin.WsHttpClient - GetRequestXml: Request=(username=001d09cca2bc, sohSize=1375, net     )	orkInterfaceIn
02014-03-13 12:09:18,119 [Th 00000ee4] INFO OnGuardPlugin.WsHttpClient - SubmitWebAuth: Posting request to URL=/v2/PostureCheck/OnGuard	
2014-03-13 12:09:18,119 [Th 00000ee4] INFO OnGuardPlugin.HttpClientWrapper - SetRequestEntity: Mime Type - text/xml Post Data Size - 353	
2014-03-13 12:09:18,119 [Th 00000ee4] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.23	, url: https:/
02014-03-13 12:09:18,674 [Th 00000ee4] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200	
02014-03-13 12:09:18,675 [Th 00000ee4] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 1957	
2014-03-13 12:09:18,676 [Th 00000ee4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response=(status=0, statusMsg=, sohrSize=703, op	queAuthState=w
•	
	► //.

## **Process WebAuth Response**

The CPPM Server replies with WebAuth Response which contains evaluation results - Authentication Result, Statement of Health Response (SoHR) and Agent Enforcement Profile attributes.



If the Authentication fails then the **OnGuard Agent** ignores the health check results and shows "Authentication Failed." message to user.



### **OnGuard Plugin Logs (Authentication Failed):**

2014-03-13 15:47:38,785 [Th 000013a4] INFO OnGuardPlugin.WsHttpClient - GetRequestXml: Request={username=dj, sohSize=1370, networkInterfaceInfo=(ip=10.20.23.123,mac=001d09cca2bc), , Attributes=(name=Host:FQDN,value=Deepak-PC), (name=Host:InterfaceType,value=WIRED), (name=Host:OSArch,value=i386), }
2014-03-13 15:47:38,786 [Th 000013a4] INFO_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/networkservices/webauthservice/v2/Access/OnGuard
2014-03-13 15:47:38,995 [Th 000013a4] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
2014-03-13 15:47:38,996 [Th 000013a4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response={status=1, statusMsg=Authentication Failed, opaqueAuthState=, attributes=[]}
2014-03-13 15:47:38,996 [Th 000013a4] INFO_OnGuardPlugin.AuthSession - ProcessResponse: Authentication server returned status=1 msg=Authentication Failed
2014-03-13 15:47:38,996 [Th 000013a4] ERROR OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Null or empty SoHR recieved for Health Check mode

🕻 ClearPassOnGuard_0.log (896.0 KB) - BareTail
Elle Edit View Preferences Help
😰 Open 🥑 Highlighting 🔲 Follow Tail 🗛 SI 💽 C:Users/Deepak/AppData/Roaming/Aruba Networks/ClearPassOnGuard//ClearPassOnGuard_0.log (896.0 KB)
ClearPassOnGuard_0.log V winagert_0.log V
02014-03-13 15:47:38,785 [Th 000013a4] INFO OnGuardPlugin.WsHttpClient - GetRequestXml: Request=(username=dj, sohSize=1370, networkInterfaceInfo=(ip=10.20
02014-03-13 15:47:38,785 [Th 000013a4] INFO OnGuardPlugin.WsHttpClient - SubmitWebAuth: Posting request to URL=/v2/Access/OnGuard
02014-03-13 15:47:38,786 [Th 000013a4] INFO OnGuardPlugin.HttpClientWrapper - SetRequestEntity: Mime Type - text/xml Post Data Size - 3504
2014-03-13 15:47:38,786 [Th 000013a4] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://1
02014-03-13 15:47:38,995 [Th 000013a4] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
02014-03-13 15:47:38,995 [Th 000013a4] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 188
o 2014-03-13 15:47:38,996 [Th 000013a4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response=(status=1, statusMsg=Authentication Failed, opaqueAuthSt
o 2014-03-13 15:47:38,996 [Th 000013a4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Authentication server returned status=1 msg=Authentication Failed
o 2014-03-13 15:47:38,996 [Th 000013a4] ERROR OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Null or empty SoHR recieved for Health Check mode
02014-03-13 15:47:38,997 [Th 000013a4] INFO OnGuardPlugin.InterfaceSessionHelper - GenerateSessionExpiryMessage: No valid session timeout in response. Tim
c 2014-03-13 15:47:38,997 [Th 000013a4] DEBUG OnGuardPlugin.BackendClientInfoCollector - StartManaged: Start Managed called for interfaces=[Local Area Conne
o 2014-03-13 15:47:38,997 [Th 000013a4] DEBUG OnGuardPlugin.MessageRequestDispatcher - AddPendingResponse: Adding message id - 18
02014-03-13 15:47:38,997 [Th 000013a4] DEBUG OnGuardPlugin. MessageRequestDispatcher - SendMessage: Encoded message = 112:("content":("ifNames":["Local Area

If the Authentication is successful, then the **OnGuard Agent** forwards SoHR to **Backend Service** for processing. **Backend Service** processes SoHR which includes auto-remediation and final results are sent back to **OnGuard Agent** in form of remediation messages.

🔋 ClearPass OnGuard 6.3.1.61950
Health Status: Quarantined
Connection Details Diagnostics Settings
Health Status: Quarantined Logout INFO:Response processed

Once Health Check Results are processed by **Backend Service**, the **OnGuard Agent** checks if its health state has changed because of auto-remediation.

# OnGuard Plugin Logs (Authentication Passed and No Health Change After Processing SoHR):

2014 02-12 12:00:18 676 [Th 00000004] INFO. On Cuard Plugin Auth Soccion - Process Posponeo-Istatus-0. status-0. status-0. status-0.
opaqueAuthState=wcy1DvZOW8g3h3VKkjyUkg+XB5HLlbh5oa0AgpRGYgt9OvfP3QLJEuVQA=, attributes=[{N=BounceClient V=false}, {N=HealthCheckQuietPeriod V=0}, {N=Message V=Test}, ]}
2014-03-13 12:09:18,677 [Th 00000ee4] DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Language: <b>en SoHR:</b> 0x000702bb824adff010e044d3b
2014-03-13 12:09:18,679 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 2519:{"content":{"language":"en","remediate":true,"sohr":[0,7,2,-69,0,0,1,55,0,2,,120,36,-83,-1,1,14,4,77,59]},"id":14,"name":" <b>ProcessSoHRRequest</b> "}
2014-03-13 12:09:18,680 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>ProcessSoHRRequest</b> Timeout value (ms) – 300000
2014-03-13 12:09:21 725 [Th 00000c60] DEBUG OnGuardPlugin ConnectionReader - Read Data =
419:{"content":{" <b>healthStatus":false</b> ,"messages":[null,[10,0,70,0,,0,13,0]],"remediationURL":"","status":true},"id":14,"name":"ProcessSoHRResponse"}
2014-03-13 12:09:21,727 [Th 00000ee4] DEBUG OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: <b>Healthy - 0</b> Success - 1
2014-03-13 12:09:21,728 [Th 00000e4] INFO_OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response= Success=True <b>Healthy=False</b> Remediation URL= Msg: Msg: <b>Firewall Check:</b> Msg: Enable Microsoft Windows Firewall.
2014-03-13 12:09:21,728 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - ProcessSohrStatus: No remediation URL in response
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false 2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false 2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":16,"name":"QueryHealthStateChangeRequest"}
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false 2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":16,"name":"QueryHealthStateChangeRequest"} 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=QueryHealthStateChangeRequest Timeout value (ms) - 180000
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false 2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":16,"name":"QueryHealthStateChangeRequest"} 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=QueryHealthStateChangeRequest Timeout value (ms) - 180000
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false 2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":16,"name":"QueryHealthStateChangeRequest"} 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=QueryHealthStateChangeRequest Timeout value (ms) - 180000 2014-03-13 12:09:22,356 [Th 00000c60] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 77:{"content":{"status":false},"id":16,"name":"QueryHealthStateChangeResponse"}
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false 2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":16,"name":"QueryHealthStateChangeRequest"} 2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=QueryHealthStateChangeRequest Timeout value (ms) - 180000 2014-03-13 12:09:22,356 [Th 00000c60] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 77:{"content":{"status":false},"id":16,"name":"QueryHealthStateChangeResponse"} 2014-03-13 12:09:22,358 [Th 00000c64] DEBUG OnGuardPlugin.BackendClientInfoCollector - IsHealthStateChanged: QueryHealthStateChange Response =0
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: BounceClient=false         2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test         2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =         49:("id":16,"name": "QueryHealthStateChangeRequest")         2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for         request=QueryHealthStateChangeRequest Timeout value (ms) - 180000                   2014-03-13 12:09:22,356 [Th 00000c60] DEBUG OnGuardPlugin.ConnectionReader - Read Data =         77:("content":("status":false),"id":16,"name":"QueryHealthStateChangeResponse")         2014-03-13 12:09:22,358 [Th 00000ee4] DEBUG OnGuardPlugin.BackendClientInfoCollector - IsHealthStateChanged: QueryHealthStateChange Response         2014-03-13 12:09:22,358 [Th 00000ee4] DEBUG OnGuardPlugin.AuthSession - Authenticate: No health state change after first submit

ClearPassOnGuard 0.log (347.7 KB) - BareTail	s la s
Elle Edit View Preferences Help	
😂 Open 🌙 Highlighting 🗖 Follow Tail 🗛 🔽 🗖	C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (347.7 KB)
ClearPassOnGuard_0.log  winagent_0.log	< ▶
5 2014-03-13 12:09:18,676 [Th 00000ee4] INFo 0 2014-03-13 12:09:18,677 [Th 00000ee4] DEBU 0 2014-03-13 12:09:18,679 [Th 00000ee4] DEBU 0 2014-03-13 12:09:18,680 [Th 00000ee4] DEBU	OnGuardPlugin.AuthSession - ProcessResponse: Response=(status=0, statusMsg=, sohrSize=703, opaqueAuthState=wcy_A G OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Language: en SoHR: 0x000702hb00000137000202h50007001e00000 G OnGuardPlugin.MessageRequeStispatcher - SendMessage:Encoded message = 2519:"content"; ("language":"em","remed G OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=ProcessSoHRRequest Tim
0 2014-03-13 12:09:21,725 [Th 00000c60] DEBU	G OnGuardPlugin.ConnectionReader - Read Data = 419:("content":("healthStatus":false,"messages":[null,[10,0,70,0,
<ul> <li>2014-03-13 12:09:21,727 [Th 00000ee4] DEBU</li> <li>2014-03-13 12:09:21,728 [Th 00000ee4] INFO</li> <li>Firewall Check: Msg; Enable Microsoft Wind</li> </ul>	G OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: Healthy - O Success - OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response= Success=True Healthy=False Remediation UR ows Firevall.
	a Andread Diversa Internation - December 400 March 10 Annual (1997 - 199
2014-03-13 12:09:21,729 [Th 000000ee4] DEBU	© OnQuarteringin, Authoession - processionistatus: No remediation UKA in tesponse © OnQuarteringingin, uthoession - getterfProfileAttrs: Auth Attribute: BounceClient=false
0 2014-03-13 12:09:21,729 [Th 00000ee4] DEBU	G OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: HealthCheckQuietPeriod=0
0 2014-03-13 12:09:21,729 [Th 00000ee4] DEBU	G OnGuardPlugin.AuthSession - GetEnfProfileAttrs: Auth Attribute: Message=Test
0 2014-03-13 12:09:21,729 [Th 00000ee4] INFO	OnGuardPlugin.InterfaceSessionHelper - GenerateSessionExpiryMessage: No valid session timeout in response. Time
0 2014-03-13 12:09:21,729 [Th 00000ee4] DEBU	G OnGuardPlugin.MessageRequestDispatcher - AddPendingResponse: Adding message id - 16
0 2014-03-13 12:09:21,730 [Th 00000ee4] DEBU	G OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":16,"name":"QueryHealthStateChar
2014-03-13 12:09:21,730 [Th 00000ee4] DEBU	G OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=QueryHealthStateChangeF
02014-03-13 12:09:22,356 [Th 000000c60] DEBU	G OnGuardPlugin.ConnectionReader - Read Data = 77:("content":("status":false),"id":16,"name":"QueryHealthStateCha
2014-03-13 12:09:22 358 [Th 00000ee4] DEBIN	C OnGuardDlugin RackandCliantInfoCollector _ TaHaalthStateChanged. OueruHealthStateChange Resnonse =0
2014-03-13 12:09:22.358 [Th 00000ee4] INFO	OnGuardPlugin.AuthSession - Authenticate: No health state change after first submit
◆ 2014-03-13 12:09:22.358 [Th 00000ee4] DEBU	G OnGuardPlugin.AuthSession - Authenticate: Local Area Connection is Unhealthy.

# Backend Service Logs (Process SoHR – No Health Change):

2014-03-13 16:05:25,477 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 2519:{"content":{"language":"en","remediate":true,"sohr":[0,7,2,-69,0,0,1,55,0,2,2,-77,0,36,-83,- 1,1,14,4,77,59]},"id":18,"name":" <b>ProcessSoHRRequest</b> "}
2014-03-13 16:05:25,485 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.ProcessSoHRMessageHandler - Processing health response
2014-03-13 16:05:25,497 [Th 00000d38 Evt 04F64030] INFO WinAgent.WinAgentHealthProcessor - Remediation flag from SSoH = 0  <b>Remediation flag</b> from ProcessSoHR = 1 Remediation URL =
2014-03-13 16:05:27,172 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: <b>Processing ClearPass Windows Universal</b> System compressed SoHR
2014-03-13 16:05:27,185 [Th 0000019C] INFO_WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: <b>Status of Firewall Health Class is</b> <mark>Not_Healthy. Global Remediate Flag - 0</mark>
2014-03-13 16:05:27,187 [Th 0000019C] INFO_WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Application Microsoft Windows Firewall is Unhealthy.
2014-03-13 16:05:27,187 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - GetEnableRemediationAttrValue: Value of EnableRemediation attribute of Application Microsoft Windows Firewall is 1
2014-03-13 16:05:27,188 [Th 0000019C] ERROR WinSHA.HealthFactoryEx - ProcessHealthResponse: Processing Health Class - 2 response failed.
2014-03-13 16:05:27,195 [Th 0000019C] ERROR WinSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - <b>Processing</b> failed.
2014-03-13 16:05:27,196 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message= <b>Firewall Check:</b> 2014-03-13 16:05:27,196 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message= <b>Enable Microsoft Windows</b> Firewall. 2014-03-13 16:05:27,197 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentHealthProcessor - ProcessHealthResponse: Done
2014-03-13 16:05:27,198 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 419:{"content":{ <b>"healthStatus":false</b> ,"messages":[null,[10,0,70,0,46,0,13,0]],"remediationURL":"","status":true},"id":18,"name":" <b>ProcessSoHRResponse</b> "}
I construction of the second se
2014-03-13 16:05:27,216 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 49:("id":20 "name":"OuervHealthStateChangeRequest"}

2014-03-13 16:05:27,217 [Th 00000d38 Evt 04F64030] INFO JavaAgent.WinHealthDataCollector - **isHealthStateChanged**: Start collecting health info 2014-03-13 16:05:27,218 [Th 00000d38 Evt 04F64030] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - Firewall (2) 2014-03-13 16:05:28,036 [Th 00000d38 Evt 04F64030] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Finished collecting Health of the Client 2014-03-13 16:05:28,044 [Th 00000d38 Evt 04F64030] INFO JavaAgent.WinHealthDataCollector - **isHealthStateChanged**: **Health state has not changed** 2014-03-13 16:05:28,044 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinHealthDataCollector - **isHealthStateChanged**: **Health state has not changed** 2014-03-13 16:05:28,044 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message=QueryHealthStateChangeRequest

2014-03-13 16:05:28,044 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 77:{"content":{**"status":false**},"id":20,"name":"QueryHealthStateChangeResponse"}

🕽 winagent_0.log (250.2 KB) - BareTail	_0×
Elle Edit View Breferences Help	
CVProgramDataVaruba Networks/ClearPassDnGuard/winagen_DIog (250.2 KB)	
ClearPassOnGuard_0.0g 🛡 winagent_0.log 🔻	
o 2014-03-13 16:05:25,477 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 2519:("content":("language":"en", "remediate":	rue,"soh
0. . Bria no io iconecide des (TR nononico But national Berlin Minister Decompositedine - Decomposite totte toppose	
a a a a a a a a a a a a a a a a a a a	
o 2014-03-13 16:05:25,497 [Th 00000d38 Evt 04F64030] INFO WinAgent.WinAgentHealthProcessor - Remediation flag from SSoH = 0 Remediation flag from Pro	cessSoHR
02014-03-13 16:05:25,497 [Th 00000d38 Evt 04F64030] INFO Winkgent.WinkgentHealthProcessor - ProcessHealthResponse: Remediate Flag - 0	
0. 02014-03-13 16:05:27,172 (Th 000001901 DEBNG Javakgent, WinHealthDataCollector - processHealthDesnonse: Processing ClearPass Windows Universal System	compress
	Compileoo,
o 2014-03-13 16:05:27,185 [Th 0000019C] INFO WinSHA.SysInfoHealthClassInfoFactory - ProcessHealthResponse: Status of SystemInfo Health Class is Healt	hy
o 2014-03-13 16:05:27,185 [Th 00000190] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Processing Health Class - O response succeeded.	() - h - h
olut-us-is lo:Us:2/,los [in 0000190] info winshk.fwhealthclassiniofactory - Processnealthkesponse: Status of Firewall health class is Not_healthy.	GIODAL .
02014-03-13 16:05:27,187 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Application Microsoft Windows Firewall is Unhee	althy.
02014-03-13 16:05:27,187 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - GetEnableRemediationAttrValue: Value of EnableRemediation attribute of	: Applica
22014-03-13 16:05:27,187 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - GetEnableNotificationAttrValue: Value of EnableNotification attribute	of Appli
2. 2014-03-13 16:05:27.187 [Th 00000190] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Reply from Server contains FirewallUpdateStatus att	ribute
o 2014-03-13 16:05:27,188 [Th 0000019C] ERROR WinSHA.HealthFactoryEx - ProcessHealthResponse: Processing Health Class - 2 response failed.	
0/2/14-03-13 16:U5:27,195 [Th UUUUU19C] ERKOK WINSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - Processing Tailed	
2014-03-13 16:05:27,195 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing health response done. Quarantine mu	sg=
o 2014-03-13 16:05:27,196 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message=	
o Firewall Check: 2014-03-13 16:05:27, 196 [Th 0000019C] DEBUG JavaAgent. WinHealthDataCollector - processHealthResponse: Adding message=Enable Microsoft	. Windows
QU14-03-13 16:0527,197 [In 0000035 EVE 04F64030] DEBUG Windgent.WindgentRealFMandler - Successfully processed for message=ProcessonKRequest QU14-03-13 16:0527,198 [In 00000185 EVE 04F64030] DEBUG Windgent.WindgentFWendler - Encoded message = 419:("contentr":("healthStatus":false."met	sages": []
	Cageo . [
o 2014-03-13 16:05:27,216 [Th 00000d38 Evt 04F64030] DEBUG Winkgent.WinkGentReadEvHandler - Read data = 49:("1d":20,"name":"QueryHealthStateChangeRequ	lest")
0. - 2014 02.12.15:05:07.217 FTK 00000422 Fut 045540201 TNFO. Levelgave WinHealthDeteCollector. isHealthStateChanged: Start collecting kealth info	
2014-05-13 16:05:27,217 [H 00000035 EV: 04F64050] INFO Savaget.sinteritimatacuritector = Isheartchatactenanget: Start Correcting meatin file 2014-05-13 16:05:27,217 [H 00000035 EV: 04F64030] DEBIG WinSHA.HealthFactoryEV = GetHealthFactoryEV	
02014-03-13 16:05:27,218 [Th 00000d38 Evt 04F64030] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - SystemInfo (0)	
2014-03-13 16:05:27,218 [Th 000000d38 Evt 04F64030] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - Firewall (2)	_
a.	
o 2014-03-13 16:05:28,044 [Th 00000d38 Evt 04F64030] INFO Javakgent.WinHealthDataCollector - isHealthStateChanged: Health state has not changed	
o 2014-03-13 16:05:28,044 [Th 00000038 Evt 04F64030] DEBUG Winkgent.WinkGentReadEvMandler - Successfully processed the message=QueryHealthStateChangel	equest
DEU14-03-13 16:05:28,044 [In 00000038 Evt 04F64030] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 77:("content":("status":false),"id":20,"i	ame":"Qu
	Þ

If the **OnGuard Agent** detects change in health state, it sends another WebAuth Request (a client may become healthy after auto-remediation) and processes the Response.



# OnGuard Plugin Logs (Authentication Passed and Health Changed After Processing SoHR):

2014-03-13 16:47:53,877 [Th 00001004] INFO_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/networkservices/webauthservice/v2/Access/OnGuard
2014-03-13 16:47:54,043 [Th 00001004] INFO_OnGuardPlugin.AuthSession - ProcessResponse: Response={status=0, statusMsg=, sohrSize=428, opaqueAuthState=wcy1DvZOU9YU8Bk0JrHQ, attributes=[]}
2014-03-13 16:47:54,044 [Th 00001004] DEBUG OnGuardPlugin.InterfaceSessionHelper - <b>ProcessSohr</b> : Language: en SoHR: 0x000701a80000013700028f881c3cbbed6aba13ed02efafa37f21867fc
2014-03-13 16:47:54,045 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 1492:{"content":{"language":"en","remediate":true,"sohr":[0,7,1,-88,0,0,1,55,0,2,1,-96,046,-6,-6,55,-14,24,103,- 4]},"id":18,"name":" <b>ProcessSoHRRequest</b> "}
2014-03-13 16:47:54,045 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>ProcessSoHRRequest</b> Timeout value (ms) - 300000
2014-03-13 16:47:56,484 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 493:{"content": <b>{"healthStatus":false,"</b> messages":[null,[10,0,70,0,105,0,111,0,110,0,46,0,13,0]],"remediationURL":"","status":true},"id":18,"name":" <b>Pr</b> <mark>ocessSoHRResponse"}</mark>
2014-03-13 16:47:56,487 [Th 00001004] DEBUG OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: Healthy - 0 Success - 1
2014-03-13 16:47:56,487 [Th 00001004] INFO OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response= Success=True <b>Healthy=Fals</b> e Remediation URL= Msg: Msg:
Firewall Check: Enabled Microsoft Windows Firewall application.
2014-03-13 16:47:56,488 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":20,"name":" <b>QueryHealthStateChangeRequest</b> "}
2014-03-13 16:47:56,488 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>QueryHealthStateChangeRequest</b> Timeout value (ms) - 180000
2014-03-13 16:47:56,653 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 76:{"content":{" <b>status":true</b> },"id":20,"name":" <b>QueryHealthStateChangeResponse</b> "}
2014-03-13 16:47:56,655 [Th 00001004] INFO OnGuardPlugin.AuthSession - Authenticate: Health state has changed after first submit

2014-03-13 16:47:	:56,655 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =
44:{"id":22,"name'	":"CollectHealthDataRequest"}
2014-03-13 16:47:	:56,656 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request= <b>CollectHe</b>	ealthDataRequest Timeout value (ms) - 1200000
2014-03-13 16:47:	:56,701 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
71:{"content":{"sta	atus":true},"id":22,"name":" <b>CollectHealthDataResponse</b> "}
2014-03-13 16:47;	:56,703 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =
30:{"id":24,"name'	": <b>"SoHRequest</b> "}
2014-03-13 16:47:	:56,703 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>SoHReques</b>
Timeout value (ms	s) - 180000
2014-03-13 16:47:	:56,713 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 2561:{"content":{"soh":[0,7,3,65,0,0,1,55,0,55,-
128,0,4,2,0]},"id":2	24,"name":" <b>SoHResponse</b> "}
1	
2014-03-13 16:47:	:56,725 [Th 00001004] DEBUG OnGuardPlugin.AuthSession - <b>SubmitWebAuthRequest</b> : Authenticating user dj. Retry count=0
• 2014-03-13 16:47: https://10.17.4.23	:56,744 [Th 00001004] INFO_OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: ;4/networkservices/webauthservice/v2/Access/OnGuard
2014-03-13 16:47:	:56,930 [Th 00001004] INFO_OnGuardPlugin.AuthSession - ProcessResponse: Response={status=0, statusMsg=, sohrSize=409,
opaqueAuthState=	wcy1DvZOWZU9YU8Bk0JrHQ, attributes=[{N=BounceClient V=false}, {N=HealthCheckQuietPeriod V=0}, {N=Message V=Test}, ]}
<mark>2014-03-13 16:47:</mark>	:56,931 [Th 00001004] DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Language: en SoHR:
0x000701950000(	01370002018d
2014-03-13 16:47:	:56,932 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =
1419:{"content":{"	'language":"en","remediate":true,"sohr":[0,7,1,-107,0,0,1,55,0,2,1,-115,0,7,0,30,1,97,-
115,96,106]},"id":2	28,"name":" <b>ProcessSoHRRequest</b> "}
2014-03-13 16:47:	:56,933 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request= <b>ProcessS</b>	oHRRequest Timeout value (ms) - 300000
2014-03-13 16:47:	:58,546 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
123:{"content":{"h	lealthStatus":true,"messages":[null],"remediationURL":"","status":true},"id":28,"name":" <b>ProcessSoHRResponse</b> "}
2014-03-13 16:47:	:58,548 [Th 00001004] INFO OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response= Success=True Healthy=True

2014-03-13 16:47:58,548 [Th 00001004] INFO OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response Remediation URL= Msg:

🛟 ClearPassOnGuard_0.log (97.0 KB) - BareTail	٦×
Elle Edit View Preferences Help	
😂 Open 🖉 Highlighting 🗖 Follow Tail 🗛 NST 🤍 C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log(97.0 KB)	
(ClearPassOnGuard_0.log ▼ winagert_0.log ▼	×
2014-03-13 16:47:53.877 [Th 00001004] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://j	10 -
0 2014-03-13 16:47:54,043 [Th 00001004] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response=(status=0, statusHsg=, sohrSize=428, opaqueAuthState=work	y1
2014-03-13 16:47:54,044 [Th 00001004] DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Language: en SoHR: 0x000701a8000001370002	
0 2014-03-13 16:47:54,045 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 1492:("content":("language":"en","remed	di.
02014-03-13 16:47:54,045 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=ProcessSoHRRequest Tir	me
02014-03-13 16:47:56,484 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 493:("content":("healthStatus":false,"messages":[null,[10,0,70,0,	, 1
0 2014-03-13 16:47:56,487 [Th 00001004] DEBUG OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: Healthy - 0 Success -	
2014-03-13 16:47:56,487 [Th 00001004] INFO OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response= Success=True Healthy=False Remediation UK	RI
o Firewall Check: Msg: Enabled Microsoft Windows Firewall application.	
2014-03-13 16:47:56.488 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:("id":20."name":"OpervHealthStateChe	ar
2014-03-13 16:47:56.488 [Th 00001004] DEBUG OnGuardPlugin, MessageRequestDispatcher - WaitForResponse: Wait for response for request=OvervHealthStateChange	e i
o 2014-03-13 16:47:56,653 [Th 0000107c] DEBUG OnGuardPlugin. ConnectionReader - Read Data = 76:("content":("status":true),"id":20,"name":"OuervHealthStateChe	ar
2014-03-13 16:47:56,655 [Th 00001004] INFO OnGuardPlugin.AuthSession - Authenticate: Health state has changed after first submit	-
o 2014-03-13 16:47:56,655 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:("id":22,"name":"CollectHealthDataRe	ec
o 2014-03-13 16:47:56,656 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataReque	es
o 2014-03-13 16:47:56,701 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:("content":("status":true),"id":22,"name":"CollectHealthDataRe	es
2014-03-13 16:47:56,703 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 30:("id":24,"name":"SoHRequest")	
02014-03-13 16:47:56,703 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=SoHRequest Timeout val	.lı
2014-03-13 16:47:56,713 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 2561:("content":("soh":[0,7,3,65,0,0,1,55,0,55,-12	28
0. 2014.02-12 16:47:56 725 (Th 00001004) DEPUG (mcMartelumin hutbénging - SubwitEnblutbengungt, hutbentigating upper di Dater gaunt-0	
o.	
2014-03-13 16:47:56,744 [Th 00001004] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://J	10
2014-03-13 16:47:56,929 [Th 00001004] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200	
0 2014-03-13 16:47:56,930 [Th 00001004] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response=(status=0, statusMsg=, sohrSize=409, opaqueAuthState=work	y1
2014-03-13 16:47:56,931 [Th 00001004] DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Language: en SoHR: 0x00070195000001370002018d	
02014-03-13 16:47:56,932 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 1419:("content":("language":"en","remed	di
02014-03-13 16:47:56,933 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=ProcessSoHRRequest Tir	me
02014-03-13 16:47:58,546 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 123:("content":("healthStatus":true,"messages":[null],"remediation	or
2014-03-13 16:47:58,548 [Th 00001004] INFO OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response= Success=True Healthy=True Remediation URI	.L=
	-
	• //

# Backend Service Logs (SoHR Processing -Health Changed after Auto-Remediation):

2014-03-13 16:47:54,063 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Read data =
1492:{"content":{"language":"en","remediate":true,"sohr":[0,7,1,-88,0,0,1,55,0,2,1,-96,0,7,0,30,0,0,1,55,35,72,0,0,-66,24,0,0,-124,103,0,0,-
31,74,0,0,108,61,0,0,-42,44,0,0,0,0,0,2,0,4
2014.02.13.16.47.55.602 [Th.0000010C] DERUC Java Agent Win Health Data Collector _ process Health Decourses Processing Clear Pass Windows Universal
2017-05-15 10.47.55,005 [11:00000176] DEDOG Javangent. Winneartinbataconector - processineartinkesponse. Frocessing clear ass windows onversai
System compressed softw
2014-03-13 16:47:55,610 [Th 0000019C] DEBUG WinSHA.HealthFactoryEx - ProcessHealthResponse: Started processing Health Response. Remediate
Flag - 1
2014-03-13 16:47:55.610 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not Healthy.
Global Remediate Flag - 1
2014 02 12 17 47 FF (12) [Th 00000100] INFO With CHATCHARD IN Classify Franking Descare Chatter Atter Deschart Id (015 Deschart Version, 7
2014-03-13 16:47:55,612 [10 0000019C] INFO WINSHAF WHEalthClassinioractory - ProcessitatusAttr: Product Id: 6015 Product Version: 7
2014-03-13 16:47:56,467 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Firewall application Microsoft Windows Firewall
enabled
2014-02-13 16:47:56 469 [Th 0000019C] INFO. WinSHA HealthFactoryEx - ProcessHealthPesponse: Remediation of Health Class - 2 succeeded
2014-03-13 16:47:56,471 [Th 0000019C] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - Remediation
succeeded.
2014-03-13 16:47:56,472 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message=
Firewall Check: Enabled Microsoft Windows Firewall annication
r newan eneck. Enabled File osoft w indows i newan application.
2014-03-13 16:47:56,475 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the
message=ProcessSoHRRequest
2014 02 12 16:47:56 475 [Th 000015ac Fut 04F5C679] DEPLIC WinAgent WinAgent FuentHandler - Encoded message -
492 ("contant", ("health Status" follo "more space" (ou) [10,0,70,0]
To a content of nearboards rates, interstages, intuil[10,07,00,
U,11U,U,40,U,13,UJJ, remediationUKL : , Status :true}, Id :18, name : ProcessSOHKKesponse }

2014-03-13 16:47:56,494 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 49:{"id":20,"name <b>":"QueryHealthStateChangeRequest</b> "}
2014-03-13 16:47:56,501 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Started collecting Health of the Client
2014-03-13 16:47:56,645 [Th 000015ac Evt 04F5C678] INFO WinSHA.FWHealthClassInfoFactory - GetProductStatus: Firewall Status - Enabled
2014-03-13 16:47:56,646 [Th 000015ac Evt 04F5C678] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - Firewall (2)
2014-03-13 16:47:56,650 [Th 000015ac Evt 04F5C678] INFO JavaAgent.WinHealthDataCollector - isHealthStateChanged: Health state has changed
2014-03-13 16:47:56,650 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message= <b>QueryHealthStateChangeRequest</b>
2014-03-13 16:47:56,650 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 76:{"content": <b>{"status":true</b> },"id":20,"name <b>":"QueryHealthStateChangeResponse</b> "}
2014-03-13 16:47:56,662 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 44:{"id":22,"name":" <b>CollectHealthDataRequest</b> "}
2014-03-13 16:47:56,664 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Started collecting Health of the Client
2014-03-13 16:47:56,664 [Th 000015ac Evt 04F5C678] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - Firewall (2)
2014-03-13 16:47:56,667 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Finished collecting Health of the Client
2014-03-13 16:47:56,692 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message= <b>CollectHealthDataRequest</b>
2014-03-13 16:47:56,692 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 71:{"content":{"status":true},"id":22,"name":" <b>CollectHealthDataResponse</b> "}
2014-03-13 16:47:56,704 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 30:{"id":24,"name":" <b>SoHRequest</b> "}
2014-03-13 16:47:56,707 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message=SoHRequest
2014-03-13 16:47:56,708 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 2561:{"content":{"soh":[0,7,3,65,0,0,1,55,0,,8,0,1,55,-128,0,4,2,0]},"id":24,"name":" <b>SoHResponse</b> "}
2014-03-13 16:47:56,939 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 1419:{"content":{"language":"en","remediate":true,"sohr":[0,7,1,-107,0,0,1,-46,50,62,1,97,-115,96,106]},"id":28,"name":" <b>ProcessSoHRRequest</b> "}
2014-03-13 16:47:58,522 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing ClearPass Windows Universal System compressed SoHR
2014-03-13 16:47:58,532 [Th 0000019C] DEBUG WinSHA.HealthFactoryEx - ProcessHealthResponse: Started processing Health Response. Remediate Flag - 0
2014-03-13 16:47:58,532 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Healthy
2014-03-13 16:47:58,535 [Th 0000019C] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - Processing succeeded.
2014-03-13 16:47:58,537 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message= <b>ProcessSoHRRequest</b>
2014-03-13 16:47:58,537 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 123:{"content":{ <b>"healthStatus":true</b> ,"messages":[null],"remediationURL":"","status":true},"id":28,"name":" <b>ProcessSoHRResponse</b> "}

🕽 winagent_0.log (206.8 KB) - BareTail	
Elle Edit View Breferences Help	
😰 Opeg 🤣 Highlighting 🔽 Follow Tail 🗛 St 👱 CAProgramData/Aruba Networks/ClearPassOnGuard/winagent_0.log (206.8 KB)	
ClearPassOnGuard_0.log  winagent_0.log	> X
o 2014-03-13 16:47:54,063 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 1492:("content":("language":"en","remediate":true,	"sol 🔺
to 2014-03-13 16:47:55,603 [Th 00000190] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing ClearPass Windows Universal System computed and a statistic	ces:
2014-03-13 16:47:55,610 [Th 00000156] DNFO WINSH.SysIndHealthClassInfoFactory - ProcessMealthResponse: Status of SystemInfo Health Class is Healthy	
2014-03-13 16:47:55,610 [Th 0000019C] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Remediation of Health Class - O succeeded.	
02014-03-13 16:47:55,610 [Th 00000190] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_HealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_HealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_HealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_HealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_HealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_HealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health ClassInfoFactory - ProcessHealthResponse: Status of Firewall HealthResponse: Status of Firewall Health ClassInfoFactory - ProcessHealthResponse: Status of Firewall Health ClassInfoFactory - ProcessHealthResponse: Status of Firewall Health ClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Cl	oal
10/2014-03-13 16:47:55,612 [IN UUUUU90] INFO WINSHA.FWHEALTALASSINTOFACTORY - ProcessStatuSATCT: Product A: bulb Product Version: /	
2014-03-13 16:47:55,469 [Th 0000019] INFO WINSHA.HealthFactoryEx - ProcessHealthResponse: Remediation of Health Class - 2 succeeded.	
02014-03-13 16:47:56,471 [Th 0000019C] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - Remediation succeeded	
lo 2014-03-13 16:47:56,472 [Th 0000019C] DEBUG JavaAgent, WinHealthDataCollector - processHealthResponse: Adding message=	C
portrevari check: Enduted nicrosoft windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:56,475 [in Oubriad Eve Orfschorg] Debug windows frewari approache.col=05-13 16:47:	s":
o 2014-03-13 16:47:56,494 [Th 000015ac Evt 04F5C678] DEBUG Winkgent.WinkGentReadEvHandler - Read data = 49:("id":20,"name":"QueryHealthStateChangeRequest".	
o 2014-03-13 16:47:56,496 [Th 000015ac Evt 04F5C678] DEBUG Winkgent.QueryHealthStateChangeMessageHandler - Inside QueryHealthStateChangeMessageHandler()	
De2014-03-13 16:47:56,551 [Th 000015ac Evt 04F5C676] INFO JavaAgent.WinHealthDataCollector - isHealthStateChanged: Start collecting health info 2014-03-13 16:47:56,551 [Th 000015ac Evt 04F5C678] INFO JavaAgent.WinHealthDataCollector - isHealthStateChanged: Start collecting health of 2014-03-13 16:47:56,551 [Th 000015ac Evt 04F5C678] INFO JavaAgent.WinHealthDataCollector - isHealthStateChanged: Start collecting health of Collecting and Collecting health of the collecting health of the collecting health of the collecting health of the Collecting health of the collecting health of the coll	
2014-03-13 16:47:55,502 [Th 000015ac bvt 04756578] DEBG WinSHA FWHealthClassInforactory - GetHealth: Updating cached Firewall Health Class Info.	
0 2014-03-13 16:47:56,645 [Th 000015ac Evt 04F5C678] INFO WinSHA.FWHealthClassInfoFactory - GetProductStatus: Firewall Status - Enabled	
2014-03-13 16:47:56,645 [Th 000015ac Evt 04F5C678] INFO WinSHA, FWHealthClassInfoFactory - GetHealth: Adding Firewall application Microsoft Windows Fire	wal.
a 2014-03-13 16:47:56,550 [In OUDISAC EVE OFFSCH/G] INFO WINSAR REALFRACEOFYX - GetHealthRequest: Adding Health Class Info - FifeWall (2) 2014-03-13 16:47:56,550 [In OUDISAC EVE OFFSCH/G] INFO WINSAR REALFRACEOFYX - GetHealthRequest: Adding Health Class Info - FifeWall (2) 2014-03-13 16:47:56,550 [In OUDISAC EVE OFFSCH/G] INFO WINSAR REALFRACEOFYX - GetHealthRequest: Adding Health Class Info - FifeWall (2) 2014-03-13 16:47:56,550 [In OUDISAC EVE OFFSCH/G] INFO WINSAR REALFRACEOFYX - GetHealthRequest: Adding Health Class Info - FifeWall (2) 2014-03-13 16:47:56,550 [In OUDISAC EVE OFFSCH/G] INFO WINSAR REALFRACEOFYX - GetHealthRequest: Adding Health Class Info - FifeWall (2) 2014-03-13 16:47:56,550 [In OUDISAC EVE OFFSCH/G] INFO WINSAR REALFRACEOFYX - GETHEALTHREAD LESS ADDING HEALTH ENDING	
o 2014-03-13 16:47:56,650 [Th 000015ac Evt 04F5C678] DEBUG Winkgent.WinkGentReadEvHandler - Successfully processed the message=QueryHealthStateChangeRequer	st
o 2014-03-13 16:47:56,650 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 76:("content":("status":true),"id":20,"name":)	"Que
o 2014-03-13 16:47:55,562 [Th 000015ac Evt 04750578] DEBUG Winkgente WinkGentReadEvHandler - Read data = 44:("id":22,"mame":"CollectHealtDataRequest")	
2014-05-13 16:47:56.664 [Th 000015ac Evt 0475676] DE00 WinSHA.HealthRecury - GethealthRequest: Statict Confecting means of the Chemical Confecting Confect	
0 2014-03-13 16:47:56,667 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Finished collecting Health of the Client	
o 2014-03-13 16:47:56,692 [Th 000015ac Evt 04F5C678] DEBUG Winkgent.WinkGentReadEvHandler - Successfully processed the message=CollectHealthDataRequest	
<pre>bold14-03-13 16:47:55,592 [Th OU0015ac Evt O4FSC5/6] DEBUG Windgent WindgentEventHandler - Encoded message = 71:["content":("Status":true)"10":22,"name": 2014-03:13 16:47:55,704 [Th OU0015ac Evt O4FSC5/8] DEBUG Windgent Windgent Pachtment = Read data = 30:["dift":24 Imagent":"SOBGenuest"]</pre>	7C0
2014-03-13 16:47:55,707 [Th 000015ac Evt 0475:678] DEBUG Winkgent.WinkGentReadEvMandler - Successfully processed the message=SoffRequest	
o 2014-03-13 16:47:56,708 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 2561:("content":("soh":[0,7,3,65,0,0,1,55,0,.	
o 2014-03-13 16:47:55,939 [Th 000015ac Evt 04F5C678] DEBUG WinAgent WinAGentReadEvHandler - Read data = 1419:("content":("language":"enu", "remediate":true,	"sol
2014-03-13 16:47:59.522 [IN 0000156] DEBUG WARAGENERATOREACOFIECCOF = processing companying companying and a second companying a s	
0 2014-03-13 16:47:58,532 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Healthy	
o 2014-03-13 16:47:58,535 [Th 0000019C] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - Processing succeeded	
Ducut-us-is 1:4/:55/53/ [in uuuulsac EVC UPICE/3] DEBUG Windern Windern Kandkar - Successfully processed the message=processOHRequest	
	<u> </u>
	<u> </u>

# **Agent Enforcement Actions**

After processing the response, the **OnGuard Agent** performs Agent Enforcement Actions. There are several possible actions –

- 1. Bounce the Network Interface.
- 2. Set Session Timeout.
- 3. Display Agent Enforcement Message.
- 4. Set Health Check Interval (Added in 6.3.1).

### **OnGuard Plugin Logs (Agent Enforcement Action – Bounce Interface):**

2014-03-17 11:57:51,192 [Th 00000e14] INFO_OnGuardPlugin.AuthSession - DoEnforcementActions: Enforcement actions for Local Area Connection: Bounce=1 timeout=-1 secs messages='You are Healthy! healthcheckquietperiod=-1 secs'
2014-03-17 11:57:51,199 [Th 00000e14] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 87:{"content":{"ifName":"Local Area Connection"},"id":26,"name":" <b>BounceInterfaceRequest</b> "}
2014-03-17 11:57:51,199 [Th 00000e14] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>BounceInterfaceRequest</b> Timeout value (ms) - 180000
1
2014-03-17 11:57:51,646 [Th 000005cc] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName <b>":"Local Area</b> Connection","ifName":"Local Area Connection","ifTyne":"WIRED,","inAddress":"10.20.23,123","macAddress":"001d09cca2bc"},"id":5,"name":"InterfaceDown"}
2014-03-17 11:57:51,648 [Th 000005cc] DEBUG OnGuardPlugin.BackendClientMessageHandler - ProcessNotificationMessage: Received InterfaceDown Message. IfName=Local Area Connection, IP Address=10.20.23.123
2014-03-17 11:57:51,648 [Th 000005cc] DEBUG OnGuardPlugin.AgentController - InterfaceDown: InterfaceDown message received from backend server for Local Area Connection
2014-03-17 11:57:57,715 [Th 000005cc] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 69:{"content":{"status":true},"id":26,"name":" <b>BounceInterfaceResponse</b> "}
2014-03-17 11:57:57,719 [Th 00000e14] DEBUG OnGuardPlugin.BackendClientInfoCollector - BounceInterface: Bounce Interface Response Status =1
2014-03-17 11:57:58,008 [Th 000005cc] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 185:{"content":{"displayName <b>":"Local Area</b> Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":7,"name":"InterfaceUp"}
2014-03-17 11:57:58,011 [Th 000005cc] DEBUG OnGuardPlugin.AgentController - InterfaceUp: InterfaceUp message received from backend server for Local Area Connection



# **Backend Service Logs (Bounce Interface):**

2014-03-17 11:57:51,219 [Th 000000d8 Evt 04DF7530] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 87:{"content":{"ifName":"Local Area Connection"},"id":26,"name":" <b>BounceInterfaceRequest</b> "}
2014-03-17 11:57:51,221 [Th 000000d8 Evt 04DF7530] INFO_WinAgent.WinAgentNetworkProcessor - CWinAgentNetworkProcessor:: <b>BounceInterface(</b> ) IfName= <b>Local Area Connection</b>
2014-03-17 11:57:51,393 [Th 000000d8 Evt 04DF7530] INFO_WinAgent.WinAgentNetworkControl <b>- Disabling the Network interface Local Area</b> Connection
2014-03-17 11:57:51,562 [Th 00000fe0] DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification
2014-03-17 11:57:51,576 [Th 000001E0] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
2014-03-17 11:57:51,576 [Th 000001E0] INFO_WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=1 Current num interfaces=0
2014-03-17 11:57:51,577 [Th 000001E0] WARN_WinAgent.WinAgentNetworkProcessor - The interface information has changed. Following interface information has changed. Following interface information, ip={10.20.23.123} mac={00:1d:09:cc:a2:bc} can't be found
2014-03-17 11:57:51,641 [Th 000001E0] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 187:{"content":{"displayName <b>":"Local Area</b> Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":5,"name":"InterfaceDown"}
2014-03-17 11:57:53,512 [Th 000000d8 Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Successfully disabled(BOUNCE) the Network interface Local Area Connection
2014-03-17 11:57:55,513 [Th 000000d8 Evt 04DF7530] INFO_WinAgent.WinAgentNetworkControl - Enabling the Network interface Local Area Connection

2014-03-17 interface L	11:57:57,664 [Th 000000d8 Evt 04DF7530] INFO_WinAgent.WinAgentNetworkControl - Successfully enabled(BOUNCE) the Network ocal Area Connection
2014-03-17 message=I	11:57:57,695 [Th 000000d8 Evt 04DF7530] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the SounceInterfaceRequest
2014-03-17 69:{"conter	11:57:57,695 [Th 000000d8 Evt 04DF7530] DEBUG WinAgent.WinAgentEventHandler - Encoded message = it":{"status":true},"id":26,"name":" <b>BounceInterfaceResponse</b> "}
2014-03-17 notification	11:57:57,907 [Th 00000fe0] DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change
2014-03-17	11:57:57,935 [Th 000001E0] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
2014-03-17 interfaces	11:57:57,935 [Th 000001E0] INFO_WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num =0 Current num interfaces=1
l	
2014-03-17 <mark>network i</mark> r	11:57:57,935 [Th 000001E0] WARN_WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new terface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc}
l	
2014-03-17 Connection	11:57:57,939 [Th 000001E0] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 185:{"content":{"displayName": <b>"Local Area</b> ","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":7,"name":" <b>InterfaceU</b>

🕽 winagent_0.log (551.0 KB) - BareTail
Ele Edit View Preferences Help
🗳 Opeg 🤣 Highlighting 🔽 Folloy Tail ASCII 💽 C.\Program Data Varuba Networks\ClearPassOnGuard/winagent_0.log (551.0 KB)
ClearPassOnGuard (0.log ) winagent (0.log )
o Evt 04DF7530] DEBUG WinAgent.WinAGentReadEvHandler - Read data = 87:("content":("ifName":"Local Area Connection"),"id":26,"name":"BounceInterfaceRequest", o Evt 04DF7530] INFO WinAgent.WinAgentNetworkProcessor - CWinAgentNetworkProcessor::BounceInterface() IfName=Local Area Connection
o Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection
<ul> <li>DEBUG Winkgent.WinkgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification</li> </ul>
o] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
<ul> <li>DINFO Windgent.WindgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=1 Current num interfaces=0</li> </ul>
o WARN Winkgent.WinkgentNetworkProcessor - The interface information has changed. Following interface information, ip=(10.20.23.123) mac=(00:1d:09:cc:a2)
o 1 DEBUG WinAgent.WinAgentEventHandler - Encoded message = 187:("content":("displayMame":"Local Area Connection","ifName":"Local Area Connection","ifType":
o Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Successfully disabled(BOUNCE) the Network interface Local Area Connection
o Evt 04DF7530] INFO Winkgent.WinkgentNetworkControl - Enabling the Network interface Local Area Connection
Evt 04DF7530] INFO Winkgent.WinkgentNetworkControl - Successfully enabled(BOUNCE) the Network interface Local krea Connection
o Evt 04DF7530] DEBUG WinAgent.WinAGentReadEvHandler - Successfully processed the message=BounceInterfaceRequest
o Evt U4DF7530] DEBUG Winkgent.WinkgentEventHandler - Encoded message = 69:("content":("status":true),"1d":25,"name":"BounceInterFaceResponse")
o o] DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification
o o] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
o] INFO Winkgent.WinkgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interfaces=1
0 VARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; jp=(10.20.23.123)  mac=(00:1d:09:cc:a2:1
oj Debuo winagent.winagent.ventnangier - incodeg message = 105:("content":("displayName":"Local Area Connection","liName":"Local Area Connection", "iTiype":

# **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:

- 1. Showing Online/Offline status on 'OnGuard Activity' Page.
- 2. Broadcasting Messages from CPPM Server to all Online clients.
- 3. 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.

### **OnGuard Plugin Logs (Establish Control Channel – Success):**

2014-03-17 13:27:09,109 [Th 00000f10] INFO OnGuardPlugin.AuthSession - DoEnforcementActions: Enforcement actions for Local Area Connection: Bounce=0 timeout=-1 secs messages='You are Healthy! healthcheckquietperiod=-1 secs'
2014-03-17 13:27:09,112 [Th 00000f10] INFO_OnGuardPlugin.AuthSession - EstablishControlChannel: <b>Trying to establish control channel for Local Area</b> Connection to 10.17.4.234
2014-03-17 13:27:09,139 [Th 00000f10] DEBUG OnGuardPlugin.ConnectionConnector - Connect: <b>Trying to connect from 10.20.23.123 to 10.17.4.234 at</b> port - 6658
2014-03-17 13:27:13,648 [Th 00000f10] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Successfully connected to <unknown>. Server IP = 10.17.4.234, Port = 6658</unknown>
2014-03-17 13:27:13,650 [Th 00000f10] INFO_OnGuardPlugin.AuthSession - EstablishControlChannel: Control channel established for Local Area Connection
2014-03-17 13:27:13,652 [Th 00000f10] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from <b>AUTH_SERVER_DISCOVERY</b> (1) to AUTH_COMPLETE (3) after 14 seconds
2014-03-17 13:27:18,652 [Th 00000f10] INFO_OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= <b>AUTH_COMPLETE</b> (3) (Seconds in this state=5) for Local Area Connection
2014-03-17 13:27:18,653 [Th 00000f10] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 42:{"content":"","id":30,"name":" <b>KeepAlive</b> "}
2014-03-17 13:27:23,654 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= <b>AUTH_COMPLETE</b> (3) (Seconds in this state=10) for Local Area Connection
2014-03-17 13:27:28,659 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= <b>AUTH_COMPLETE</b> (3) (Seconds in this state=15) for Local Area Connection

🙀 ClearPassOnGuard_0.log (107.7 KB) - BareTail	
Elle Edit View Preferences Help	
😂 Opeg 🥔 Highlighting 🔲 Follow Tail 🛛 ANSI 📃 🔽 C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearF	assOnGuard_0.log (107.7 KB)
winagent_0.log  ClearPassOnGuard_0.log	
02014-03-17 13:27:09,109 [Th 00000f10] INFO OnGuardPlugin.AuthSession - DoEnforcementAction	s: Enforcement actions for Local Area Connection: Bounce=O time
○2014-03-17 13:27:09,112 [Th 00000f10] INFO OnGuardPlugin.AuthSession - EstablishControlCha	nnel: Trying to establish control channel for Local krea Connec
•	
0 2014-03-17 13:27:09,139 [Th 00000f10] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Tr	ying to connect from 10.20.23.123 to 10.17.4.234 at port - 6658
02014-03-17 13:27:13,648 [In 0000010] DEB0G OnGuardPlugin.connectionconnector - connect: Su	ccessfully connected to <unknown>. Server IP = 10.17.4.234, Por</unknown>
2014-03-17 13:27:13.650 [Th 00000f10] INFO. OnGuardPlugin.AuthSession - EstablishControlCha	nnel: Control channel established for Local Area Connection
· · ·	
02014-03-17 13:27:13,652 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - SetState: Movi	ng from AUTH SERVER DISCOVERY (1) to AUTH COMPLETE (3) after 14
•	
2014-03-17 13:27:18,652 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: No	Op handling in state=AUTH_COMPLETE (3) (Seconds in this state=5
02014-03-17 13:27:18,653 [Th 00000f10] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMe	ssage:Encoded message = 42:{"content":"","id":30,"name":"KeepAl
o 2014 02 17 10 27 10 CD (Th 00000510) DEDUC Or Crand Direct Provent Direct Prove the Conduction of Conduction	Deve
02014-03-17 13:27:10,633 [In 00000110] DEBUG OnGuardPlugIn.messagewequestDispatcher - Senume	ssage: Done sending the data. Size - 40 Result - 40
02014-03-17 13:27:23.654 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOn: No	On handling in state=AUTH COMPLETE (3) (Seconds in this state=1
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
02014-03-17 13:27:28,659 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: No	Op handling in state=AUTH COMPLETE (3) (Seconds in this state=1-
•	
2014-03-17 13:27:33,660 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: No	Op handling in state=AUTH_COMPLETE (3) (Seconds in this state=2
	×

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.

### **OnGuard Plugin Logs (Establish Control Channel – Fail):**

2014-03-17 13:38:50,517 [Th 00000ebc] INFO OnGuardPlugin.AuthSession - EstablishControlChannel: Trying to establish control channel for Local Area Connection to 10.17.4.234
2014-03-17 13:38:50,592 [Th 00000ebc] DEBUG OnGuardPlugin.ConnectionConnector - Connect: <b>Trying to connect from 10.20.23.123 to 10.17.4.234 at</b> port - 6658
2014-03-17 13:38:50,592 [Th 00000ebc] ERROR OnGuardPlugin.ConnectionConnector - Connect: Failed to connect to Remote Server. Error - 10049 (The requested address is not valid in its context.)
2014-03-17 13:38:50,592 [Th 00000ebc] ERROR OnGuardPlugin.AuthSession - EstablishControlChannel: Establishing control channel failed for Local Area Connection
2014-03-17 13:38:50,593 [Th 00000ebc] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from <b>AUTH_SERVER_DISCOVERY</b> (1) to AUTH_COMPLETE (3) after 17 seconds
ClearPassOnGuard_O.log (225.4 K8) - BareTail
Eie gant verw Preterences peip 20 Open 2/ Highlighting Follow Tail ANSI C:Users/Deepak/AppData/Roaming/Aruba Networks/ClearPassOnGuard/ClearPassOnGuard_O.log (225.4 KB)
winagent_0.log  ClearPassOnGuard_0.log  ClearPassOnGuard_0.log  X INFO OnGuardPlugin.AuthSession - EstablishControlChannel: Trying to establish control channel for Local Area Connection to 10.17.4.234
o DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect from 10.20.23.123 to 10.17.4.234 at port - 6658
o ERROR OnGuardPlugin.ConnectionConnector - Connect: Failed to connect to Remote Server. Error - 10049 (The requested address is not valid in its context.)

After Establishing Control Channel, the Network Interface is moved from AUTH\_SERVER\_DISCOVERY to AUTH\_COMPLETE state.

Channel: Establishing control

INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH SERVER DISCOVERY (1) to AUTH COMPLETE (3) after 17 seconds INFO OnGuardPlugin.AgentController - SetGachedCredentials: Setting cache user credentials dj for interface=bocal krea Connection

DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Local Area Connection

Aruba Networks

# **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.

For Soft Re-Auth, the **OnGuard Agent** sends only Health Info (SoH) in a WebAuth Request to the CPPM server. The CPPM Server evaluates the health and responds with a SoHR. The **OnGuard Agent** processes the SoHR and compares the health status with previous cached health status. If there is change in the health status i.e. before client was healthy, now it is unhealthy or vice-versa, then **OnGuard Agent** sends a Full WebAuth (Credentials and Health Info) to the CPPM Server.

Differences between Soft Re-Auth and Full WebAuth:

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

### **OnGuard Plugin Logs (Soft Re-Auth):**



2014-03-17 14:00:18,098 [Th 00000fac] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:{"content":{"status":true},"id":40,"name":" <b>CollectHealthDataResponse</b> "}
2014-03-17 14:00:18,131 [Th 000008ac] DEBUG OnGuardPlugin.BackendClientInfoCollector - CollectHealthData: Collect Health Data Response Status =1
2014-03-17 14:00:18,131 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 30:{"id":42,"name":" <b>SoHRequest</b> "}
2014-03-17 14:00:18,133 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>SoHRequest</b> Timeout value (ms) - 180000
2014-03-17 14:00:18,163 [Th 00000fac] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 2544:{"content":{"soh":[0,7,3,67,0,0,1,55,0,2,3,59,,7,0,8,0,1,55,-128,0,4,2,0]},"id":42,"name":" <b>SoHResponse</b> "}
Ⅰ
2014-03-17 14:00:18,174 [Th 000008ac] DEBUG OnGuardPlugin.InterfaceSessionHelper - CollectHealthData: SoH: 0x0007034300000137001378000000700080001378000040200
2014-03-17 14:00:18,174 [Th 000008ac] DEBUG OnGuardPlugin.AuthSession - DoSoftReAuth: Local Area Connection: Messages returned by CollectHealth -
1
2014-03-17 14:00:18,175 [Th 000008ac] INFO OnGuardPlugin.WsHttpClient - Posting request to URL=/v2/PostureReeval/OnGuard
2014-03-17 14:00:18,175 [Th 000008ac] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/networkservices/webauthservice/v2/PostureReeval/OnGuard
2014-03-17 14:00:18,290 [Th 000008ac] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
2014-03-17 14:00:18,292 [Th 000008ac] DEBUG OnGuardPlugin.InterfaceSessionHelper - <b>ProcessSohr</b> : Language: en SoHR: 0x000701a800000137000201a00007c6338f881c3cbbed6aba13ed02efafa37f21867fc
2014-03-17 14:00:18,293 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 1493:{"content":{"language":"en","remediate":false,"sohr":[0,7,1,-88,0,0,1,55,0,2,1,-96,0,7,053,-66,-42,-85,-95,62,-48,46,-6,-6,55,-14,24,103,- 4]},"id":44,"name":" <b>ProcessSoHRRequest</b> "}
2014-03-17 14:00:18,293 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>ProcessSoHRRequest</b> Timeout value (ms) - 300000
2014-03-17 14:00:19,857 [Th 00000fac] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 419:{"content":{" <b>healthStatus":false</b> ,"messages":[null,[10,0,70,0,105,0,114,0,101,0,119,0,97,0,108,0,108,0,32,0,67,0,104,0,101,0,99,0,107,0,58,0,13,0],[69,0,1 10,0,97,0,98,0,108,0,101,0,32,0,77,0,105,0,99,0,114,0,111,0,115,0,111,0,102,0,116,0,32,0,87,0,105,0,110,0,100,0,111,0,119,0,115,0,32,0,70,0,105,0,114,0,101, 0,119,0,97,0,108,0,108,0,46,0,13,0]],"remediationURL":"","status":true},"id":44,"name":" <b>ProcessSoHRResponse</b> "}
2014-03-17 14:00:19,860 [Th 000008ac] DEBUG OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: Healthy - 0 Success - 1
1
2014-03-17 14:00:19,861 [Th 000008ac] DEBUG OnGuardPlugin.AuthSession - IsHealthStateChanged: Health state from soft re-auth for Local Area Connection = 3
2014-03-17 14:00:19,861 [Th 000008ac] INFO_OnGuardPlugin.AuthSession - IsHealthStateChanged: Status of health evaluation has changed for Local Area Connection. Old state=1 New state=3
•
2014-03-17 14:00:25,897 [Th 000008ac] INFO_OnGuardPlugin.InterfaceManager - SetState: <b>Moving from AUTH_COMPLETE (3) to</b> AUTH_SERVER_DISCOVERY (1) after 72 seconds



After detecting a change in the Health State of a client, the state of the Network Interface is changed from AUTH\_COMPLETE to AUTH\_SERVER\_DISCOVERY, to restart a new session.

**Backend Service** collects system health every 30 seconds to check if a health state has changed or not. But it does not collect health of each health class every 30 seconds as this will put too much load on the endpoint CPU.

**Backend Service** caches the health of each health class for a predefined time (non-configurable). When the cached health of a health class expires, it collects the health again.

Refer section Health Collection Interval for Each Health Class for details.

# **Automatic Remediation**

**OnGuard Agent** can do automatic remediation of unhealthy health classes to make a client compliant, if auto-remediation is enabled.

On Windows, automatic remediation for some of the health checks are done by the **Backend Service** itself and for some health checks, it uses **Universal Sytem Health Agent** (USHA) **Remediate** Application (ClearPassUSHARemediate.exe on Windows Only).

On Mac OS X, automatic remediation of all the health checks is done by **Backend Service** but have separate log file for remediation (macagent\_remediate\_\*.log).

Refer to the section <u>Health Checks and Auto-Remediation</u> for lists of Health Checks and module responsible for performing auto-remediation for respective health checks.

If auto-remediation is not enabled or not supported then the **OnGuard Agent** displays a message to the user indicating what health checks failed and instructions to remediate manually.



### **Backend Service Logs (Auto-Remediation):**

2014-03-17 16:16:07,321 [Th 0000019C] INFO\_WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not\_Healthy. Global Remediate Flag - 1

2014-03-17 16:16:07,322 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Application Microsoft Windows Firewall is Unhealthy.

2014-03-17 16:16:07,359 [Th 0000019C] INFO\_WinSHA.FWHealthClassInfoFactory - GetEnableRemediationAttrValue: Value of EnableRemediation attribute of Application Microsoft Windows Firewall is 1

2014-03-17 16:16:07,360 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - GetEnableNotificationAttrValue: Value of EnableNotification attribute of Application Microsoft Windows Firewall is 1

2014-03-17 16:16:07,360 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Product Id: 6015 Product Version: 7

2014-03-17 16:16:08,970 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Firewall application Microsoft Windows Firewall enabled



### USHA Remediate Logs (Auto-Remediation):

2014-03-17 16:16:05,239 [MainTh 2020:1920] INFO WinSHARemediate - \_tWinMain: ClearPassUSHARemediate 6.3.1.61950

2014-03-17 16:16:05,239 [MainTh 2020:1920] INFO WinSHARemediate - \_tWinMain: Initializing OESIS SDK

2014-03-17 16:16:07,281 [MainTh 2020:1920] INFO WinSHARemediate - tWinMain: OESIS SDK Version: "3.6.8769.2"

2014-03-17 16:16:12,071 [MainTh 2020:1920] DEBUG WinSHARemediate - SetRTPStatus: Name: Microsoft Security Essentials, ID: 6020, Version: 4.2.0223.0

2014-03-17 16:16:17,576 [MainTh 2020:1920] INFO WinSHARemediate - SetRTPStatus: Enabled real time protection status of Microsoft Security Essentials application

2014-03-17 16:16:17,696 [MainTh 2020:1920] INFO WinSHARemediate - \_tWinMain: Uninitializing OESIS SDK

🕈 winagent remediate 0.log (3.0.KB) - BareTail	
File Edit View Preferences Help	
😰 Opeg 🌽 Highlighting 🔽 Follog Tail ANSI 🤍 C::VPogramData/Aruba Networks/ClearPassOnGuard/winagent_remediate_0.log (3.0 KB)	
whagent_0.log 🗢 ClearPassOnGuard_0.log 🗢 winagent_remediate_0.log 🗢	_
O [MainTh 2020:1920] INFO WinSHARemediatetWinMain: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassUSHARemediate.exe -Embedding     O [MainTh 2020:1920] INFO WinSHARemediatetWinMain: ClearPassUSHARemediate 6.3.1.61950     O [MainTh 2020:1920] INFO WinSHARemediatetWinMain: Initializing OESIS SDK     O [MainTh 2020:1920] INFO WinSHARemediatetWinMain: SDK Version: "3.6.8769.2"	
o [MainTh 2020:1920] DEBUG WinSHARemediate - SetRTPStatus: Name: Microsoft Security Essentials, ID: 6020, Version: 4.2.0223.0 o [MainTh 2020:1920] INFO WinSHARemediate - SetRTPStatus: Enabled real time protection status of Microsoft Security Essentials application o [MainTh 2020:1920] INFO WinSHARemediatetWinMain: Uninitializing OESIS SDK o	
	• •

# Retry

When a user clicks on the Retry button, the **OnGuard Agent** closes the current session and moves the Network Interface from AUTH\_COMPLETE to a RECONNECT\_USER state.

If the OnGuard is running in Health-Only mode then it will start a new session immediately i.e. it will start collecting health.

# **OnGuard Plugin Logs (Retry in Health-Only Mode):**

2014-03-21 11:48:57,147 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= <b>AUTH_COMPLETE</b> (3) (Seconds in this state=20) for Local Area Connection
I construction of the second
2014-03-21 11:49:00,786 [Th 3660:3016] INFO_OnGuardPlugin.NetworkInterfaceActionListener - Reconnect: Reconnect requested for Local Area Connection
2014-03-21 11:49:00,795 [Th 000003e8] DEBUG OnGuardPlugin.AgentController - HandleAction: Handling action= <b>RECONNECT</b> (9) after a delay of 0.9 seconds
2014-03-21 11:49:00,795 [Th 000003e8] INFO_OnGuardPlugin.InterfaceManager - HandleReconnect: Got Reconnect in state=AUTH_COMPLETE (3) for Local Area Connection
2014-03-21 11:49:00,795 [Th 000003e8] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to RECONNECT_USER (5) after 23 seconds
I contraction of the second
2014-03-21 11:49:06,826 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Local Area Connection
I contraction of the second
2014-03-21 11:49:06,875 [Th 000003e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
I second s
2014-03-21 11:49:06,876 [Th 000003e8] INFO_OnGuardPlugin.InterfaceManager - HandleReconnect: Automatically starting Health check Local Area Connection
I construction of the second se
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:{"id":42,"name":" <b>CollectHealthDataRequest</b> "}
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000
I contraction of the second
2014-03-21 11:49:06,929 [Th 0000138c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:{"content":{"status":true}."id":42."name":" <b>CollectHealthDataResponse</b> "}

ClearPassOnGuard 0.Jon (187.0 KB) - RareTail	
File Edit View Preferences Help	
Open 2 Highlighting Follow Tail ANSI     CLUsers/Deepak/AppData/Roaming/Aruba Networks/ClearPass/DnGuard/ClearPass/	
	×
02014-03-21 11:48:57,147 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state	<u>&gt;</u>
2014-03-21 11:49:00.786 [Th 3660:3016] INFO OnGuardPlugin.NetworkInterfaceActionListener - Reconnect: Reconnect requested for Local Area Connection	
2014-03-21 11:49:00,795 [Th 000003e8] DEBUG OnGuardPlugin.AgentController - HandleAction: Handling action=RECONNECT (9) after a delay of 0.9 seconds	
2014-03-21 11:49:00,795 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - HandleReconnect: Got Reconnect in state=AUTH COMPLETE (3) for Local Area C	on
o 2014-03-21 11:49:00,795 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH COMPLETE (3) to RECONNECT USER (5) after 23 sec	on
2014-03-21 11:49:06,826 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Loca	al
2014-03-21 11:49:06,875 [Th 000003e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234	
o 2014-03-21 11:49:06,876 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - HandleReconnect: Automatically starting Health check Local Area Connection	
02014-03-21 11:49:06,876 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - GetNetworkInterfaceList: Network interfaces list size for Local Area Connec	st
o 2014-03-21 11:49:06,876 [Th 000003e8] DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: IsHealthCheckQuietPeriodEnabled() returned false for 1	Lo
02014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: Possible cause - InterfaceType==VPN   Mode!=HealthOnis	y
o 2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.AuthSession - Authenticate: Not In HealthCheckQuietPeriod. Performing full Auth with health ch	ne
02014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:("id":42,"name":"CollectHealthDate	aR
0 2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataResponse: Wait for response for request=CollectHealthDataResponse.	qu
•	
2014-03-21 11:49:06,929 [Th 0000138c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:("content":("status":true),"id":42,"name":"CollectHealthData	aR
	-
	٠Ċ
	<u> </u>

After the health checks are complete, the Network Interface is moved from RECONNECT\_USER to AUTH\_COMPLETE state.

### **OnGuard Plugin Logs (Moved from RECONNECT\_USER to AUTH\_COMPLETE state):**

2014-03-21 11:49:13,488 [Th 000003e8] DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for I Connection	Local Area
2014-03-21 11:49:13,488 [Th 000003e8] INFO_OnGuardPlugin.InterfaceManager - <b>SetState: Moving from RECONNECT_USER (5) to AUTH</b> after 12 seconds	I_COMPLETE (3)
🕻 ClearPassOnGuard_Olog (187.0 KB) - BareTail	
Elle Edit View Breferences Help	
😂 Open 🤌 Highlighting 🔽 Folow Tail ANSI 🗾 C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPasSOnGuard\ClearPasSOnGuard\ClearPasSOnGuard\ClearPasSOnGuard\ClearPasSOnGuard\ClearPasSOnGuard\ClearPasSOnGuar	
winagent_0.log 🔽 ClearPassOnGuard_0.log 🔽	
2014-03-21 11:49:13,488 [Th 000003:8] DEBUG OnGuardPlugin.InterfaceManager - Dokuth: kuth success. Updating cached credentials for Local krea Connection	
o poly-US-21 11:49:13,466 [In UUUUUSEG] INFO UNGUARGPLUGIN.INCEFTACEMANAGEF - SETSTATE: Roving from RECONNECT USER (5) to AUTH COMPLETE (3) after 12 Been 0 0	

If OnGuard is running in Auth or Auth+Health mode then OnGuard will wait for user to click on Login button to start new session. When user clicks on Login button and enters credentials, Network Interface is moved from RECONNECT\_USER to AUTH\_SERVER\_DISCOVERY state.
# OnGuard Plugin Logs (Retry in Auth+Health Mode):

2014-03-21 12:10:35,266 [Th 00000218] INFO_OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=370) for Local Area Connection
2014-03-21 12:10:36,722 [Th 4932:4908] INFO_OnGuardPlugin.NetworkInterfaceActionListener - Reconnect: Reconnect requested for Local Area Connection
I construction of the second
2014-03-21 12:10:36,731 [Th 00000218] INFO_OnGuardPlugin.InterfaceManager - HandleReconnect: Got Reconnect in state=AUTH_COMPLETE (3) for Local Area Connection
2014-03-21 12:10:36,731 [Th 00000218] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to RECONNECT_USER (5) after 371 seconds
2014-03-21 12:10:42,761 [Th 00000218] INFO_OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Local Area Connection
l de la construcción de la constru
2014-03-21 12:10:42,806 [Th 00000218] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
2014-03-21 12:10:47,809 [Th 00000218] INFO_OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=RECONNECT_USER (5) (Seconds in this state=11) for Local Area Connection
2014-03-21 12:11:17,689 [Th 4932:4908] INFO_OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Connection Username=dj
2014-03-21 12:11:17,697 [Th 00000218] DEBUG OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Local Area Connection
2014-03-21 12:11:17,700 [Th 00000218] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from RECONNECT_USER (5) to AUTH_SERVER_DISCOVERY (1) after 40 seconds
2014-03-21 12:11:17,748 [Th 00000218] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
2014-03-21 12:11:17,749 [Th 00000218] INFO_OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area
2014-03-21 12:11:17,750 [Th 00000218] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded messag <mark>e =</mark> 45:{"id":164,"name":" <b>CollectHealthDataRequest</b> "}
2014-03-21 12:11:17,750 [Th 00000218] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000
2014-03-21 12:11:17,792 [Th 00001250] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 72:{"content":{"status":true} "id":164 "name":"CollectHealthDataResponse"}

After health checks are complete, the Network Interface is moved from AUTH\_SERVER\_DISCOVERY to AUTH\_COMPLETE state.

### **OnGuard Plugin Logs (Moved from AUTH\_SERVER\_DISCOVERY to AUTH\_COMPLETE state):**

2014-03-21 12:11:24,448 [Th 00000218] DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Local Area Connection

2014-03-21 12:11:24,449 [Th 00000218] INFO\_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH\_SERVER\_DISCOVERY (1) to AUTH\_COMPLETE (3) after 6 seconds

2014-03-21 12:11:24,449 [Th 00000218] INFO OnGuardPlugin.AgentController - SetCachedCredentials: Setting cache user credentials dj for interface=Local Area Connection



## Logout

When a user clicks on the Logut button, **OnGuard Agent** closes its current session, moves the Network Interface from AUTH\_COMPLETE to LOGGED\_OUT state and Bounces the Network Interface.

If OnGuard is running in Health-Only mode then it will wait for the user to click on the Start button to start a new session. When the user clicks on the Login button and enters there credentials, the Network Interface is moved from a LOGGED\_OUT to AUTH\_SERVER\_DISCOVERY state.

## **OnGuard Plugin Logs (Logout in Health-Only Mode):**

2014-03-21 15:11:09,757 [Th 00000140] INFO_OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= <b>AUTH_COMPLETE</b> (3) (Seconds in this state=225) for Local Area Connection
2014-03-21 15:11:10,572 [Th 5236:3988] INFO OnGuardPlugin.NetworkInterfaceActionListener - Logout: Logout requested Local Area Connection
I and the second se
2014-03-21 15:11:10,577 [Th 00000140] INFO_OnGuardPlugin.InterfaceManager - HandleLogout: Got Logout in state=AUTH_COMPLETE (3) for Local Area Connection
2014-03-21 15:11:10,577 [Th 00000140] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to LOGGED_OUT (4) after 225 seconds
2014-03-21 15:11:16,592 [Th 00000140] DEBUG OnGuardPlugin.InterfaceManager - <b>DoLogout: Logout not supported or did not work. Trying bounce</b> Local Area Connection
2014-03-21 15:11:16,593 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 87:{"content":{"ifName":"Local Area Connection"},"id":42,"name":" <b>BounceInterfaceRequest</b> "}
2014-03-21 15:11:16,593 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>BounceInterfaceRequest</b> Timeout value (ms) - 180000
2014-03-21 15:11:17,050 [Th 00000d2c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName": <b>"Local Area</b> Connection","ifName":"Local Area Connection","ifType":"WIRED", "ipAddress":"10.20.23.123", "macAddress":"001d09cca2bc"},"id":9,"name":"InterfaceDown"}
2014-03-21 15:11:17,052 [Th 00000d2c] DEBUG OnGuardPlugin.AgentController - InterfaceDown: InterfaceDown message received from backend server for Local Area Connection
2014-03-21 15:11:21,183 [Th 00000d2c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 69:{"content":{"status":true},"id":42,"name":" <b>BounceInterfaceResponse</b> "}
2014-03-21 15:11:21,248 [Th 00000d2c] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message = {"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":11,"name":"InterfaceUp"}
I contraction of the second
2014-03-21 15:11:21,251 [Th 00000d2c] DEBUG OnGuardPlugin.AgentController - InterfaceUp: InterfaceUp message received from backend server for Local Area Connection
4
2014-03-21 15:11:21,328 [Th 00000140] DEBUG OnGuardPlugin.AgentController - HandleIfUp: New Interface Up = IfName=Local Area Connection IfType=WIRED DisplayName=Local Area Connection MAC=001d09cca2bc IP=10.20.23.123
2014-03-21 15:11:21,328 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - HandleIfUp: Got IfUp in state=LOGGED_OUT (4)

2014-03-21 15:11:21,329 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - HandleifUp: Notify interface up. Waiting for user action Local Area Connection.
2014-03-21 15:12:20,910 [Th 5236:3988] INFO_OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Connection Username=
1
2014-03-21 15:12:20,918 [Th 00000140] DEBUG OnGuardPlugin.AgentController - HandleUserCredentials: <b>Handling User Credentials for Local Area</b> Connection
2014-03-21 15:12:20,919 [Th 00000140] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from LOGGED_OUT (4) to AUTH_SERVER_DISCOVERY (1) after 70 seconds
1
2014-03-21 15:12:20,957 [Th 00000140] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
2014-03-21 15:12:20,961 [Th 00000140] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_SERVER_DISCOVERY (1) to WAIT_FOR_CREDENTIALS (2) after 0 seconds
2014-03-21 15:12:20,961 [Th 00000140] INFO_OnGuardPlugin.InterfaceManager - <b>DoWaitForAuthCredentials: Only health checks required for Local</b> Area Connection
I
2014-03-21 15:12:20,963 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 45:{"id":104,"name":" <b>CollectHealthDataRequest</b> "}
2014-03-21 15:12:20,964 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>CollectHealthDataRequest</b> Timeout value (ms) - 1200000
1

2014-03-21 15:12:23,153 [Th 00000d2c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 72:{"content":{"status":true},"id":104,"name":"**CollectHealthDataResponse**"}

関 ClearPa	assOnl	Guard	_0.log (207.9 )	(B) - Bar	ztail	
<u>File E</u> dit	View	Prefe	rences <u>H</u> elp			
൙ Open	🌽 Hi	ighlighti	ng 🔲 Follo <u>w</u> T	ail ANSI	C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassDnGuard\ClearPassDnGuard_0.log (207.9 KB)	
winagent	0 log			, ard 0.loc		×
11:09	757	LTP.	000001401	TNEO	DurdiardBlugin InterfaceManagar - HandleNcOn: NoOn bandling in state=MITH COMPLETE (3) (Seconds in this state=225) for Local	
0 11:10	.572	[Th	5236:39881	I INFO	OndurardPlugin. MetworkInterfaceActionListener - Logout: Logout. Logout. Logout. Logout. Logout. Logout. Logout.	
0	,			,		
11:10,	,577	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - HandleLogout: Got Logout in state=AUTH_COMPLETE (3) for Local Area Connection	
11:10,	,577	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to LOGGED_OUT (4) after 225 seconds	
11:16	.592	[ Th	000001401	DEBUG	OnGuardPlugin.InterfaceManager - DoLogout: Logout not supported or did not work. Trying bounce Logal Area Connection	
0 11:16	, 593	[Th	00000140]	DEBUG	OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 87:("content":("iName":"Local Area Connection"),"id	<b>"</b> :
◊ 11:16,	,593	[Th	00000140]	DEBUG	OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=BounceInterfaceRequest Timeout valu	e
11:17,     1	,050	[Th	00000d2c]	DEBUG	OnGuardPlugin.ConnectionReader - Read Data = 187:("content":("displayName":"Local Area Connection","ifName":"Local Area Con	ne
	,052	[Th	00000d2c]	DEBUG	OnGuardPlugin.AgentController - InterfaceDown: InterfaceDown message received from backend server for Local Area Connection	_
0 11.21	,105	[ ] ]	000000203	DEDUG	onduartrugin.connectionneauer - neau pata - 05.; content :; status :tue;; iu :tr; name : bouncerneertacenesponse ;	-
11:21,	,248	[Th	00000d2c]	DEBUG	JsonWrapper.Netstrings - Extracted Netstrings message = ("content":("displayName":"Local &rea Connection","ifName":"Local &	re
•						_
° 11:21,	,251	[Th	00000d2cj	DEBUG	OnGuardPlugin.AgentController - InterfaceUp: InterfaceUp message received from backend server for Local Area Connection	_
0 11:21	.328	ſTh	000001401	DEBUG	OnGuardPlugin,AgentController - HandleIfUp: New Interface Up = IfName=Local Area Connection IfType=WIRED DisplayName=Local	Ar
0 11:21	,328	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - HandleIfUp: Got IfUp in state=LOGGED_OUT (4)	
•						
0 11:21,	,329	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - HandleIfUp: Notify interface up. Waiting for user action Local Area Connection	
12:20.	.910	ſTh	5236:39881	I INFO	OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Connection Usernam	e=
0	,			,		
	,918	[Th	00000140]	DEBUG	OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Local Area Connection	
	,919	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - SetState: Moving from LOGGED_OUT (4) to AUTH_SERVER_DISCOVERY (1) after 70 seconds	- 1
0 12:20.	,957	ſTh	000001401	DEBUG	OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234	
0 12:20	,961	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection	
♦ 12:20,	,961	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_SERVER_DISCOVERY (1) to WAIT_FOR_CREDENTIALS (2) after 0 second	8
0 12:20,	,961	[Th	00000140]	INFO	OnGuardPlugin.InterfaceManager - DoWaitForAuthCredentials: Only health checks required for Local Area Connection	
• 12:20	.963	[Th	000001401	DEBUG	OnGuardPlugin MessagePermestDisnatcher - SendMessage:Encoded message = 45.("id":104."name":"CollectHealthDataPermest")	-
◊ 12:20	,964	[Th	00000140]	DEBUG	OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout va	10
• <u>12:23</u>	,153	[Th	00000d2c]	DEBUG	OnGuardPlugin.ConnectionReader - Read Data = 72:("content":("status":true),"id":104,"name":"CollectHealthDataResponse")	
•						
•						_
						1 1

After health checks are done, the Network Interface is moved to an AUTH\_COMPLETE state.

### **OnGuard Plugin Logs (Moved to AUTH\_COMPLETE state after Health Checks):**



If OnGuard is running in an Auth+Health mode then OnGuard will wait for a user to click on the Login button to start a new session. When a user clicks on the Login button and enters there credentials, the Network Interface is moved from a LOGGED\_OUT to AUTH\_SERVER\_DISCOVERY state.

# OnGuard Plugin Logs (Logout in Auth+Health Mode):

2014-03-21 13:47:47,016 [Th 00001504] INFO_OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= <b>AUTH_COMPLETE</b> (3) (Seconds in this state=25) for Local Area Connection
2014-03-21 13:47:48,215 [Th 5556:5108] INFO OnGuardPlugin.NetworkInterfaceActionListener - Logout: Logout requested Local Area Connection
I construction of the second se
2014-03-21 13:47:48,217 [Th 00001504] INFO_OnGuardPlugin.InterfaceManager - HandleLogout: Got Logout in state=AUTH_COMPLETE (3) for Local Area Connection
2014-03-21 13:47:48,217 [Th 00001504] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to LOGGED_OUT (4) after 26 seconds
2014-03-21 13:47:54,234 [Th 00001504] DEBUG OnGuardPlugin.InterfaceManager - DoLogout: Logout not supported or did not work. Trying bounce Local Area Connection
2014-03-21 13:47:54,234 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 87:{"content":{"ifName":"Local Area Connection"},"id":32,"name":" <b>BounceInterfaceRequest</b> "}
2014-03-21 13:47:54,235 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request= <b>BounceInterfaceRequest</b> Timeout value (ms) - 180000
2014-03-21 13:47:55,546 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName <b>": "Local Area</b> <b>Connection"</b> ,"ifName":"Local Area Connection", "ifType":"WIRED","ipAddress":"10.20.23.123" ,"macAddress":"001d09cca2bc"},"id":5,"name":" <b>InterfaceDown</b> "}
2014-03-21 13:47:55,552 [Th 000016b8] DEBUG OnGuardPlugin.AgentController - InterfaceDown: InterfaceDown message received from backend server for Local Area Connection
2014-03-21 13:48:07,365 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 69:{"content":{"status":true},"id":32,"name":" <b>BounceInterfaceResponse</b> "}
2014-03-21 13:48:07,450 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Local Area Connection
2014-03-21 13:48:07,642 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 185:{"content":{"displayName": <b>"Local Area</b> Connection","ifName":"Local Area Connection","ifType":"WIRED", "ipAddress":"10.20.23.123", "macAddress":"001d09cca2bc"},"id":9,"name":"InterfaceUp"}
2014-03-21 13:48:07,683 [Th 000016b8] DEBUG OnGuardPlugin.AgentController - InterfaceUp: InterfaceUp message received from backend server for Local Area Connection
2014-03-21 13:48:07,710 [Th 00001504] DEBUG OnGuardPlugin.AgentController - HandleIfUp: <b>New Interface Up = IfName=Local Area Connection</b> IfType=WIRED DisplayName=Local Area Connection MAC=001d09cca2bc IP=10.20.23.123
2014-03-21 13:48:07.710 [Th 00001504] INFO_OnGuardPlugin.InterfaceManager - HandlelfUp: Got IfUp in state=LOGGED_OUT (4)

Aruba Networks

2014-03-21 13:48:07,711 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - HandlelfUp: Notify interface up. Waiting for user action	n Local Area
2014-03-21 13:48:07,711 [Th 00001504] INFO_OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in Local Area Connection	n logged out state
1	
2014-03-21 13:48:07,891 [Th 00001504] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth serv	<mark>er=10.17.4.234</mark>
2014-03-21 13:48:17,959 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=LOGGED_OUT (4)	(Seconds in this
state=29) for Local Area Connection	
* 2014-03-21 13:48:57,591 [Th 55 <mark>56:5108] INFO OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info availa</mark>	ble for Local
Area Connection Username=dj	
- 2014-03-21 13:48:57,598 [Th 00001504] DEBUG OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Connection	<mark>or Local Area</mark>
2014-03-21 13:48:57,599 [Th 00001504] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from LOGGED_OUT (4) to AUTH_SERVER_DISCOVERY (1) after 69 seconds	
2014-03-21 13:48:57,648 [Th 00001504] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth serv	<mark>er=10.17.4.234</mark>
2014 02 21 12:49:57 651 FTb 000015041 DEPLIC On Guard Divin Massage Dequest Dispetshor Sand Massage Encoded message -	
4:{"id":84,"name":"CollectHealthDataRequest"}	
2014 02 24 12 40 57 604 [Th 000016b0] DEBUG On Guard Dhuain Connection Product Product Product	
71:{"content":{"status":true},"id":84,"name":" <b>CollectHealthDataResponse</b> "}	

🛃 Clear	PassOnG	iuard_0.log (151.)	9 KB) - I	BareTail			_ 8 ×
<u>Eile E</u> dit	t <u>V</u> iew	Preferences Help					
൙ Open	y 🌽 Hig	hlighting 🔲 Follow	yTail 🗛	NSI	- C	2: Wisers/Deepak/AppData/Roaming/Aruba Networks/ClearPassOnGuard/ClearPassOnGuard_O.log (151.9 KB)	
winagen	t_0.log 🏾	ClearPassOn	Guard_0	.log 🔻			< > ×
∘ ∘2014 ∘2014	-03-21 -03-21	13:47:47,01 13:47:48,21	.6 [Th .5 [Th	00001504] 5556:5108	INFO ] INFO	OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state O OnGuardPlugin.NetworkInterfaceActionListener - Logout: Logout requested Local Area Connection	±=25)
<ul> <li>○ .</li> <li>○ 2014</li> <li>○ 2014</li> <li>○ .</li> </ul>	-03-21 <mark>-03-21</mark>	13:47:48,21 13:47:48,21	.7 [Th .7 [Th	00001504] 00001504]	INFO INFO	OnGuardPlugin.InterfaceManager - HandleLogout: Got Logout in state=AUTH_COMPLETE (3) for Local Area Connecti OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to LOGGED_OUT (4) after 26 seconds	lon
<ul> <li>◇ 2014</li> <li>◇ 2014</li> <li>◇ 2014</li> <li>◇ 2014</li> </ul>	-03-21 -03-21 -03-21 -03-21	13:47:54,23 13:47:54,23 13:47:54,23 13:47:55,54	4 [Th 4 [Th 5 [Th 6 [Th	00001504] 00001504] 00001504] 000016b8]	DEBUG DEBUG DEBUG	<sup>1</sup> OnGuardPlugin.InterfaceManager - DoLogout: Logout not supported or did not work. Trying bounce Local Area Co <sup>1</sup> OnGuardPlugin.MessageRequestDispatcher - SendHessage:Encoded message = 07:("content":("iNmam":"Local Area C <sup>2</sup> OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=BounceInterfaceReque <sup>2</sup> OnGuardPlugin.ConnectionReader - Read Data = 167:("content":("displayName":"Local Area Connection","ifName"	onnec Conne Est T "Loc
<ul> <li>○ 2014</li> <li>○ 2014</li> <li>○ 2014</li> </ul>	-03-21 -03-21	13:47:55,55 13:48:07,36	2 [Th 5 [Th	000016b8]	DEBUG	; OnGuardPlugin.AgentController - InterfaceDown: InterfaceDown message received from backend server for Local 5 OnGuardPlugin.ConnectionReader - Read Data = 69:("content":("status":true),"id":32,"name":"BounceInterfaceRe	Ares Espor
∘. ∘2014 ∘	-03-21	13:48:07,45	0 [Th	00001504]	INFO	OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Loca	al Ar
	-03-21	13:48:07,64	2 [Th	000016b8]	DEBUG	j OnGuardPlugin.ConnectionReader - Read Data = 185:("content":("displayName":"Local &rea Connection","ifName":	"Loc
	-03-21	13:48:07,68	3 [Th	000016b8]	DEBUG	) OnGuardPlugin.AgentController - InterfaceUp: InterfaceUp message received from backend server for Local Area	a Cor
<ul> <li>○ 2014</li> <li>○ 2014</li> <li>○ 2014</li> <li>○ 2014</li> <li>○ 2014</li> </ul>	-03-21 -03-21 -03-21 -03-21	13:48:07,71 13:48:07,71 13:48:07,71 13:48:07,71	.0 [Th .0 [Th .1 [Th .1 [Th	00001504] 00001504] 00001504] 00001504]	DEBUG INFO INFO INFO	; OnGuardPlugin.AgentController - HandleIfUp: New Interface Up = IfName=Local Area Connection IfType=WIRED Dis OnGuardPlugin.InterfaceManager - HandleIfUp: Got IfUp in state=LOGGED_OUT (4) OnGuardPlugin.InterfaceManager - HandleIfUp: Notify interface up. Waiting for user action Local Area Connect OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auch server in logged out state Locs	splay sion
∘. ∘2014	-03-21	13:48:07,89	1 [Th	00001504]	DEBUG	3 OnGuardPlugin.InterfaceManager - PickkuthServer: Current domain=default kuth server=10.17.4.234	
。 。2014	-03-21	13:48:17,95	9 [Th	00001504]	INFO	OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=LOGGED_OUT (4) (Seconds in this state=29	9) fc
∘ 2014 ∘ .	-03-21	13:48:57,59	1 [Th	5556:5108	] INFO	) OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Con	inect
	<mark>-03-21</mark> <mark>-03-21</mark> -03-21	13:48:57,59 13:48:57,59 13:48:57,64	8 [Th 9 [Th 8 [Th	00001504] 00001504] 00001504]	DEBUG INFO DEBUG	: OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Local Area Connection OnGuardPlugin.InterfaceManager - SetState: Noving from LOGGED OUT (4) to AUTH SERVER DISCOVERY (1) after 69 3 OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234	secc
	-03-21	13:48:57,65	1 [Th	00001504]	DEBUG	00GuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:("id":84,"name":"CollectHealthData	aRequ
<ul> <li>≥ 2014</li> <li></li> </ul>	-03-21	13:48:57,69	4 [Th	000016b8]	DEBUG	5 OnGuardPlugin.ConnectionReader - Read Data = 71:("content":("status":true),"id":84,"name":"CollectHealthData	iResp _1
4							

After the health checks are done, the Network Interface is moved from an AUTH\_SERVER\_DISCOVERY to an AUTH\_COMPLETE state.

#### **OnGuard Plugin Logs (Moved from AUTH\_SERVER\_DISCOVERY to AUTH\_COMPLETE state):**

2014-03-21 13:49:03,963 [Th 00001504] DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Connection	• Local Area					
2014-03-21 13:49:03,964 [Th 00001504] INFO_OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_SERVER_DISCOVERY (1) to AUTH_COMPLETE (3) after 6 seconds						
2014-03-21 13:49:03,964 [Th 00001504] INFO OnGuardPlugin.AgentController - SetCachedCredentials: Setting cache user credentials dj for Area Connection	r interface=Local					
ClearPassOnGuard_0.00g (151.9 KB) - BareTail						
<pre>vingerLDBg v LearressonGuard_LDBg v Lear</pre>						

**OnGuard Agent** bounces Network Interface after a specific interval; if it remains in a LOGGED\_OUT state i.e. user does not click on Login button. This interval is either 5 minutes (default value) or the value of "Delay to bounce after Logout (in minutes)" in Global Agent Settings parameter, if configured.

Aruba Networks

# Backend Service Logs (Bounce Network Interface After Logout):

2014-03-21 15:56:34,687 [Th 000001F4] DEBUG WinAgent.WinAgentNetworkProcessor - TimerCompletionEv: Received TimerCompletionEv with id=0
2014-03-21 15:56:34,687 [Th 000001F4] INFO_WinAgent.WinAgentNetworkProcessor - CWinAgentNetworkProcessor::BounceInterface() IfName=Local Area Connection
I construction of the second
2014-03-21 15:56:34,779 [Th 000001F4] INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection
2014-03-21 15:56:34,826 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Run: Network Interface Change event signalled
2014-03-21 15:56:34,829 [Th 000001E8] INFO_WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. <b>Previous num</b> interfaces=1 Current num interfaces=0
2014-03-21 15:56:34,829 [Th 000001E8] WARN_WinAgent.WinAgentNetworkProcessor - The interface information has changed. Following interface information, ip={10.20.23.123} mac={00:1d:09:cc:a2:bc} can't be found
2014-03-21 15:56:35,336 [Th 000001F4] INFO_WinAgent.WinAgentNetworkControl - Successfully disabled(BOUNCE) the Network interface Local Area Connection
2014-03-21 15:56:37,338 [Th 000001F4] INFO WinAgent.WinAgentNetworkControl - Enabling the Network interface Local Area Connection
2014-03-21 15:56:39,611 [Th 000001F4] INFO_WinAgent.WinAgentNetworkControl - Successfully enabled(BOUNCE) the Network interface Local Area Connection
2014-03-21 15:56:39,821 [Th 000001E8] INFO_WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=1
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc}
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc} Cf winagent_0.log (16:MB)-BareTall
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc} © uningent_0.log (1.6 MB)-BareTail Detected yow Preferences Hep Detected yow Preferences Hep Detected new Networks/DeerPassOnGuardwinagent_0.log (1.6 MB)
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc}
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc}
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0[Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc}
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0[Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc}
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0]Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:cc:a2:bc}
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0[Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123}[mac={00:1d:09:cc:a2:bc}]
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0[Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgentWinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123}[mac={00:1d:09:cc:a2:bc}
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0]Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123} mac={00:1d:09:ccca2:bc}} <pre> ************************************</pre>
2014-03-21 15:56:39,821 [Th 000001E8] INFO WinAgent.WinAgent.WinAgent.WerkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interfaces=1 2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgent.WinAgent.WerkProcessor - The interface information has changed. Detected new network interface: ip={10.20.23.123}]mac={00:1d:09:cc:a2:bc}  2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.WinAgent.WinAgent.WerkProcessor - The interface information has changed. Detected new network interface: ip={10.20.23.123}]mac={00:1d:09:cc:a2:bc}  2014-03-21 15:56:39,821 [Th 000001E8] WARN WinAgent.VinAgent.VinAge

## Quit

When a user quits the **OnGuard Agent**, **OnGuard Agent** starts a timer to bounce the interface after a default 5 minutes or "Delay to bounce after Logout (in minutes)" value.

## **Backend Service Logs (Bounce Network Interface After Quit):**

2014-03-21 16:15:44,699 [Th 000013f4 Evt 050F9218] DEBUG WinAgent.WinAGentReadEvHandler - Read data =
oz. ( content . ( interfacebounceberay .), now haiser, no .20, name . bouncebranageu ;
2014-03-21 16:15:44,702 [Th 000013f4 Evt 050F9218] INFO_WinAgent.BounceManagedMessageHandler - BounceManaged::now=false, initiating the Bounce of Managed interfaces later.
2014-03-21 16:15:44,702 [Th 000013f4 Evt 050F9218] DEBUG WinAgent.BounceManagedMessageHandler - BounceManaged::interfaceBounceDelay - 3
2014-03-21 16:16:10,828 [Th 000013f4 Evt 050FA1D8] INFO_WinAgent.WinAGentReadEvHandler - <b>Bouncing the managed network interfaces for</b> ConnId=1
2014-03-21 16:16:10,828 [Th 000013f4 Evt 050FA1D8] DEBUG WinAgent.WinAgentNetworkProcessor - Processing the disconnect for connectionId=1
2014-03-21 16:16:10,828 [Th 000013f4 Evt 050FA1D8] DEBUG WinAgent.WinAgentDisconnectHandler - Starting timer id=0 for 180000 msecs
2014-03-21 16:16:10,829 [Th 000013f4 Evt 050FA1D8] DEBUG WinAgent.WinAgentNetworkProcessor - Started the NetworkDisconnect timer with id=0 for 180 secs
2014-03-21 16:19:10,829 [Th 000001F8] DEBUG WinAgent.WinAgentNetworkProcessor - TimerCompletionEv: Received TimerCompletionEv with id=0
2014-03-21 16:19:10,830 [Th 000001F8] INFO_WinAgent.WinAgentNetworkProcessor - CWinAgentNetworkProcessor:: <b>BounceInterface() IfName=Local</b> Area Connection
2014-03-21 16:19:10,935 [Th 000001F8] INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection
2014-03-21 16:19:11,023 [Th 000001EC] INFO_WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous <b>num</b> interfaces=1 Current num interfaces=0
2014-03-21 16:19:11,024 [Th 000001EC] WARN_WinAgent.WinAgentNetworkProcessor - The interface information has changed. Following interface information has changed. Following interface information, ip={10.20.23.123} mac={00:1d:09:cc:a2:bc} can't be found
2014-03-21 16:19:11,481 [Th 000001F8] INFO_WinAgent.WinAgentNetworkControl - Successfully disabled(BOUNCE) the Network interface Local Area Connection
2014-03-21 16:19:13,481 [Th 000001F8] INFO WinAgent.WinAgentNetworkControl - Enabling the Network interface Local Area Connection
2014-03-21 16:19:15,510 [Th 000001F8] INFO WinAgent.WinAgentNetworkControl - Successfully enabled (BOUNCE) the Network interface Local Area Connection

2014-03-21 16:19:15,776 [Th 000001EC] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration

2014-03-21 16:19:15,776 [Th 000001EC] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0|Current num interfaces=1

2014-03-21 16:19:15,777 [Th 000001EC] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123}|mac={00:1d:09:cc:a2:bc}

🕽 winagent_0.log (1.6 MB) - BareTail	_ <b>_ _</b> ×
Elle Edit View Preferences Help	
😂 Open 🌽 Highlighting 🔽 Follow Tail 🔼 ANSI 📃 C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagen_0.log (1.6 MB)	
winagent_0.log 🔻 ClearPassOnGuard_0.log 👻	
INFO Winkgent.WinkgentDisconnectHandler - Disconnect cancel event timedout	
DEBUG Winkgent.WinkgentNetworkProcessor - TimerCompletionEv: Received TimerCompletionEv with id=0	
<ul> <li>INFO Winkgent.WinkgentNetworkProcessor - CWinkgentNetworkProcessor::BounceInterface() IfName=Local Area Connection</li> </ul>	
INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection	
DEBUG Winkgent.WinkgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification	
<ul> <li>INFO Winkgent.WinkgentNetworkProcessor - Run: Network Interface Change event signalled</li> </ul>	
INFO Winkgent.WinkgentNetworkProcessor - Possible change in the network configuration	
INFO Winkgent.WinkgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=1 Current num interf	aces=0
VARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Following interface information, ip=(10.20	.23.123) mac=(00:1d:09:cc:a2:bc}
◇INFO WinAgent,WinAgentNetworkControl - Successfully disabled(BOUNCE) the Network interface Local Area Connection	
INFO Winkgent.WinkgentNetworkControl - Enabling the Network interface Local Area Connection	
• INFO WinAgent.WinAgentNetworkControl - Successfully enabled(BOUNCE) the Network interface Local Area Connection	
INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration	
INFO Winkgent.WinkgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0 Current num interf	aces=1
VARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip=(10.20.	23.123)   mac=(00:1d:09:cc:a2:bc)
	-
	P Z

# **Third-Party Application Logs**

On Windows, **OnGuard Agent** uses the Windows Update Service for installing missing Hotfixes and Security Updates. Sometimes, the Windows Update Log file is helpful in debugging issues related to Hotfixes and Security Updates.

Location - "%SystemRoot%\WindowsUpdate.log"

Whenever **OnGuard Agent** uses Windows Update Service, it sets the ClientId as 'ClearPass **OnGuard Agent**' which can be seen in the Windows Update Log file.

## Windows Update Logs (Search Successful):

2014-02-21	16:38:58:568	2280	9fc	Misc	= Process: C:\Program Files\Aruba
<mark>Networks\Clear</mark>	PassOnGuard\Clear	PassAgent(	Controlle	<mark>exe</mark>	
2014-02-21	16:38:58:568	2280	9fc	COMAPI	START COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-21	16.28.58.600	2280	Ofc	COMADI	Con SUBMITTED COMADI: Search [ClientId - ClearDass OnGuard Agent]
2014-02-21	10.30.30.009	2200	n	COMALI	Solution and a search [Chentin - Clear ass onotiand Agent]
2014-02-21	16:38:58:610	1028	16c4	Agent	** START ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]
2014-02-21	16:38:58:610	1028	16c4	Agent	* Online = No; Ignore download priority = No
2014-02-21	16.38.58.610	1028	16c4	Agent	* Criteria - "IsInstalled-0 and CategoryIDs contains '0fa1201d-4330-4fa8-8ae9-
b877473b6441'''	10.30.30.010	1020	1004	Agent	
00//4/300441					
2014-02-21	16:38:58:610	1028	16c4	Agent	* ServiceID = {7971F918-A847-4430-9279-4A52D1EFE18D} Third party service
2014-02-21	16:38:58:610	1028	16c4	Agent	* Search Scope = {Machine}
2014-02-21	16.40.48.426	1028	16c4	Agent	* Added undate (RFF25D62-3828-44FF-9860-502DC4F14C28) 104 to search
rocult	10.40.40.420	1020	1004	Agent	
result					
2014-02-21	16:40:48:426	1028	16c4	Agent	* Added update {0D0CF44E-972C-44F3-BC97-B705E2EDD736}.201 to search
result					
2014-02-21	16:40:48:426	1028	16c4	Agent	* Added update {D8DCB8C5-4130-4AAF-8C68-C652EAD3A7EA}.201 to search
<mark>result</mark>					
2014-02-21	16.40.48.426	1028	16c4	Agent	* Added undate /348303FC-CCBB-4FB1-88CD-191FF876FFCA) 201 to search
rocult	10.40.40.420	1020	1004	Agent	
result					
		1000			
2014-02-21	16:40:48:427	1028	16c4	Agent	Update {200DFFAD-C01D-49ED-9BA4-80EC7D6EA6F0}.201 is pruned out due to
potential superse	edence				
2014-02-21	16:40:48:427	1028	16c4	Agent	* Added update {B5C84092-6294-4358-86EB-7D743AABD04A}.201 to search
result				U	
2014-02-21	16.40.48.427	1028	16.4	Agont	Undate (406288AE 1205-40D2-8880-14D852C8280E) 201 is pruned out due to
2014-02-21	10.40.40.427	1020	1004	Agent	opuale (49020DAI-1303-40D2-DDB)-14D032002D0B3201 is pruned out due to
potential superse					
2014-02-21	16:40:48:427	1028	16c4	Agent	* Added update {7BDE8A96-F0DA-485F-8778-F2927A2B1D2B}.201 to search
result					
-					
2014-02-21	16.40.48.431	1028	16c4	Agent	* Added undate {9655393D-1846-4642-4021-04D185E960D1} 202 to correl
rocult	10.10.10.10.101	1020	TUCT	ngent	Mada aparte (90000900 1010 1012-1021-0401001-90001-202 10 Startin
i court					

Aruba Networks

2014-02-21 out of 2424 dep	16:40:48:432 loyed entities	1028	16c4	Agent	* Found 63 updates and 10 categories in search; evaluated appl. rules of 1221
2014-02-21	16:40:48:513	1028	16c4	Agent	** END ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]
2014-02-21	16:40:48:577	2280	15cc	COMAPI	>> RESUMED COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-21	16:40:48:835	2280	15cc	COMAPI	- Updates found = 63
2014-02-21	16:40:48:835	2280	15cc	COMAPI	END COMAPI: Search [ClientId = ClearPass OnGuard Agent]

WindowsUpda	ite.log (1.8 MB) - BareTail					_1	J×
	Historius E Estan Tail ANCI			Laure VI Canalaur	and the second se		-
Upen V Hig			- C. Wind		supportering (1.0 mb)		
winagent_0.log	ClearPassOnGuard_0.log	V wina	gent_remediate	_0.log •	WindowsUpdate.log 🗸	< )	×
02014-02-21	16:38:58:568	2280	9fc	Misc	======= Logging initialized (build: 7.6.7600.256, tz: +0530) ==========		
◆2014-02-21	16:38:58:568	2280	9fc	Misc	= Process: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassAgentController.exe		
02014-02-21	16:38:58:568	2280	9fc	Misc	= Module: C:\Windows\system32\wuapi.dll		
02014-02-21	16:38:58:568	2280	9fc	COMAPI			
◆2014-02-21	16:38:58:568	2280	9fc	COMAPI	START COMAPI: Search [ClientId = ClearPass OnGuard Agent]		
02014-02-21	16:38:58:568	2280	9fc	COMAPI			_
02014-02-21	16:38:58:609	2280	9fc	COMAPI	< SUBMITTED COMAPI: Search [ClientId = ClearPass OnGuard Agent]		
02014-02-21	16:38:58:609	1028	16c4	Agent	*******		_
02014-02-21	16:38:58:610	1028	1604	Agent	** START ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]		-
02014-02-21	16:38:58:610	1028	1604	Agent	*****		
02014-02-21	16:38:58:610	1028	16c4	Agent	* Online = No; Ignore download priority = No		
02014-02-21	16:38:58:610	1028	16c4	Agent	* Criteria = "IsInstalled=0 and CategoryIDs contains 'Ofal201d-4330-4fa8-8ae9-b877473b6441'"		
02014-02-21	16:38:58:610	1028	1604	Agent	* ServiceID = {7971F918-A847-4430-9279-4A52D1EFE18D} Third party service		
02014-02-21	16:38:58:610	1028	16c4	Agent	* Search Scope = {Machine}		
02014-02-21	16:40:48:426	1028	1604	Agent	* Added update (BEE25D62-3828-44EF-9B60-502DC4F14C2B).104 to search result		
02014-02-21	16:40:48:426	1028	1604	Agent	* Added update {DDUCF44E-972C-44F3-BC97-B705E2EDD736}.201 to search result		
02014-02-21	16:40:48:426	1028	16c4	Agent	* Added update (DBDCB8C5-4130-4AAF-8C68-C652EAD3A7EA).201 to search result		
02014-02-21	16:40:48:426	1028	1604	Agent	* Added update (348303EC-CCBB-4EB1-88CD-191EF876EFCA).201 to search result		
02014-02-21	16:40:48:427	1028	16c4	Agent	Update {200DFFAD-C01D-49ED-9BA4-80EC7D6EA6F0}.201 is pruned out due to potential supersedence		
02014-02-21	16:40:48:427	1028	16c4	Agent	* Added update (BSC84092-6294-4358-86EB-7D743AABD04A).201 to search result		
02014-02-21	16:40:48:427	1028	1604	Agent	Update {496288AF-1305-40D2-BBB9-14D852C82B0E}.201 is pruned out due to potential supersedence		
02014-02-21	16:40:48:427	1028	1664	Agent	* Added update {'BDE8A96-FUDA-485F-87/8-F2927A2B1D2B}.201 to search result		
• ·							
• ·							
02014-02-21	16:40:48:431	1028	1664	agent	* Added update (9745C5C2-5497-4882-9911-69D869531C3).201 to search result		
02014-02-21	16:40:48:431	1028	1604	agent	* Added update (S4D21173-SDSC-4416-8893-C14DE13D18E).201 to Search result		
02014-02-21	16:40:48:431	1028	1604	Agent	* Added update {EA312223-97/1-4708-5548-5981/5141EF4}.203 to search result		
02014-02-21	16:40:46:431	1028	1604	agent	* Added update {/1//401/-3/40-4240-B012-E0500/0E0059}.204 to Search result		
02014-02-21	16:40:48:431	1028	1604	Agent	* Added update (9655393)-1846-4622-c41185196001):202 to search result		
02014-02-21	16:40:48:432	1028	1604	Agent	* Found 53 updates and 10 categories in search; evaluated appl. rules of 1221 out of 2424 de ************************************	pro?	e
02014-02-21	16:40:48:512	1028	1604	agent		_	_
2014-02-21	16:40:48:513	1028	1604	Agent	END Agenc: Finding updates [Callerid = ClearPass Unduard Agent]		-
2014-02-21	16:40:46:513	1028	1604	agent		_	_
2014-02-21	10:40:40:577	2200	1500	COMAPI	Whether found and the search [clientia - clearPass Undura Agenc]		-
2014-02-21	10:40:40:835	2200	1500	COMARI	- opuaces round - os		
2014-02-21	10:40:40:035	2280	1500	COMART	PUR COMMEL, Secret IclientId - ClearDess OnCoard Agenti	_	
2014-02-21	16:40:40:035	2290	1500	COMART	END CONAFT. SCALCH [CITCHCIU - CICALF435 ONGUARD Agent]		-
1	10.10.10.000	2200	1000	CONAP I		(	Ľ.

# Windows Update Logs (Search Failed):

2014-02-22	18:27:53:134	1648	69c	Misc	======= Logging initialized (build: 7.6.7600.256, tz: +0530) ====================================
2014-02-22	18:27:53:134	1648	69c	Misc	= Process: C:\Program Files\Aruba
Networks \Clear	PassonGuaru\Cleari	PassAgente	ontroller	.exe	
2014-02-22	18:27:53:134	1648	69c	Misc	= Module: C:\Windows\system32\wuapi.dll
2014-02-22	18:27:53:134	1648	69c	COMAPI	
2014-02-22	18:27:53:134	1648	69c	COMAPI	START COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-22	18:27:53:134	1648	69c	COMAPI	
2014-02-22	18:27:53:139	1648	69c	COMAPI	< SUBMITTED COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014 02 22	10.27.52.141	1050	110-	Amerik	******
2014-02-22	18:27:53:141	1052	1130	Agent	
2014-02-22	18.27.53.141	1052	113c	Agent	** START ** Agent: Finding undates [CallerId = ClearPass OnGuard Agent]
	10.27.00.111	1001	1100	ingent	onner ingener inneng apaares foaner in eien rass onotar angenej
2014-02-22	18:27:53:141	1052	113c	Agent	******
2014-02-22	18:27:53:141	1052	113c	Agent	* Online = No; Ignore download priority = No

2014-02-22	18:27:53:141	1052	113c	Agent	* Criteria = "IsInstalled=0 and CategoryIDs contains '0fa1201d-4330-4fa8-8ae9-
<mark>b877473b6441'"</mark>					
224 4 22 22		1050	440		
2014-02-22	18:27:53:141	1052	113c	Agent	* ServiceID = {7971F918-A847-4430-9279-4A52D1EFE18D} Third party service
2014 02 22	10.27.52.1/1	1052	1120	Agont	* Search Scone - (Machina)
2014-02-22	10.27.33.141	1032	1150	Agent	Search Scope – {Machine}
2014-02-24	00.55.31.535	1052	134	AH	All setting next sam report timeout to 2014-02-24 19:25:31
	00.00.01.000	1002	101	110	
2014-02-24	00:56:19:590	1052	134	AU	AU initiates service shutdown
2014-02-24	00:56:19:590	1052	134	AU	############ AU: Uninitializing Automatic Updates ####################################
2014-02-24	00:56:25:455	1052	113c	Agent	* WARNING: Exit code = 0x8024000B
2014-02-24	00:56:25:455	1052	113c	Agent	*****
2011.02.24		1050	440	<b>A</b> .	
2014-02-24	00:56:25:455	1052	113C	Agent	** END ** Agent: Finding updates [Callerid = ClearPass UnGuard Agent]
2014-02-24	00.56.25.455	1052	1120	Agont	*******
2014-02-24	00.30.23.433	1052	1150	Agent	
2014-02-24	00:56:25:455	1052	113c	Agent	WARNING: WU client failed Searching for undate with error 0x8024000b
				8	8
<mark>2014-02-24</mark>	00:56:25:502	1648	418	COMAPI	>> RESUMED COMAPI: Search [ClientId = ClearPass OnGuard Agent]
<mark>2014-02-24</mark>	00:56:25:502	1052	134	Agent	Sending shutdown notification to client
2014-02-24	00:56:25:502	1648	fa4	COMAPI	WARNING: Received service shutdown/self-update notification.
2014 02 24		1(40	410	COMADI	
<mark>2014-02-24</mark>	00:56:25:564	1648	418	COMAPI	- Updates round = 0
2014-02-24	00.56.25.564	1648	418	СОМАРІ	- WARNING: Evit code - 0v0000000 Result code - 0v8024001F
2011-02-21	00.30.23.304	1010	110	COMMI	Windiand, Exit cout = 0.00000000, Result cout = 0.0024001E
2014-02-24	00:56:25:564	1648	418	COMAPI	
2014-02-24	00:56:25:564	1648	418	COMAPI	END COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-24	00:56:25:564	1648	418	COMAPI	
2014-02-24	00:56:25:596	1648	14c	COMAPI	WARNING: Operation failed due to earlier error, hr=8024001E
2014 02 24	00.56.25.506	1640	14-	COMADI	EATAL Unable to complete complete complete control (in 0024004E)
<mark>2014-02-24</mark>	00:56:25:596	1048	14C	COMAPI	FATAL: Unable to complete asynchronous search. (hr=8024001E)
2014-02-24	00.56.25.611	1052	134	Report	CWERReporter finishing event handling (0000000)
	0.00.20.011	1034	151	Report	- or Encoporter millioning event nandmiller (0000000)

関 Window	wsUpdate.	log (1.8 MB) - BareTail					>
<u>File E</u> dit	<u>V</u> iew Pre	ferences <u>H</u> elp					
൙ Ope <u>n</u>	🌽 Highlig	hting 🔲 Follo <u>w</u> Tail 🛛 ANSI		C:\Window	vs\Window	rsUpdate.log (1.8 MB)	
winagent_	0.log 🔹	ClearPassOnGuard_0.log	V wina	gent_remediate_0.	log 🔍	WindowsUpdate.log 🔹	< > >
02014-	02-22	18:27:53:134	1648	69c 1	Misc	======= Logging initialized (build: 7.6.7600.256, tz: +0530) =========	
<ul> <li>2014-</li> </ul>	02-22	18:27:53:134	1648	69c I	Misc	= Process: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassAgentController.exe	
◇2014-	02-22	18:27:53:134	1648	69c I	Misc	= Module: C:\Windows\system32\wuapi.dll	
02014-	02-22	18:27:53:134	1648	69c (	COMAPI		
♦ 2014-	02-22	18:27:53:134	1648	69c (	COMAPI	START COMAPI: Search [ClientId = ClearPass OnGuard Agent]	
2014-	02-22	18:27:53:134	1648	69c (	COMAPI		
<ul> <li>2014-</li> </ul>	02-22	18:27:53:139	1648	69c (	COMAPI	< SUBMITTED COMAPI: Search [ClientId = ClearPass OnGuard Agent]	
02014-	02-22	18:27:53:141	1052	113c .	Agent	********	
<ul> <li>2014-</li> </ul>	02-22	18:27:53:141	1052	113c .	àgent	** START ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]	
0 2014-	02-22	18:27:53:141	1052	113c .	Agent	*****	
02014-	02-22	18:27:53:141	1052	113c .	lgent	* Online = No; Ignore download priority = No	_
02014-	02-22	18:27:53:141	1052	113c .	lgent	* Criteria = "IsInstalled=0 and CategoryIDs contains 'Ofa1201d-4330-4fa8-8ae9-b877473b6441'"	
02014-	02-22	18:27:53:141	1052	113c .	Agent	* ServiceID = (7971F918-1847-4430-9279-4152D1EFE18D) Third party service	
◊ 2014-	02-22	18:27:53:141	1052	113c .	lgent	* Search Scope = (Machine)	
02014-	02-24	00:55:31:535	1052	134 .	AU	AU setting next sqm report timeout to 2014-02-24 19:25:31	
02014-	02-24	00:56:19:590	1052	134 .	AU	AU initiates service shutdown	
02014-	02-24	00:56:19:590	1052	134 .	AU	########### AU: Uninitializing Automatic Updates ####################################	
♦ 2014-	02-24	00:56:25:455	1052	113c .	Agent	* WARNING: Exit code = 0x8024000B	
◊ 2014-	02-24	00:56:25:455	1052	113c .	lgent	****	
o 2014-	02-24	00:56:25:455	1052	113c .	àgent	** END ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]	
0 2014-	02-24	00:56:25:455	1052	113c .	Agent	******	
♦ 2014–	02-24	00:56:25:455	1052	113c .	Agent	WARNING: WU client failed Searching for update with error 0x8024000b	
♦ 2014-	02-24	00:56:25:502	1648	418 (	COMAPI	>> RESUMED COMAPI: Search [ClientId = ClearPass OnGuard Agent]	
0 2014-	02-24	00:56:25:502	1052	134 .	Agent	Sending shutdown notification to client	
♦ 2014-	02-24	00:56:25:502	1648	fa4 (	COMAPI	WARNING: Received service shutdown/self-update notification.	
0 2014-	02-24	00:56:25:564	1648	418 (	COMAPI	- Updates found = 0	
♦ 2014-	02-24	00:56:25:564	1648	418 0	COMAPI	- WARNING: Exit code = 0x00000000, Result code = 0x8024001E	
0 2014-	02-24	00:56:25:564	1648	418 (	COMAPI		
0 2014-	02-24	00:56:25:564	1648	418 (	COMAPI	END COMAPI: Search [ClientId = ClearPass OnGuard Agent]	
◊ 2014-	02-24	00:56:25:564	1648	418 (	COMAPI		
♦ 2014-	02-24	00:56:25:596	1648	14c (	COMAPI	WARNING: Operation failed due to earlier error, hr=8024001E	
02014-	02-24	00:56:25:596	1648	14c (	COMAPI	FATAL: Unable to complete asynchronous search. (hr=8024001E)	
02014-	02-24	00:56:25:611	1052	134 1	Report	CWERReporter finishing event handling. (00000000)	
L com	m		1050		- · ·	and a second secon	-
							<u> </u>

# **Appendix A – Tools and Utilities**

List of Third-Party Tools and utilities that are helpful in debugging:

TCPView – To view all the open Ports on Windows OS.

Link - http://technet.microsoft.com/en-in/sysinternals/bb897437.aspx

TCPView - Sysinternals: www.sysinternals.com									
File Options Process View	File Options Process View Help								
Process A	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
chrome.exe     chrome.exe     chrome.exe     chrome.exe     ClearPassAgentController.exe     ClearPassAgentController.exe	28132 28132 28132 40720 40720	TCP TCP TCP TCP TCP TCP	lap-01-1617.ad.cs lap-01-1617.ad.cs lap-01-1617.ad.cs LAP-01-1617 LAP-01-1617	41371 41372 41373 25427 25427	umps2-c2-2-chi.sal umps2-c2-2-chi.sal umps2-c2-2-chi.sal LAP-01-1617 LAP-01-1617	https https https 0 0	ESTABLISHED ESTABLISHED ESTABLISHED LISTENING LISTENING		
ClearPassUncluard exe     ClearPassUncluard exe     CmRcService.exe     CmRcService.exe     CmRcService.exe     Communicator.exe     Communicator.exe     Porpbox.exe     Porpbox.exe	55572 5200 5200 5152 5152 6696 6696	UDP TCP TCPV6 TCP UDP TCP TCP	LAP-01-1617 LAP-01-1617 LAP-01-1617.ad.cs lap-01-1617.ad.cs LAP-01-1617 LAP-01-1617 LAP-01-1617	26671 60215 sms-rcinfo sms-rcinfo 23647 51979 3983 17500	localhost * LAP-01-1617 lap-01-1617.ad.cs sjclync02.arubane * localhost LAP-01-1617	* 0 0 5061 * 19872 0	ESTABLISHED LISTENING LISTENING ESTABLISHED ESTABLISHED LISTENING		24 2,61

Baretail - Log viewer for Windows.

Link - https://www.baremetalsoft.com/baretail/

Baretail has option to highlight matching text in different colors – Preferences->Highlighting.

Highlighting			×
CollectHeal ERROR SEVERE failed isHealthSts healthStatu Sohr Bounce ProcessSoHr ClearPass	CollectHez ERROR SEVERE failed isHealthSt healthSt bealthSt Bounce ProcessSo ClearPass Microsoft	alth ateChanged Js >HrResponse	
Add	D <u>e</u> lete	Move <u>U</u> p	Move <u>D</u> own
Eoreground Color:	•	Background Co	lor:
InterfaceUp			
☑ Ignore Case	In <u>v</u> ert Ma	atch 🗖 B <u>o</u> ld	Lītalic Cancel

To view open Ports on Mac OS X, use following commands:

```
>netstat -a -p tcp
>sudo lsof -i -P | grep -i "listen"
```

#### CLI Command to check if **Backend Service** is running on Mac OS X:

>sudo launchctl list | grep -i arubanetworks.servicedaemon

### Command to Start **Backend Service** on Mac OS X:

>sudo launchctl load /Library/LaunchDaemons/com.arubanetworks.servicedaemon.plist

#### Command to Stop **Backend Service** on Mac OS X:

>sudo launchctl unload /Library/LaunchDaemons/com.arubanetworks.servicedaemon.plist

# **Appendix B – References**

1. OnGuard In A Cluster Tech Note - <u>https://arubapedia.arubanetworks.com/arubapedia/images/2/2e/OnGuard\_in\_a\_Cluster.pdf</u>



- 2. ClearPass OnGuard FAQ https://arubapedia.arubanetworks.com/arubapedia/index.php/OnGuard\_FAQ
- 3. ClearPass OnGuard Overview https://arubapedia.arubanetworks.com/arubapedia/index.php/ClearPass\_OnGuard
- 4. ClearPass OnGuard Evaluation CheckList https://arubapedia.arubanetworks.com/arubapedia/index.php/ClearPass\_OnGuard\_Evalualtion\_ Checklist
- 5. ClearPass OnGuard Firewall WhiteList https://arubapedia.arubanetworks.com/arubapedia/index.php/OnGuard\_Firewall\_Whitelist
- 6. ClearPass 6.3 OnGuard Dissolvable Agent Workflow and Configuration https://arubapedia.arubanetworks.com/arubapedia/index.php/ClearPass\_6.3\_OnGuard\_Dissolva ble\_Agent\_Workflow\_and\_Configuration
- 7. ClearPass OnGuard Auto-Remediation -<u>https://arubapedia.arubanetworks.com/arubapedia/index.php/Clearpass\_Onguard\_Auto-Remediation</u>