



ClearPass

OnGuard Troubleshooting

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

Table of Contents

Overview	4
Introduction	4
ClearPass OnGuard Agent Components	4
Communication between ClearPass OnGuard Agent Components and CPPM Server	7
ClearPass OnGuard Agent Installation.....	8
Language Selection.....	8
Post Installation	9
Launching OnGuard Agent.....	9
Health Monitoring and Auto-Remediation	10
Health Collection Interval for Each Health Class	10
Health Checks and Auto-Remediation	11
Troubleshooting ClearPass OnGuard	13
OnGuard Health Log View	13
Troubleshooting Common Issues	15
ClearPass OnGuard Agent does not start health checks automatically	15
ClearPass OnGuard Agent bounces the Network Interface and performs health checks every 3 minutes	22
ClearPass OnGuard Agent shows Healthy and connects to the Network but no WebAuth Request is seen in Access Tracker	22
Network Interface is bounced a few minutes after OnGuard Agent is closed	22
Auto-Remediation does not work and the client remains Unhealthy	23
ClearPass OnGuard Agent Flow	26
Read CPPM Server IP Address List	28
Establish Connection with Backend Service.....	30
Active Network Interface List.....	33

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	88
Appendix B – References	90

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™ 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:

1. **ClearPass OnGuard User Interface (OnGuard Frontend) – OnGuard Frontend** is the main UI window of ClearPass OnGuard. It has separate UI sections for VPN and Health Checks. It 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”

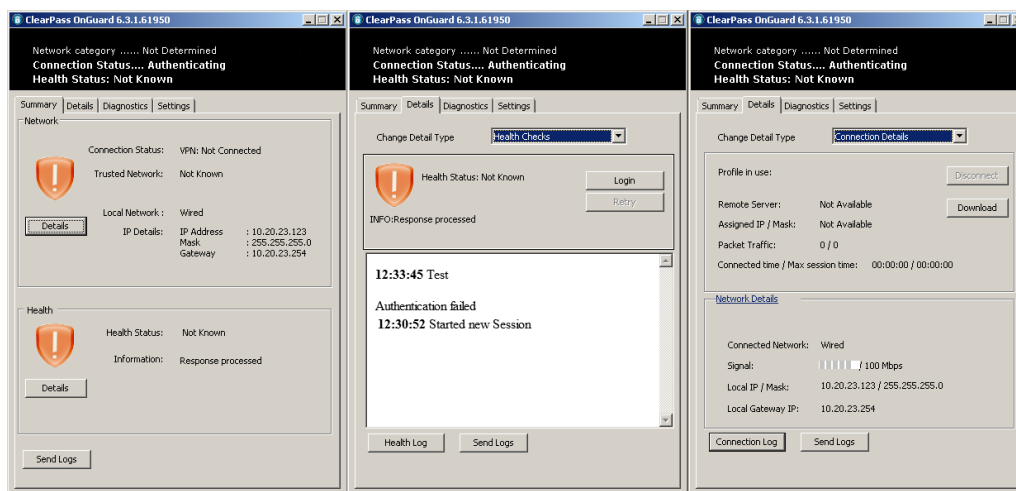


Figure 1 - Windows GUI Summary

Mac OS X:

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

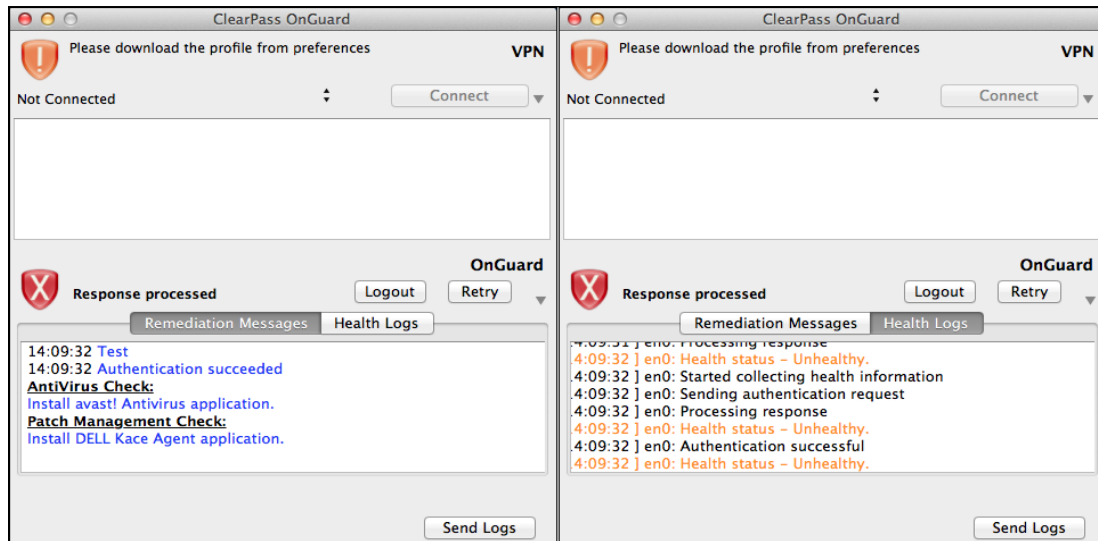


Figure 2 - OSX GUI Summary

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

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

Windows:

- File Name – ClearPassOnGuardPlugin.dll
- Path - %ProgramFiles%\Aruba Networks\ClearPassOnGuard
- 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 auto-remediation 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

7. **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.

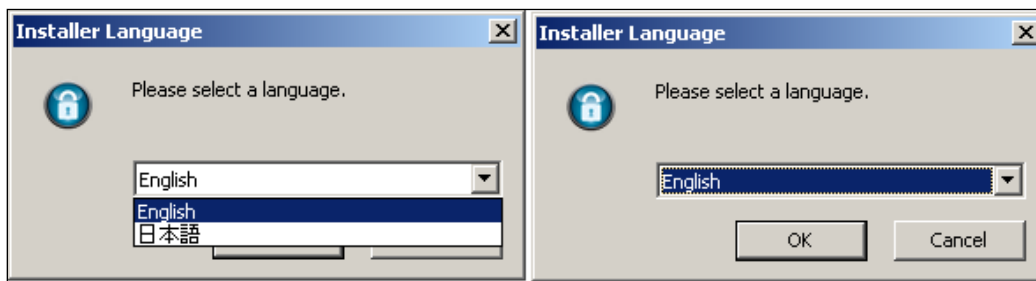


Figure 3 - Language installation selection

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.

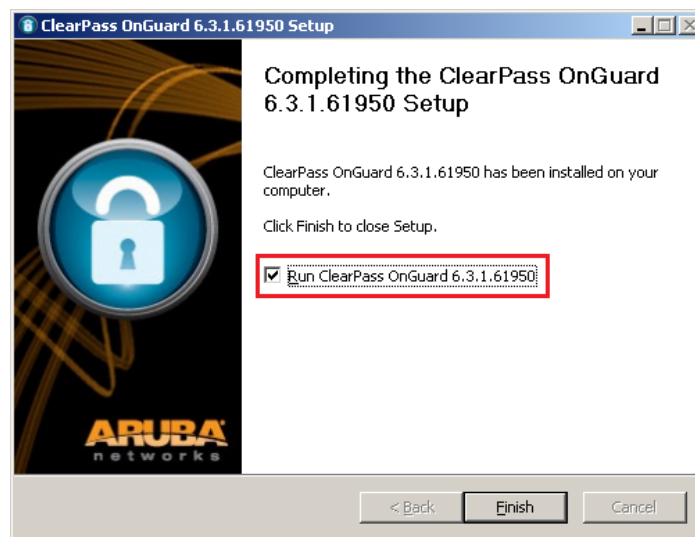
Post Installation

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 '[Monitor Health State & Soft Re-Auth](#)' 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 auto-remediation of which health check/health class:

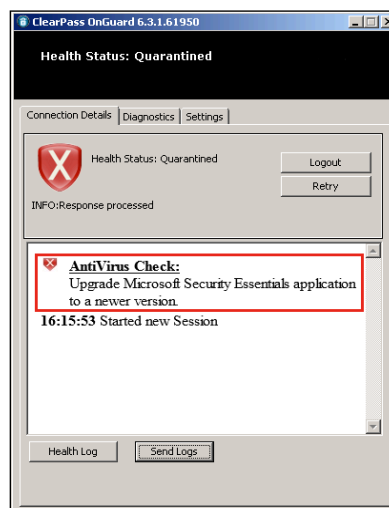
Health Class Name	Health Check	Auto-Remediation Done By
Services	Start/Stop Services	Backend Service
Firewall	Change Status	Backend Service
AntiVirus	Set RTP Status, Dat File Update, Full System Scan	USHA Remediate Application
AntiSpyware	Set RTP Status, Dat File Update, Full System Scan	USHA Remediate 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
	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 – Security Updates	Enable	Backend Service
	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:

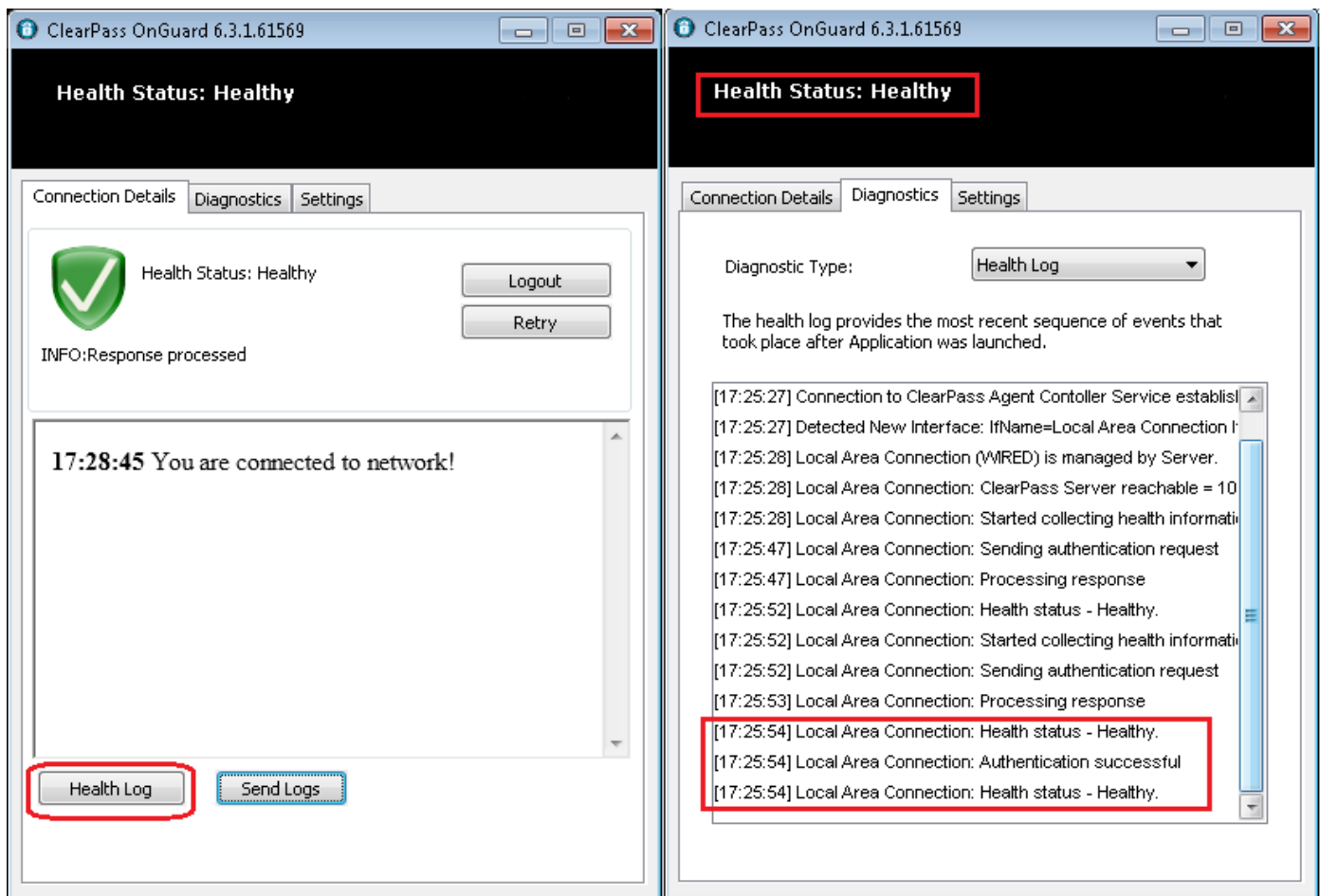


Figure 4 Windows OnGuard – Health Logs

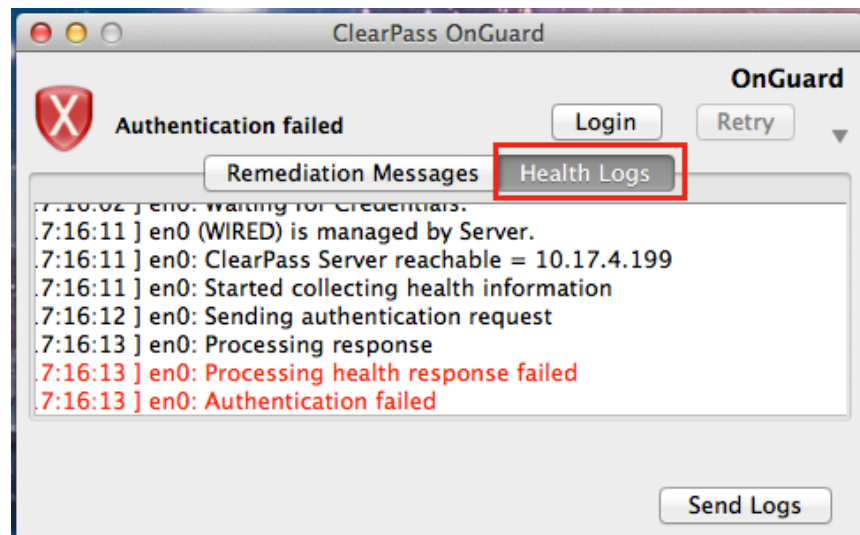


Figure 5 Mac OnGuard – Health Logs

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.

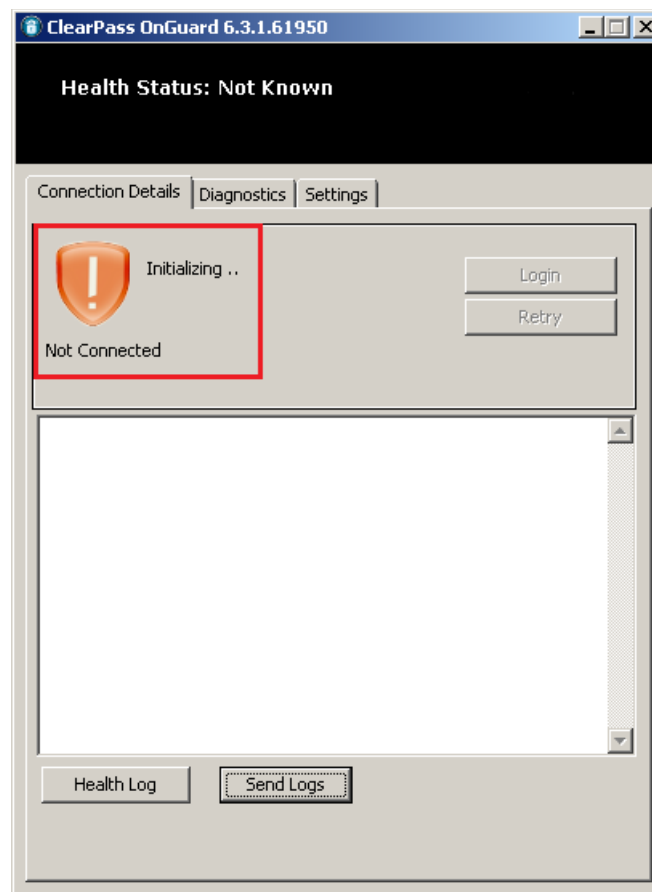


Figure 6 OnGuard stuck at Initializing

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.

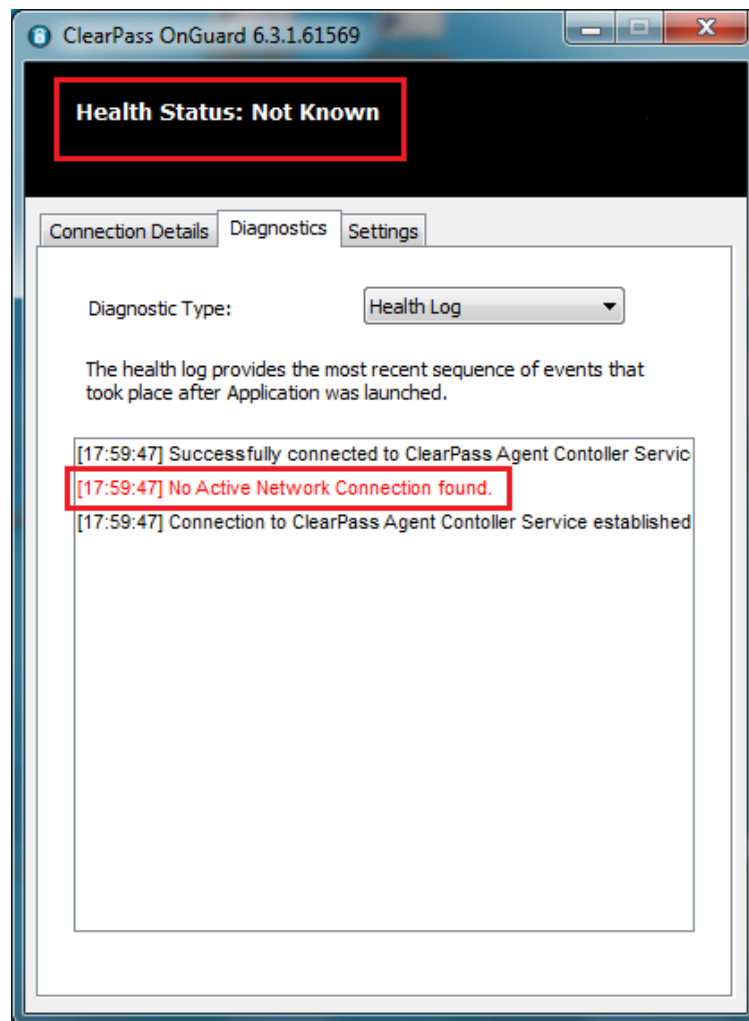


Figure 7 OnGuard - No Active Network Connection

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.

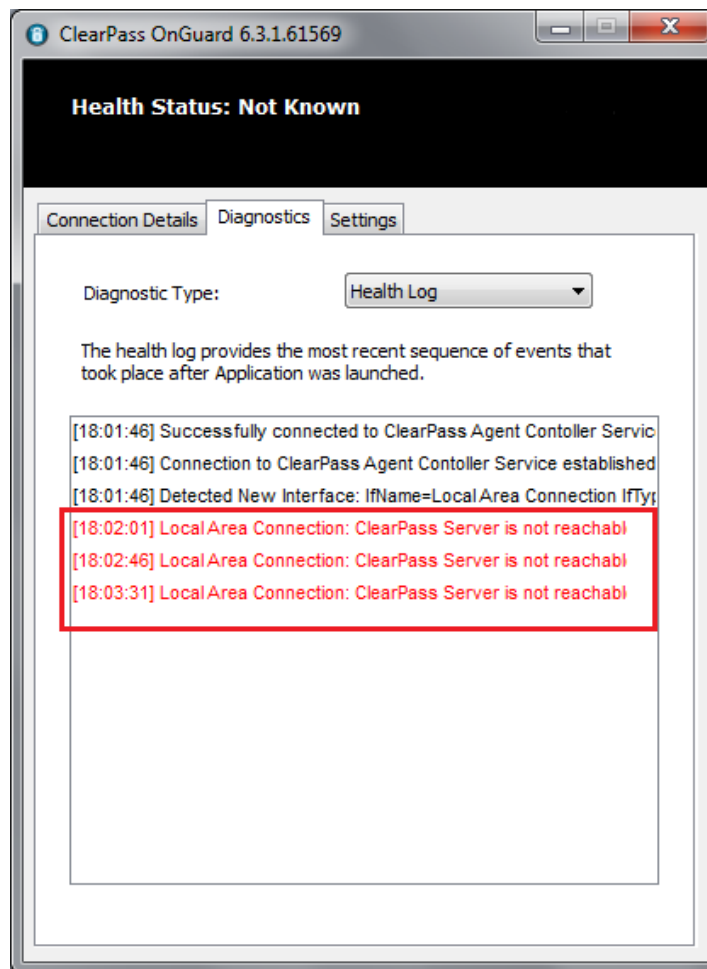


Figure 8 OnGuard - CPPM Server Not Reachable

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.

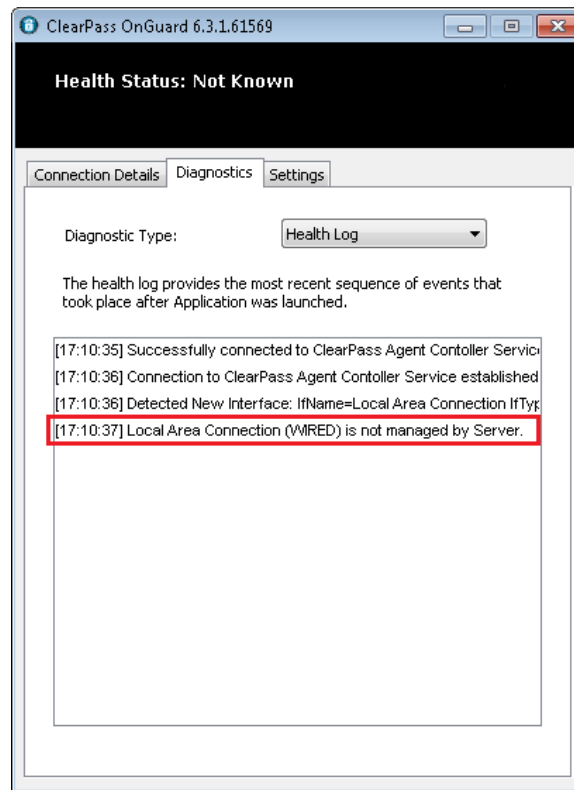


Figure 9 OnGuard - Unmanaged Network Interface

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

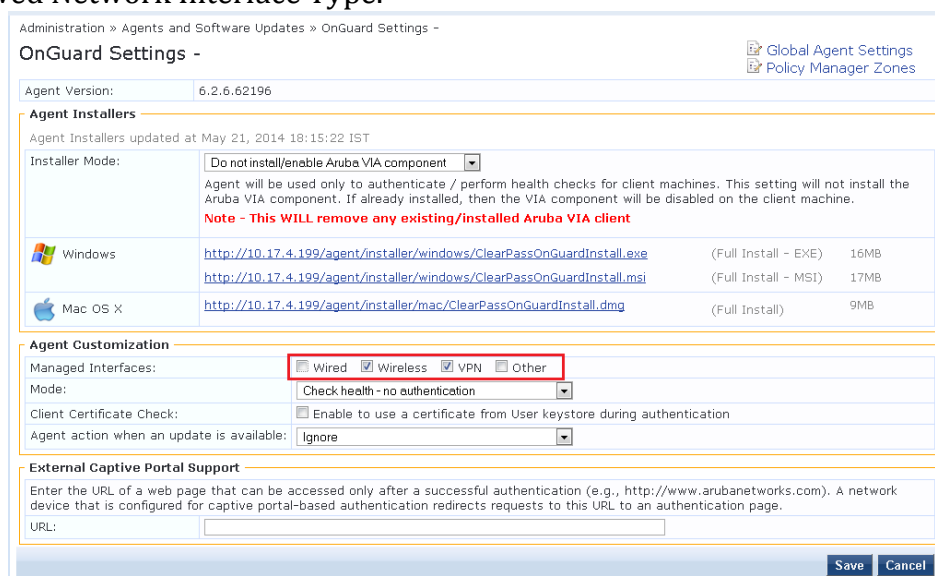


Figure 10 CPPM - Managed Interfaces

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

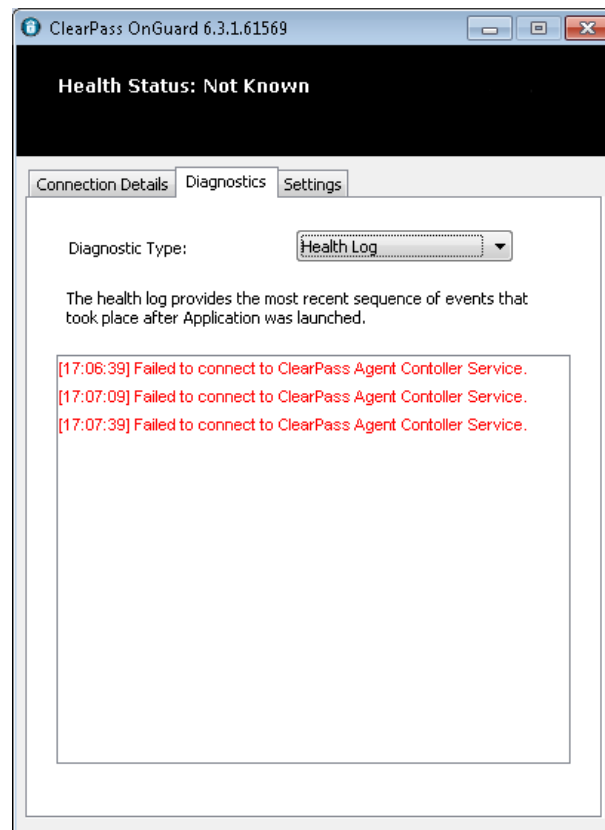


Figure 11 OnGuard - Backend Service Not Running

Resolution – Start **Backend Service** manually. On Windows OS, use Windows Service Manager. For Mac OS X, refer point 5 of [Appendix A](#).

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.

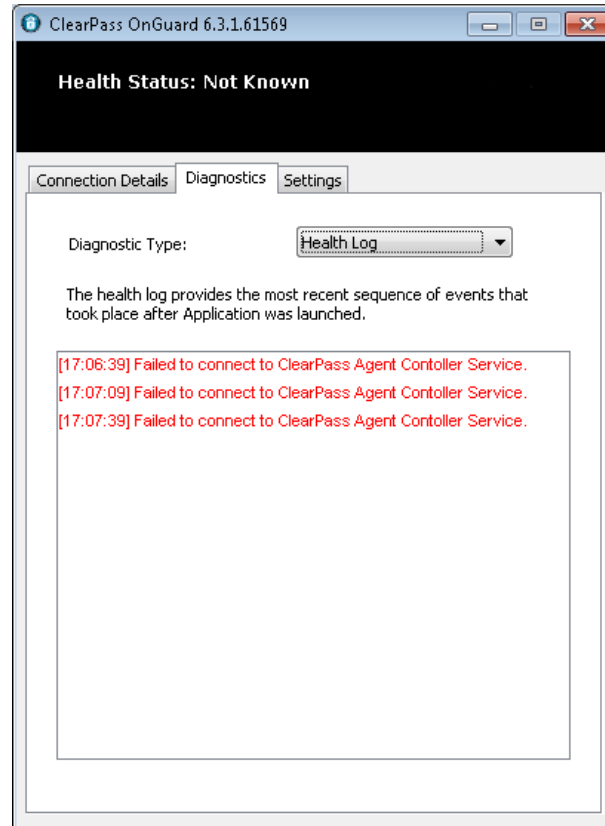


Figure 12 OnGuard - Backend Service Not Running

This can happen because of the following reasons:

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

Resolution –

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

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 [ClearPass OnGuard Agent Components](#) 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 [ClearPass OnGuard Agent Components](#) 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 [Establish Control Channel](#) 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 [Quit](#) 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.

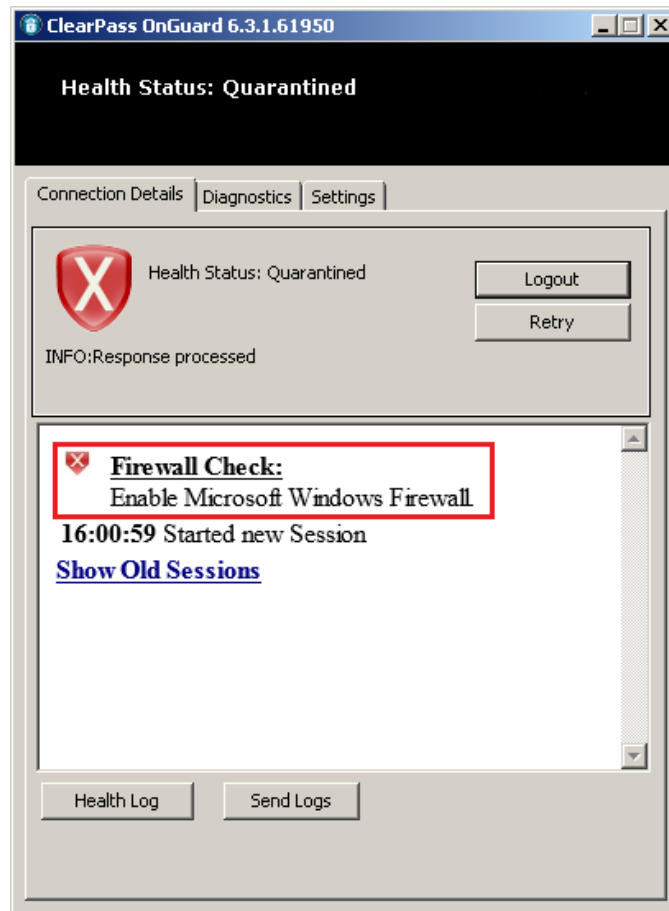


Figure 13 OnGuard - Auto-Remediation failed

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 auto-remediation at the Service Level. If this flag is FALSE, then the **OnGuard Agent** will not perform the auto-remediation for **any** of the health classes.

Configuration » Services » Edit - health-only

Services - health-only

Summary Service Roles **Posture** Enforcement

Posture Policies:

Posture Policies: Only OnGuard agent type posture policies are applicable for this service

windows
mac

Remove View Details Modify

–Select to Add–

Default Posture Token: QUARANTINE (20)

Remediate End-Hosts: ☒ Enable auto-remediation of non-compliant end-hosts

Remediation URL:

Posture Servers:

Posture Servers:

Remove View Details Modify

–Select to Add–

[Add new Posture Policy](#)

[Add new Posture Server](#)

[Back to Services](#) Disable Copy Save Cancel

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 Universal System Health Validator

Windows Server 2003 ☒ Enable checks for Windows 7

Windows XP ☒ A firewall application is on

Windows Vista ☒ Remediation checks ☒ Auto Remediation ☒ User Notification

Windows 7 ☒ Product-specific checks ☒ (Uncheck to allow any product)

Services
Processes
Registry Keys
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

Firewall Product Name	Product Version
Microsoft Windows Firewall	no check

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 [Appendix B - References](#) 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	FullSystemScan	GetVirusDefServ	IsFullScanInProg
avast! Endpoint Protection Suite Plus	7.x	V	V	O	V	V	V	V	V	X	V	V
avast! Endpoint Protection Suite Plus	8.x	V	V	O	V	V	V	V	X	X	V	V
avast! File Server Security	7.x	V	V	O	X	V	V	X	V	X	V	V
avast! Free Antivirus	2014.x	V	V	X	V	X	X	X	V	X	X	X
avast! Free Antivirus	5.x	V	V	X	V	V	V	X	X	V	V	X
avast! Free Antivirus	6.x	V	V	X	V	V	V	V	X	V	V	X
avast! Free Antivirus	7.x	V	V	O	V	V	V	V	V	X	V	V
avast! Free Antivirus	8.x	V	V	X	V	V	V	X	V	X	X	X

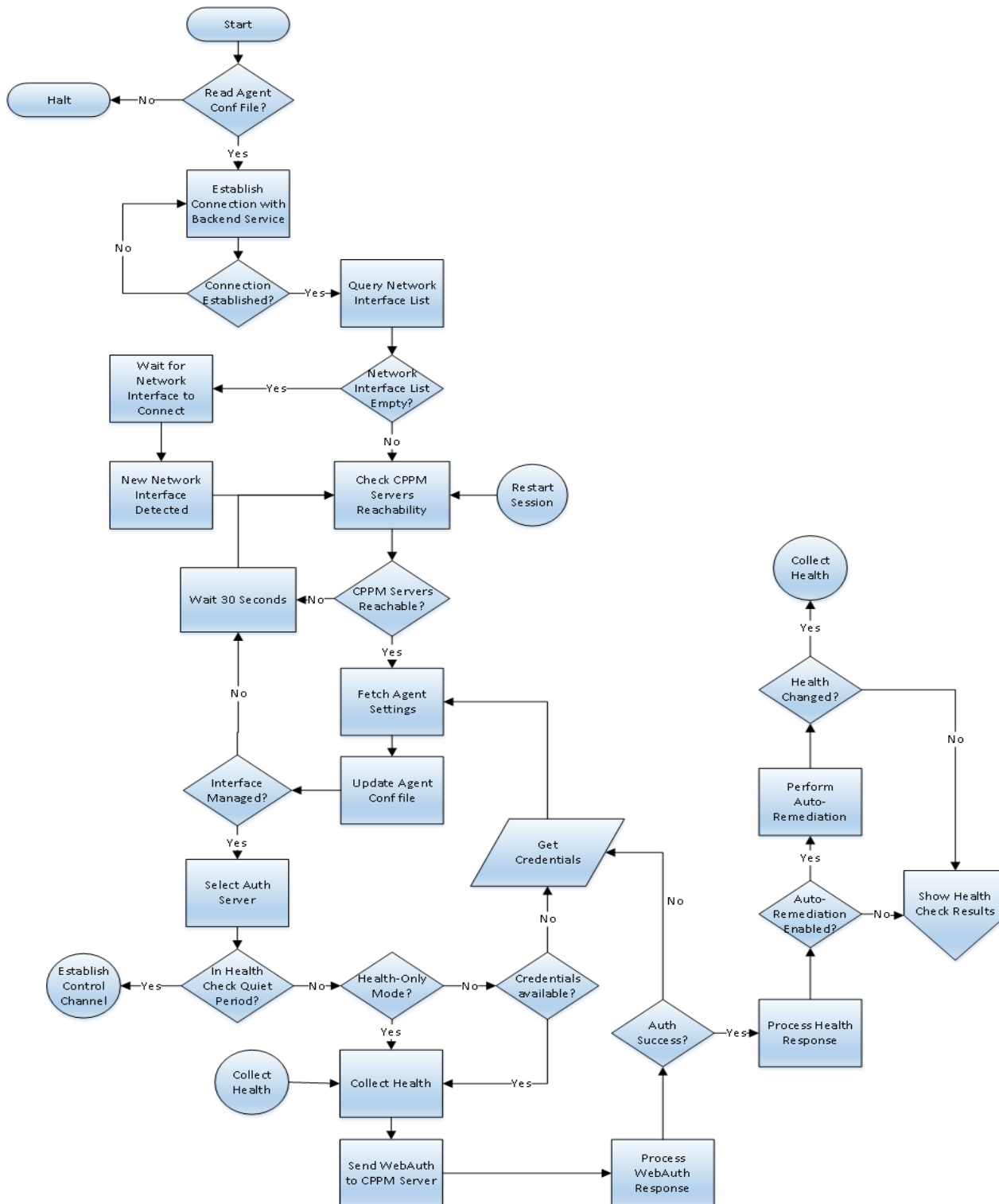
Figure 16 AntiVirus Support Chart

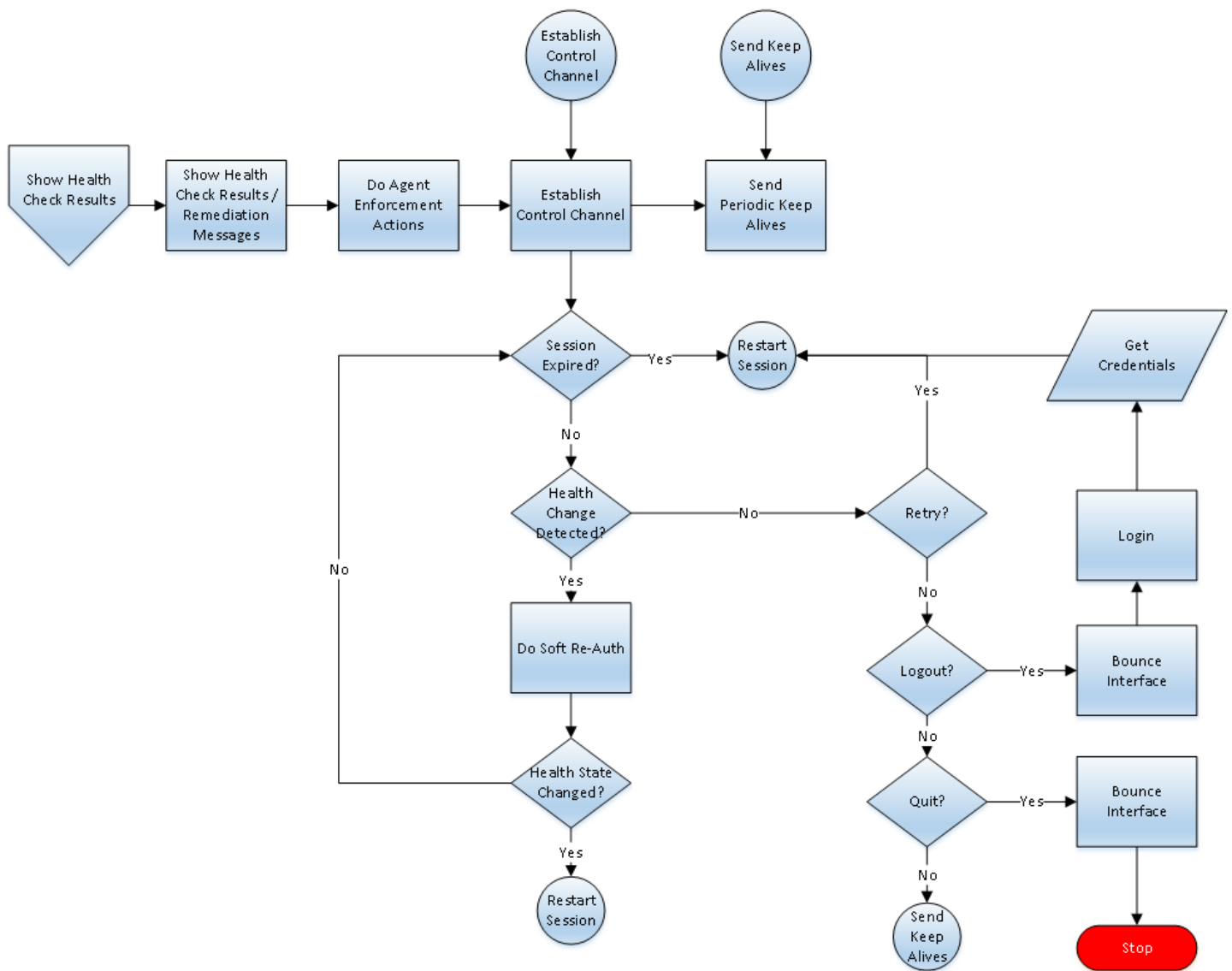
If auto-remediation is not supported or supported but **OnGuard Agent** is not able to perform auto-remediation then contact Aruba TAC Support with **OnGuard Agent** logs to analyze the issue.

Also refer section [Auto-Remediation](#) for more information.

ClearPass OnGuard Agent Flow

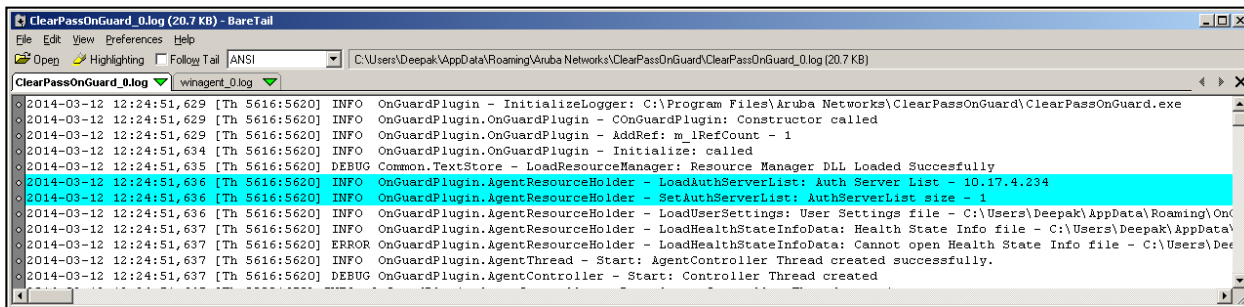
This section explains **OnGuard Agent** Flow from the moment it is launched, till the health checks are over and after that how it monitors client's health state going forward.





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.

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



For Agent Config file paths, refer point #7 in [ClassPass OnGuard Agent Components](#) section.

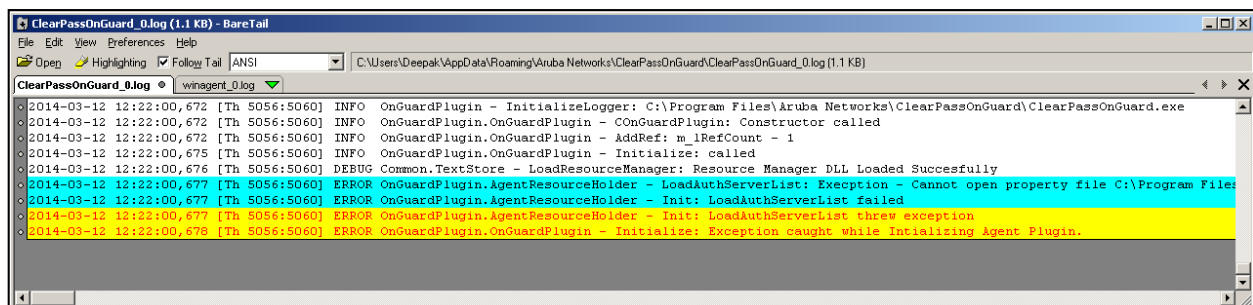
If the **OnGuard Agent** fails to read the CPPM Server IP List from Agent Config file then it will **not** start the health checking functionality and OnGuard UI will show 'Initializing...'.

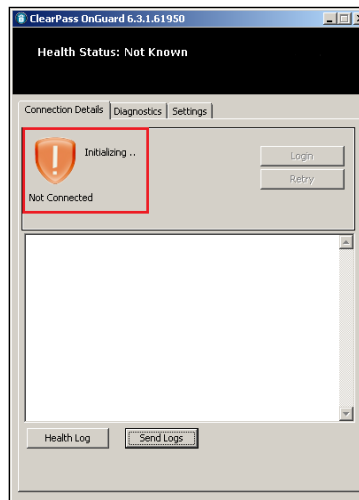
2014-03-12 11:27:22,221 [Th 2956:164] ERROR OnGuardPlugin.AgentResourceHolder - LoadAuthServerList: Exception - Cannot open property file C:\Program Files\Aruba Networks\ClearPassOnGuard\etc\agent.conf

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.





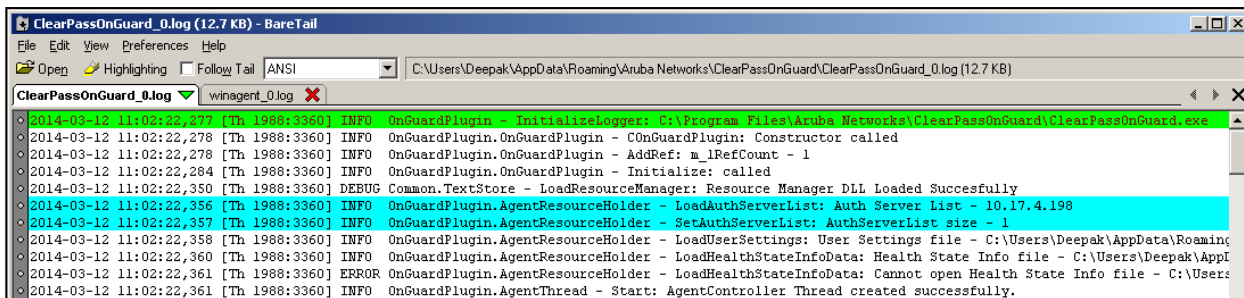
Reading of Agent Config file may fail in the following cases:

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.

Note - The first log (InitializeLogger) written by **OnGuard Agent** to ClearPassOnGuard_0.log file indicates that Agent was just launched.

2014-03-12 11:02:22,277 [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.

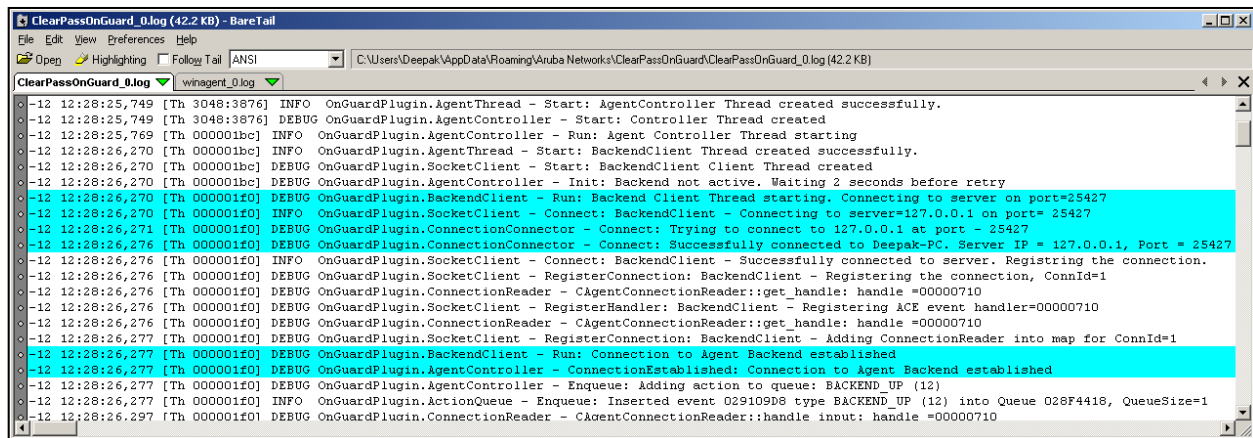


Establish Connection with Backend Service

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

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. Registering 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
```



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
```

```

4-03-12 13:30:34.314 [Th 0000021C] DEBUG WinAgent.ConnectionAcceptor - CWinAgentConnectionAcceptor::handle_input() handle=00000244
4-03-12 13:30:34.314 [Th 0000021C] DEBUG WinAgent.ConnectionAcceptor - Creating new connection for ConnId=1
4-03-12 13:30:34.314 [Th 0000021C] DEBUG WinAgent.ConnectionAcceptor - Posting ConnectionEvent with Id=101
4-03-12 13:30:34.314 [Th 0000021C] INFO Common.EventProcessor - PostEvent: Posting Event 04F3BEE0 (101) into Queue 006D8178 of Thread 00747CA0
4-03-12 13:30:34.314 [Th 0000021C] INFO Common.EventQueue - Enqueue: Inserted event 04F3BEE0 type (101) into Queue 006D8178, QueueSize=1
4-03-12 13:30:34.314 [Th 0000021C] INFO WinAgent.ConnectionAcceptor - CWinAgentConnectionAcceptor::handle_input() Accept Success: Client IP = 127.0.0.1,
4-03-12 13:30:34.314 [Th 000010a8] INFO Common.EventQueue - Dequeue: Removed event 04F3BEE0 type (101) from Queue 006D8178, QueueSize=0
4-03-12 13:30:34.315 [Th 000010a8] INFO Common.EventProcessor - EventThreadHandler: Processing Event 04F3BEE0 (101) from EventQ 006D8178 started
4-03-12 13:30:34.315 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentEventProcessor - CWinAgentEventProcess::ProcessEvent(), processing event callback
4-03-12 13:30:34.315 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentEventRegistry - Found EventHandler for the EventId=101
4-03-12 13:30:34.315 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentConnEvHandler - Processing WinAgentConnEvent
4-03-12 13:30:34.315 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentMessageHandler - Registering the connection, ConnId=1
4-03-12 13:30:34.315 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentMessageHandler - Registering ACE event handler=00000464
4-03-12 13:30:34.315 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentMessageHandler - Adding ConnectionReader into map for ConnId=1
4-03-12 13:30:34.316 [Th 000010a8] Evt 04F3BEE0] INFO WinAgent.WinAgentConnEvHandler - Registration of ReadHandler succeeded
4-03-12 13:30:34.316 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 99:{"content":{"os":"Windows","server":"ClearPass /
4-03-12 13:30:34.316 [Th 000010a8] Evt 04F3BEE0] DEBUG WinAgent.WinAgentEventHandler - Done sending the data. Size - 103
4-03-12 13:30:34.316 [Th 000010a8] Evt 04F3BEE0] INFO Common.EventProcessor - EventThreadHandler: Processing Event (101) from EventQ 006D8178 finished
4-03-12 13:30:34.316 [Th 000010a8] INFO Common.EventQueue - Dequeue: No pending events in the queue 006D8178
4-03-12 13:30:36.512 [Th 0000021C] DEBUG WinAgent.ConnectionReader - handle input: handle =00000464

```

If the **OnGuard Plugin** fails to connect with the **Backend Service** then the **OnGuard Agent** UI will show “Initialilizing...” 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 OnGuardPlugin.BackendClient - Run: Backend connection failed. Will retry after 5 seconds...

```

```

ClearPassOnGuard_0.log (10.7 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI
C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (10.7 KB)
ClearPassOnGuard_0.log winagent_0.log
2014-03-12 14:09:25,777 [Th 5560:5100] INFO OnGuardPlugin.AgentThread - Start: AgentController Thread created successfully.
2014-03-12 14:09:25,777 [Th 5560:5100] DEBUG OnGuardPlugin.AgentController - Start: Controller Thread created
2014-03-12 14:09:25,792 [Th 00001590] INFO OnGuardPlugin.AgentThread - Run: Agent Controller Thread starting
2014-03-12 14:09:26,299 [Th 00001590] INFO OnGuardPlugin.AgentThread - Start: BackendClient Thread created successfully.
2014-03-12 14:09:26,299 [Th 00001590] DEBUG OnGuardPlugin.SocketClient - Start: BackendClient Thread created
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 14:09:32,302 [Th 00001590] DEBUG Common.TextStore - GetFormattedTextFromResource: vsprintf result - 55
2014-03-12 14:09:32,302 [Th 00001590] INFO OnGuardPlugin.AgentController - SendDiagnosticLogMessage: Level - 2 Log Message - Failed to connect to ClearPass
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 OnGuardPlugin.BackendClient - Run: Backend connection failed. Will retry after 5 seconds...
2014-03-12 14:09:34,303 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry
2014-03-12 14:09:36,303 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry
2014-03-12 14:09:38,303 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry
2014-03-12 14:09:38,374 [Th 00000678] INFO OnGuardPlugin.SocketClient - Connect: BackendClient - Connecting to server=127.0.0.1 on port= 25427
2014-03-12 14:09:38,374 [Th 00000678] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect to 127.0.0.1 at port - 25427
2014-03-12 14:09:39,410 [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 14:09:39,410 [Th 00000678] ERROR OnGuardPlugin.SocketClient - Connect: BackendClient - Failed to connect. Returned value = -1
2014-03-12 14:09:39,410 [Th 00000678] ERROR OnGuardPlugin.BackendClient - Run: Backend connection failed. Will retry after 5 seconds...
2014-03-12 14:09:40,303 [Th 00001590] DEBUG OnGuardPlugin.AgentController - Init: Backend not active. Waiting 2 seconds before retry

```


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.MessageRequestDispatcher - 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":[{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"}]},{"id":0,"name":"NetworkInterfaceListResponse"}

2014-03-12 14:24:55,705 [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 = 0

2014-03-12 14:24:55,705 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - Interface List contents size = 1

2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::displayName=Local Area Connection

2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::ifName=Local Area Connection

2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.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
```

```
ClearPassOnGuard_0.log (79.7 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI
C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (79.7 KB)
ClearPassOnGuard_0.log winagent_0.log
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.MessageRequestDispatcher - 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=NetworkInterfaceListRequest
2014-03-12 14:24:55,703 [Th 00001408] DEBUG OnGuardPlugin.ConnectionReader - (AgentConnectionReader::handle_input: handle =00000710
2014-03-12 14:24:55,703 [Th 00001408] DEBUG OnGuardPlugin.Connection - Outer sock->recv() returned 220
2014-03-12 14:24:55,703 [Th 00001408] DEBUG OnGuardPlugin.Connection - Inner sock->recv() returned -1
2014-03-12 14:24:55,704 [Th 00001408] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 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 14:24:55,704 [Th 00001408] INFO OnGuardPlugin.MessageHandler - ProcessMessage: Got 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 14:24:55,704 [Th 00001408] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message = {"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 14:24:55,705 [Th 00001408] DEBUG JsonWrapper.JSONUtils - Key=id is INT
2014-03-12 14:24:55,705 [Th 00001408] DEBUG JsonWrapper.JSONUtils - Inserting Key=id|Value=0
2014-03-12 14:24:55,705 [Th 00001408] DEBUG JsonWrapper.JSONUtils - Key=name is STRING
2014-03-12 14:24:55,705 [Th 00001408] DEBUG JsonWrapper.JSONUtils - Inserting Key=name|Value=NetworkInterfaceListResponse
2014-03-12 14:24:55,705 [Th 00001408] DEBUG JsonWrapper.JSONUtils - Key=content is OBJECT
2014-03-12 14:24:55,705 [Th 00001408] DEBUG OnGuardPlugin.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 = 0
2014-03-12 14:24:55,705 [Th 000013f0] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response over. Response event occurred
2014-03-12 14:24:55,705 [Th 000013f0] DEBUG OnGuardPlugin.MessageRequestDispatcher - RemovePendingResponse: Removing message id - 0
2014-03-12 14:24:55,705 [Th 000013f0] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Response after wait=0385C140
2014-03-12 14:24:55,705 [Th 000013f0] DEBUG OnGuardPlugin.NetworkInterfaceListResponse - In CNetworkInterfaceListResponse::Deserialize()
2014-03-12 14:24:55,705 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - Interface List contents size = 1
2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::displayName=Local Area Connection
2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.NetworkInterfaceListResponse - NetworkInterface::ifName=Local Area Connection
2014-03-12 14:24:55,706 [Th 000013f0] DEBUG JsonWrapper.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
2014-03-12 14:24:55,706 [Th 000013f0] DEBUG OnGuardPlugin.AgentController - Enqueue: Adding action to queue: IF_UP (3)
2014-03-12 14:24:55,707 [Th 000013f0] INFO OnGuardPlugin.ActionQueue - Enqueue: Inserted event 0386F810 type IF_UP (3) into Queue 03865430, QueueSize=2
2014-03-12 14:24:55,712 [Th 000013f0] INFO OnGuardPlugin.ActionQueue - Dequeue: Removed event 03880AF8 type BACKEND_UP (12) from Queue 03865430, QueueSize=1
```

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":"NetworkInterfaceListRequest"}

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

!

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

```

```

winagent_0.log (204.9 KB) - BareTail
File Edit View Preferences Help
C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (204.9 KB)
ClearPassOnGuard_0.log winagent_0.log
DEBUG WinAgent.WinAgentReadEvHandler - Read data = 46:{"id":0,"name":"NetworkInterfaceListRequest"}
DEBUG WinAgent.WinAgentMessageDriver - 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"}
DEBUG JsonWrapper.JSONUtils - Key=id is INT
DEBUG JsonWrapper.JSONUtils - Inserting Key=id|Value=0
DEBUG JsonWrapper.JSONUtils - Key=name is STRING
DEBUG JsonWrapper.JSONUtils - Inserting Key=name|Value=NetworkInterfaceListRequest
DEBUG WinAgent.WinAgentJSONTransformer - Read message name NetworkInterfaceListRequest
DEBUG WinAgent.WinAgentMessageFactory - Inserting messageId=0 into message cache
DEBUG WinAgent.NetworkInterfaceListMessageHandler - Inside NetworkInterfaceListMessageHandler()
INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: {53864050-B59A-4345-99B9-CC2016A7B114} Desc: Microsoft Virtual WiFi Miniport Ad
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 Co
INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Add IfName={4228529A-5C50-4DE6-8B87-7F8B7BBA2F6A} Adapter Index=10 Display Name=Broadcom 440x
INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: {9B8DF315-1000-4597-80B0-4CFC5117FAF5} Desc: VirtualBox Host-Only Ethernet Adap
DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=NetworkInterfaceListRequest
DEBUG WinAgent.WinAgentEventHandler - Encoded message = 215:{"content":{"ifList":[{"displayName":"Local Area Connection","ifName":"Local Area Connection",
DEBUG WinAgent.WinAgentEventHandler - Done sending the data. Size - 220
DEBUG WinAgent.WinAgentMessageFactory - Deleting messageId=0 from message cache
INFO Common.EventProcessor - EventThreadHandler: Processing Event (102) from EventQ 00D08178 finished
EventQueue - Dequeue: No pending events in the queue 00D08178

```

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.

```

```

ClearPassOnGuard_0.log (19.4 KB) - BareTail
File Edit View Preferences Help
Opep Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (19.4 KB)
ClearPassOnGuard_0.log winagent_0.log
2014-03-12 14:37:26,283 [Th 00000ab8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 46:{"id":0,"name":"NetworkInterfaceListRequest"}
2014-03-12 14:37:26,284 [Th 00000ab8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 50 Result - 50
2014-03-12 14:37:26,284 [Th 00000ab8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=NetworkInterfaceListRequest
2014-03-12 14:37:26,295 [Th 0000085c] DEBUG OnGuardPlugin.ConnectionReader - CAgentConnectionReader::handle_input: handle =0000070C
2014-03-12 14:37:26,295 [Th 0000085c] DEBUG OnGuardPlugin.Connection - Outer sock->recv() returned 77
2014-03-12 14:37:26,295 [Th 0000085c] DEBUG OnGuardPlugin.Connection - Inner sock->recv() returned -1
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 14:37:26,295 [Th 0000085c] INFO OnGuardPlugin.MessageHandler - ProcessMessage: Got message=73:{"content":{"iflist":null},"id":0,"name":"NetworkInterfaceListResponse"}
2014-03-12 14:37:26,295 [Th 0000085c] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message = {"content":{"iflist":null},"id":0,"name":"NetworkInterfaceListResponse"}
2014-03-12 14:37:26,296 [Th 0000085c] DEBUG JsonWrapper.JSONUtils - Key=id is INT
2014-03-12 14:37:26,296 [Th 0000085c] DEBUG JsonWrapper.JSONUtils - Inserting Key=id|Value=0
2014-03-12 14:37:26,296 [Th 0000085c] DEBUG JsonWrapper.JSONUtils - Key=name is STRING
2014-03-12 14:37:26,296 [Th 0000085c] DEBUG JsonWrapper.JSONUtils - Inserting Key=name|Value=NetworkInterfaceListResponse
2014-03-12 14:37:26,296 [Th 0000085c] DEBUG JsonWrapper.JSONUtils - Key=content is OBJECT
2014-03-12 14:37:26,296 [Th 0000085c] DEBUG JsonWrapper.AgentJSONTransformer - Read message name NetworkInterfaceListResponse
2014-03-12 14:37:26,296 [Th 0000085c] DEBUG OnGuardPlugin.MessageHandler - ProcessMessage: Network message parsed successfully. Message Name = NetworkInterfaceListResponse
2014-03-12 14:37:26,296 [Th 0000085c] INFO OnGuardPlugin.BackendClientMessageHandler - ProcessResponse: Message Name = NetworkInterfaceListResponse Id = 0
2014-03-12 14:37:26,299 [Th 00000ab8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response over. Response event occurred
2014-03-12 14:37:26,299 [Th 00000ab8] DEBUG OnGuardPlugin.MessageRequestDispatcher - RemovePendingResponse: Removing message id - 0
2014-03-12 14:37:26,299 [Th 00000ab8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Response after wait=0285C140
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.
2014-03-12 14:37:26,299 [Th 00000ab8] INFO OnGuardPlugin.AgentController - SendDiagnosticLogMessage: Level - 2 Log Message - No Active Network Connection
2014-03-12 14:37:26,312 [Th 00000ab8] INFO OnGuardPlugin.ActionQueue - Dequeue: Removed event 02880AF8 type BACKEND_UP (12) from Queue 02865430, QueueSize 12
2014-03-12 14:37:26,312 [Th 00000ab8] DEBUG OnGuardPlugin.AgentController - Run: Removed action from queue: BACKEND_UP (12)
2014-03-12 14:37:26,312 [Th 00000ab8] DEBUG OnGuardPlugin.AgentController - HandleAction: Handling action=BACKEND_UP (12) after a delay of 2.248 seconds
2014-03-12 14:37:26,312 [Th 00000ab8] DEBUG OnGuardPlugin.AgentController - HandleConnectionEstablished: Connection with Backend established
2014-03-12 14:37:26,312 [Th 00000ab8] INFO OnGuardPlugin.AgentController - HandleConnectionEstablished: Number of Managed Interfaces - 0
2014-03-12 14:37:26,313 [Th 00000ab8] DEBUG Common.TextStore - GetFormattedTextFromResource: vsprintf result - 60

```

Backend Service Logs (Empty Network Interface List):

```

2014-03-12 14:37:26,287 [Th 000009ec Evt 04E80928] DEBUG WinAgent.WinAgentReadEvHandler - Read data =
46:{"id":0,"name":"NetworkInterfaceListRequest"}

!

2014-03-12 14:37:26,288 [Th 000009ec Evt 04E80928] DEBUG WinAgent.NetworkInterfaceListMessageHandler - Inside
NetworkInterfaceListMessageHandler()

!

2014-03-12 14:37:26,294 [Th 000009ec Evt 04E80928] DEBUG WinAgent.WinAgentEventHandler - Encoded message =
73:{"content":{"iflist":null},"id":0,"name":"NetworkInterfaceListResponse"}

```

```

winagent_0.log (148.2 KB) - BareTail
File Edit View Preferences Help
C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (148.2 KB)
ClearPassOnGuard_0.log winagent_0.log
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 46:{"id":0,"name":"NetworkInterfaceListRequest"}
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentMessageDriver - Message buffer is empty
000009ec Evt 04E80928] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message = {"id":0,"name":"NetworkInterfaceListRequest"}
000009ec Evt 04E80928] INFO WinAgent.WinAgentMessageDriver - Processing the network message = {"id":0,"name":"NetworkInterfaceListRequest"}
000009ec Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Key=id is INT
000009ec Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Inserting Key=id|Value=0
000009ec Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Key=name is STRING
000009ec Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Inserting Key=name|Value=NetworkInterfaceListRequest
000009ec Evt 04E80928] DEBUG JsonWrapper.JSONUtils - Key=content is NULL
000009ec Evt 04E80928] DEBUG WinAgent.AgentJSONTransformer - Read message name NetworkInterfaceListRequest
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentMessageFactory - Inserting messageId=0 into message cache
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentMessageHandler - Inside NetworkInterfaceListMessageHandler()
000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (63884050-B59A-4346-8B89-CC2016A7B114) Desc: Microsoft V
000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (B553619B-BD80-4F7C-9BAD-4DF6CDBE3F2E) Desc: Dell Wirele
000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (4228529A-5C50-4DE6-8B87-7F8B7BBA2F6A) Desc: Broadcom 44
000009ec Evt 04E80928] INFO Common.NetworkIfHelper - GetNetworkInterfacesWindows: Adapter Name: (9B8DF315-1000-4597-80B0-4CFC5117FAF5) Desc: VirtualBox I
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=NetworkInterfaceListRequest
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 73:{"content":{"ifList":null},"id":0,"name":"NetworkInterfaceListResponse"}
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentEventHandler - Done sending the data. Size = 77
000009ec Evt 04E80928] DEBUG WinAgent.WinAgentMessageFactory - Deleting messageId=0 from message cache
000009ec Evt 04E80928] INFO Common.EventProcessor - EventThreadHandler: Processing Event (102) from Event0_00628178 finished
  
```

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 - UpdateIfInfo: 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 - “<https://<CPPM Server IP Address>/images/index.html>”.

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
!
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: 10.20.23.123 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=10.17.4.234 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
```

```

ClearPassOnGuard_0.log (39.0 KB) - BareTail
File Edit View Preferences Help
Dnsp Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (39.0 KB)
ClearPassOnGuard_0.log winagent_0.log
15:27:43,978 [Th 000014c4] DEBUG OnGuardPlugin.AuthServerQueryComponent - FindAuthServer: Starting Auth server query for interface=Local Area Connection
15:27:43,978 [Th 000014c4] INFO OnGuardPlugin.ThreadGroup - AddThread: Adding thread to map with supplied key - Local Area Connection
15:27:43,979 [Th 000014c4] INFO OnGuardPlugin.ThreadGroup - AddThread: Thread Group Size - 1 Map Size - 1
15:27:43,979 [Th 000014c4] INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.
15:27:43,979 [Th 000012d8] INFO OnGuardPlugin.InterfaceQuery - Execute: Starting Query for - Local Area Connection
15:27:43,979 [Th 000012d8] INFO OnGuardPlugin.ThreadGroup - AddThread: Adding thread with key (id) - 14dc
15:27:43,979 [Th 000012d8] INFO OnGuardPlugin.ThreadGroup - AddThread: Adding thread to map with supplied key - 14dc
15:27:43,979 [Th 000012d8] INFO OnGuardPlugin.ThreadGroup - AddThread: Thread Group Size - 1 Map Size - 1
15:27:43,980 [Th 000014dc] INFO OnGuardPlugin.AuthServerQuery - operator: Executing auth server query thread for - Local Area Connection
15:27:43,980 [Th 000014dc] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950
15:27:43,980 [Th 000014dc] INFO OnGuardPlugin.HttpAuthChannel - SetLocalAddr: New local IP: 10.20.23.123
15:27:43,980 [Th 000014dc] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/
15:27:45,139 [Th 000014dc] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
15:27:45,139 [Th 000014dc] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 214
15:27:45,150 [Th 000014dc] INFO OnGuardPlugin.AuthServerQuery - Execute: Reachability Status for Local Area Connection to server 10.17.4.234 - 1
15:27:45,151 [Th 000012d8] INFO OnGuardPlugin.InterfaceQuery - GetActiveServers: Auth server=10.17.4.234 is active for Local Area Connection
15:27:45,151 [Th 000012d8] INFO OnGuardPlugin.ThreadGroup - RemoveAllThreads: Removing thread from map with key - 14dc
15:27:45,151 [Th 000012d8] INFO OnGuardPlugin.ThreadGroup - RemoveAllThreads: Thread Group Size - 0 Map Size - 0
15:27:45,152 [Th 000012d8] INFO OnGuardPlugin.InterfaceQuery - QueryActiveAuthServers: Active servers for interface Local Area Connection : 10.17.4.234
15:27:45,152 [Th 000012d8] DEBUG OnGuardPlugin.AgentController - Enqueue: Adding action to queue: AUTH_SERVERS (2)
15:27:45,152 [Th 000012d8] INFO OnGuardPlugin.ActionQueue - Enqueue: Inserted event 042A80D0 type AUTH_SERVERS (2) into Queue 04285430, QueueSize=1
15:27:45,153 [Th 000014c4] INFO OnGuardPlugin.ActionQueue - Dequeue: Removed event 042A80D0 type AUTH_SERVERS (2) from Queue 04285430, QueueSize=0

```

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):

```

2014-03-12 15:34:27,499 [Th 000002a0] DEBUG OnGuardPlugin.AuthServerQueryComponent - FindAuthServer: Starting Auth server query for
interface=Local Area Connection 2

!

2014-03-12 15:34:27,501 [Th 00001474] INFO OnGuardPlugin.InterfaceQuery - Execute: Starting Query for - Local Area Connection 2

!

2014-03-12 15:34:27,502 [Th 000015e8] INFO OnGuardPlugin.AuthServerQuery - operator: Executing auth server query thread for - Local Area Connection 2

2014-03-12 15:34:27,502 [Th 000015e8] INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950

2014-03-12 15:34:27,502 [Th 000015e8] INFO OnGuardPlugin.HttpAuthChannel - SetLocalAddr: New local IP: 192.168.1.10

2014-03-12 15:34:27,502 [Th 000015e8] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 192.168.1.10 Remote IP: 10.17.4.234, url:
https://10.17.4.234/images/index.html

2014-03-12 15:34:27,503 [Th 000015e8] ERROR OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Send Request failed from Local IP:
192.168.1.10 to Remote IP: 10.17.4.234. Error - 7(Couldn't connect to server)

2014-03-12 15:34:27,504 [Th 000015e8] ERROR OnGuardPlugin.HttpClientWrapper - DoSubmit: ExecuteMethod failed for Local IP: 192.168.1.10 Remote
IP: 10.17.4.234.

2014-03-12 15:34:27,504 [Th 000015e8] ERROR OnGuardPlugin.HttpAuthChannel - IsAuthServerReachable: Echo to 10.17.4.234 failed from Local IP:
192.168.1.10.

2014-03-12 15:34:27,514 [Th 000015e8] INFO OnGuardPlugin.AuthServerQuery - Execute: Reachability Status for Local Area Connection 2 to server
10.17.4.234 - 0

2014-03-12 15:34:27,515 [Th 00001474] WARN OnGuardPlugin.InterfaceQuery - GetActiveServers: Auth server=10.17.4.234 is not active/available on
interface Local Area Connection 2

2014-03-12 15:34:27,515 [Th 00001474] INFO OnGuardPlugin.InterfaceQuery - QueryActiveAuthServers: Active servers for interface Local Area
Connection 2 :

```

```

ClearPassOnGuard_0.log (47.1 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (47.1 KB)
ClearPassOnGuard_0.log winagent_0.log
DEBUG OnGuardPlugin.AuthServerQueryComponent - FindAuthServer: Starting Auth server query for interface=Local Area Connection 2
INFO OnGuardPlugin.ThreadGroup - AddThread: Adding thread to map with supplied key - Local Area Connection 2
INFO OnGuardPlugin.ThreadGroup - AddThread: Thread Group Size - 1 Map Size - 1
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.
INFO OnGuardPlugin.InterfaceQuery - Execute: Starting Query for - Local Area Connection 2
INFO OnGuardPlugin.ThreadGroup - AddThread: Adding thread with key (id) - 15e8
INFO OnGuardPlugin.ThreadGroup - AddThread: Adding thread to map with supplied key - 15e8
INFO OnGuardPlugin.ThreadGroup - AddThread: Thread Group Size - 1 Map Size - 1
INFO OnGuardPlugin.AuthServerQuery - operator: Executing auth server query thread for - Local Area Connection 2
INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950
INFO OnGuardPlugin.HttpAuthChannel - SetLocalAddr: New local IP: 192.168.1.10
INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 192.168.1.10 Remote IP: 10.17.4.234, url: https://10.17.4.234/images/index.html
ERROR OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Send Request failed from Local IP: 192.168.1.10 to Remote IP: 10.17.4.234. Error - 7(Couldn't
ERROR OnGuardPlugin.HttpClientWrapper - DoSubmit: ExecuteMethod failed for Local IP: 192.168.1.10 Remote IP: 10.17.4.234.
ERROR OnGuardPlugin.HttpAuthChannel - IsAuthServerReachable: Echo to 10.17.4.234 failed from Local IP: 192.168.1.10.
INFO OnGuardPlugin.AuthServerQuery - Execute: Reachability Status for Local Area Connection 2 to server 10.17.4.234 - 0
WARN OnGuardPlugin.InterfaceQuery - GetActiveServers: Auth server=10.17.4.234 is not active/available on interface Local Area Connection 2
INFO OnGuardPlugin.ThreadGroup - RemoveAllThreads: Removing thread from map with key - 15e8
INFO OnGuardPlugin.ThreadGroup - RemoveAllThreads: Thread Group Size - 0 Map Size - 0
INFO OnGuardPlugin.InterfaceQuery - QueryActiveAuthServers: Active servers for interface Local Area Connection 2 :
DEBUG OnGuardPlugin.AgentController - Enqueue: Adding action to queue: AUTH_SERVERS (2)
INFO OnGuardPlugin.ActionQueue - Enqueue: Inserted event 041D80E0 type AUTH_SERVERS (2) into Queue 041B5430, QueueSize=1
INFO OnGuardPlugin.InterfaceQuery - Execute: Finished Query for - Local Area Connection 2
INFO OnGuardPlugin.ActionQueue - Dequeue: Removed event 041D80E0 type AUTH_SERVERS (2) from Queue 041B5430, QueueSize=0
DEBUG OnGuardPlugin.AgentController - Run: Removed action from queue: AUTH_SERVERS (2)
DEBUG OnGuardPlugin.AgentController - HandleAction: Handling action=AUTH_SERVERS (2) after a delay of 0.0 seconds
DEBUG OnGuardPlugin.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Connection 2
INFO OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection 2 Managed state: UNKNOWN_STATE
DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: No auth servers active for Local Area Connection 2
INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: No auth server for this interface Local Area Connection 2
DEBUG Common.TextStore - GetFormattedTextFromResource: vsprintf result - 59

```


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 '[ClearPass OnGuard in a Cluster](#)' 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","nodeIp":["10.17.4.234"],"formType":"authApplet","CacheCredentialsForDays":"15","passwordLabel":"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
```


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", "passwordLabel": "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 - 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

```

ClearPassOnGuard_0.log (349.5 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Local\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (349.5 KB)
ClearPassOnGuard_0.log winagent_0.log
2014-03-12 15:51:40,774 [Th 000009e8] DEBUG OnGuardPlugin.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Co
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 - 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:
2014-03-12 15:51:40,775 [Th 00001248] INFO OnGuardPlugin.ThreadGroup - Execute: Finished Query for - Local Area Connection
2014-03-12 15:51:40,785 [Th 00001248] INFO OnGuardPlugin.ThreadGroup - RemoveThread: Removed thread from map with supplied key - Local Area Connection
2014-03-12 15:51:40,785 [Th 00001248] INFO OnGuardPlugin.ThreadGroup - RemoveThread: Thread Group Size - 0 Map Size - 0
2014-03-12 15:51:40,785 [Th 00001248] DEBUG OnGuardPlugin.AuthServerQueryComponent - RemovePendingInterface: Removing interface=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] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 359
2014-03-12 15:51:40,792 [Th 000009e8] INFO OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = {"InstallVPNComponent": "false", "field
2014-03-12 15:51:40,792 [Th 000009e8] DEBUG OnGuardPlugin.AgentAppHttpClient - UpdateGlobalAgentSettings: Domain servers: Non-domain servers: 10.17.4.
2014-03-12 15:51:40,795 [Th 000009e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=UpdateAgentConfRequ
2014-03-12 15:51:40,804 [Th 000009e8] DEBUG OnGuardPlugin.BackendClientInfoCollector - UpdateAgentConf: Update Agent Conf Response Status = 1
2014-03-12 15:51:40,804 [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
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 pi
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:
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] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 359
2014-03-12 15:51:40,824 [Th 000009e8] INFO OnGuardPlugin.AgentAppHttpClient - FetchAgentSettings: Parsing JSON = {"InstallVPNComponent": "false", "field
2014-03-12 15:51:40,824 [Th 000009e8] DEBUG OnGuardPlugin.AgentAppHttpClient - UpdateGlobalAgentSettings: Domain servers: Non-domain servers: 10.17.4.
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
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
2014-03-12 15:51:40,838 [Th 000009e8] INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Conne
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 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", "upgradeAction": "DoNothing", "nodes": { "India": ["10.17.4.234"] }, "interfaces": "wired,wireless,vpn", "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", "nodeIp": ["10.17.4.234"], "formType": "authApplet", "CacheCredentialsForDays": "15", "passwordLabel": "Password", "mode": "both", "upgradeAction": "DoNothing", "nodes": { "India": ["10.17.4.234"] }, "interfaces": "wireless,vpn", "domain": "default", "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 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

```

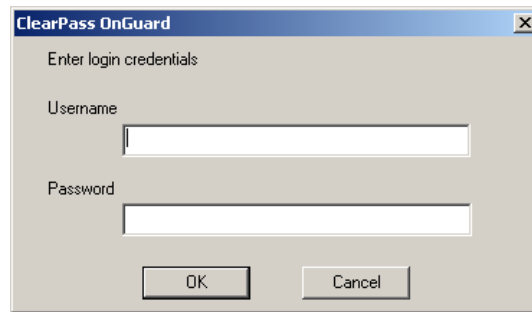
ClearPassOnGuard_0.log (47.4 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (47.4 KB)
ClearPassOnGuard_0.log winagent_0.log
DEBUG OnGuardPlugin.AgentController - HandleAuthServers: Updating authentication servers active for Local Area Connection
INFO OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection Managed state: UNKNOWN_STATE
INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950
INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950
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 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.WebHttpClient - CWebHttpClient: URL=10.17.4.234
INFO OnGuardPlugin.HttpClientWrapper - CHttpClientWrapper: UserAgent - OnGuard 6.3.1.61950
INFO OnGuardPlugin.InterfaceManager - PickAuthServer: Local Area Connection not an allowed type: WIRED
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,"name":
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 101 Result - 101
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendRequest: No response expected for message: AuthServerReachable
DEBUG Common.TextStore - GetFormattedTextFromResource: vsprintf result - 55
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue 042C5430
INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= AUTH_SERVER_DISCOVERY (1) (Seconds in this state=5) for Local Area Connection
DEBUG OnGuardPlugin.InterfaceManager - HandleNoOp: Not time for another auth server discovery run Local Area Connection
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue 042C5430
INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= AUTH_SERVER_DISCOVERY (1) (Seconds in this state=11) for Local Area Connection
DEBUG OnGuardPlugin.InterfaceManager - HandleNoOp: Not time for another auth server discovery run Local Area Connection
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue 042C5430
INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state= AUTH_SERVER_DISCOVERY (1) (Seconds in this state=16) for Local Area Connection
DEBUG OnGuardPlugin.InterfaceManager - HandleNoOp: Not time for another auth server discovery run Local Area Connection
INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.

```

Wait For Credentials

In WAIT_FOR_CREDENTIALS state, the **OnGuard Agent** waits until it get credentials (username/password) to proceed further. The credentials **OnGuard Agents** 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.



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

2. 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 - 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 check
```

2014-03-12 18:08:12,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Encoded message = 43:{"id":8,"name":"CollectHealthDataRequest"}

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=CollectHealthDataRequest Timeout value (ms) - 1200000

```

ClearPassOnGuard_0.log (90.2 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (90.2 KB)
ClearPassOnGuard_0.log winagent_0.log
12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection
12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_SERVER_DISCOVERY (1) to WAIT_FOR_CREDENTIALS (2) after 1 seconds
12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - DoWaitForAuthCredentials: Only health checks required for Local Area Connection
12,814 [Th 000008f4] INFO OnGuardPlugin.InterfaceManager - GetNetworkInterfaceList: Network interfaces list size for Local Area Connection : 1
12,817 [Th 000008f4] DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: IsHealthCheckQuietPeriodEnabled() returned false for Local Area Connection
12,835 [Th 000008f4] DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: Possible cause - InterfaceType==VPN | Mode!=HealthOnly | HealthCheckQuiet
12,837 [Th 000008f4] DEBUG OnGuardPlugin.AuthSession - Authenticate: Not In HealthCheckQuietPeriod. Performing full Auth with health check
12,837 [Th 000008f4] DEBUG Common.TextStore - GetFormattedTextFromResource: vsprintf result - 61
12,837 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - AddPendingResponse: Adding message id - 8
12,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Encoded message = 43:{"id":8,"name":"CollectHealthDataRequest"}
12,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 47 Result - 47
12,838 [Th 000008f4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value
43,132 [Th 000012d8] DEBUG OnGuardPlugin.ConnectionReader - CAgentConnectionReader::handle_input: handle =00000708
43,132 [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: Moving from WAIT_FOR_CREDENTIALS (2) to 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: Using auth server= 10.17.4.234 for Local Area 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

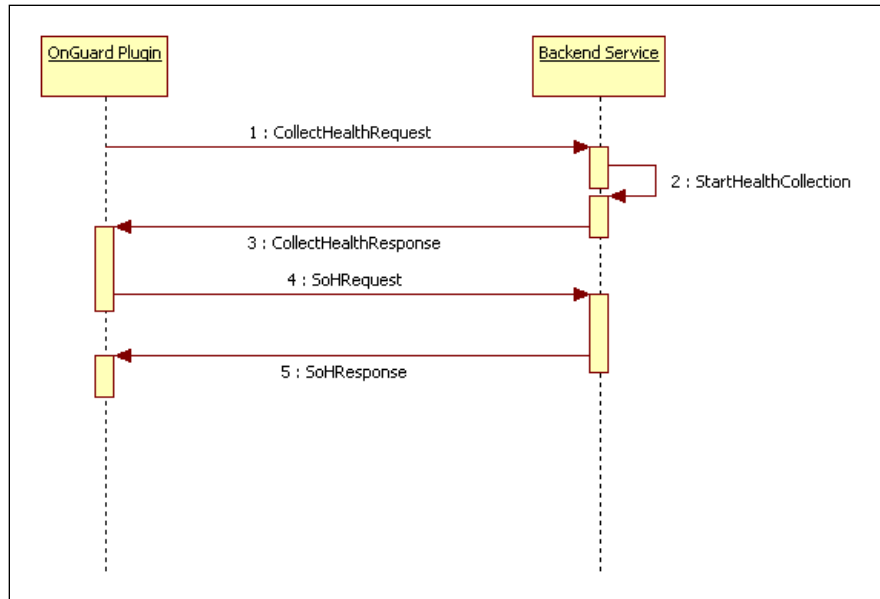
2014-03-12 17:58:05,570 [Th 00000f68] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000

```

ClearPassOnGuard_0.log (110.7 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Despak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (110.7 KB)
ClearPassOnGuard_0.log winagent_0.log
INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection
INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_SERVER_DISCOVERY (1) to WAIT_FOR_CREDENTIALS (2) after 1 seconds
INFO OnGuardPlugin.InterfaceManager - DoWaitForAuthCredentials: Need user action to proceed for Local Area Connection
INFO OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Connection Username=dj
DEBUG OnGuardPlugin.AgentController - Enqueue: Adding action to queue: USER_CREDENTIALS (1)
DEBUG OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Local Area Connection
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 OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
INFO OnGuardPlugin.InterfaceManager - DoAuthServerDiscovery: Using auth server= 10.17.4.234 for Local Area Connection
INFO OnGuardPlugin.InterfaceManager - GetNetworkInterfaceList: Network interfaces list size for Local Area Connection : 1
DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: IsHealthCheckQuietPeriodEnabled() returned false for Local Area Connection
DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: Possible cause - InterfaceType==VPN | Mode!=HealthOnly | HealthCheckQuietPeriod == 0
DEBUG OnGuardPlugin.AuthSession - Authenticate: Not In HealthCheckQuietPeriod. Performing full Auth with health check
DEBUG OnGuardPlugin.MessageRequestDispatcher - AddPendingResponse: 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
  
```

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:



Note – 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):

```

2014-03-13 12:09:03,373 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =
43:{"id":8,"name":"CollectHealthDataRequest"}

2014-03-13 12:09:03,374 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request=CollectHealthDataRequest Timeout value (ms) - 1200000

2014-03-13 12:09:18,033 [Th 00000c60] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
70:{"content":{"status":true},"id":8,"name":"CollectHealthDataResponse"}

2014-03-13 12:09:18,033 [Th 00000c60] INFO OnGuardPlugin.MessageHandler - ProcessMessage: Got
message=70:{"content":{"status":true},"id":8,"name":"CollectHealthDataResponse"}

2014-03-13 12:09:18,034 [Th 00000c60] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message =
{"content":{"status":true},"id":8,"name":"CollectHealthDataResponse"}

!

2014-03-13 12:09:18,036 [Th 00000ee4] DEBUG OnGuardPlugin.BackendClientInfoCollector - CollectHealthData: Collect Health Data Response Status =1

2014-03-13 12:09:18,037 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =
30:{"id":10,"name":"SoHRequest"}
  
```

```

2014-03-13 12:09:18,037 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 34 Result - 34

2014-03-13 12:09:18,037 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=SoHRequest
Timeout value (ms) - 180000

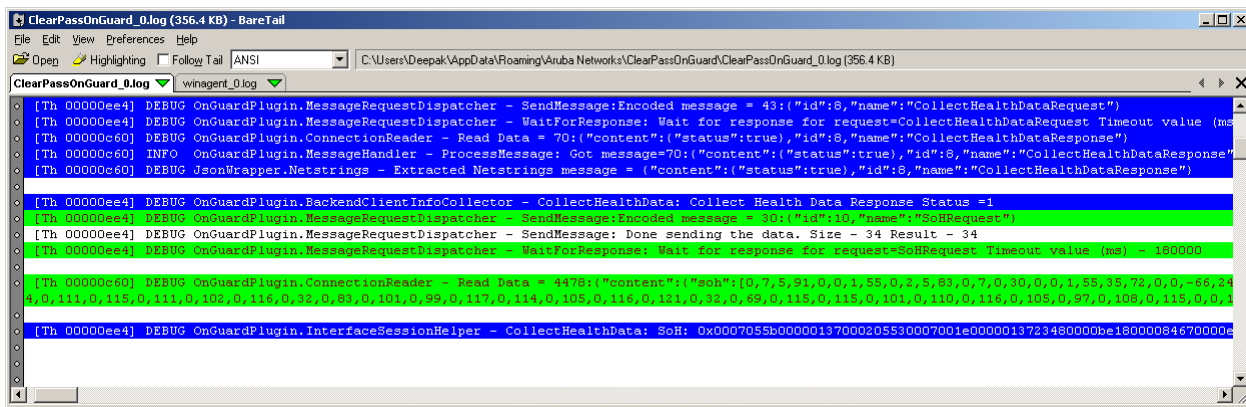
!

2014-03-13 12:09:18,050 [Th 00000c60] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 4478:{"content":{"soh":["0,7,5,91,0,0,1,55,0,2,.....,-128,0,4,2,0]","id":10,"name":"SoHResponse"}}

!

2014-03-13 12:09:18,099 [Th 00000ee4] DEBUG OnGuardPlugin.InterfaceSessionHelper - CollectHealthData: SoH:
0x0007055b.....0700080001378000040200

```



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":"CollectHealthDataRequest"}

!

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)

!

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.

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**

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=CollectHealthDataRequest

2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 70:{"content":{"status":true,"id":8,"name":"CollectHealthDataResponse"}

2014-03-13 12:09:18,038 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 30:{"id":10,"name":"SoHRequest"}

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":"SoHResponse"}

```

2014-03-13 12:09:03,392 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 43:{"id":8,"name":"CollectHealthDataRequest"}
.
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 12:09:06,376 [Th 000001A4] DEBUG WinSHA.VMHealthClassInfoFactory - GetGuestVMList: Number of Guest Virtual Machines found - 2
2014-03-13 12:09:06,444 [Th 000001A4] 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
.
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)
.
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.
.
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
.
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=CollectHealthDataRequest
2014-03-13 12:09:17,999 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 70:{"content":{"status":true,"id":8,"name":"CollectHealthDataResponse"}
.
2014-03-13 12:09:18,038 [Th 00000344 Evt 04D7EE60] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 30:{"id":10,"name":"SoHRequest"}
.
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":"SoHResponse"}

```

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
```

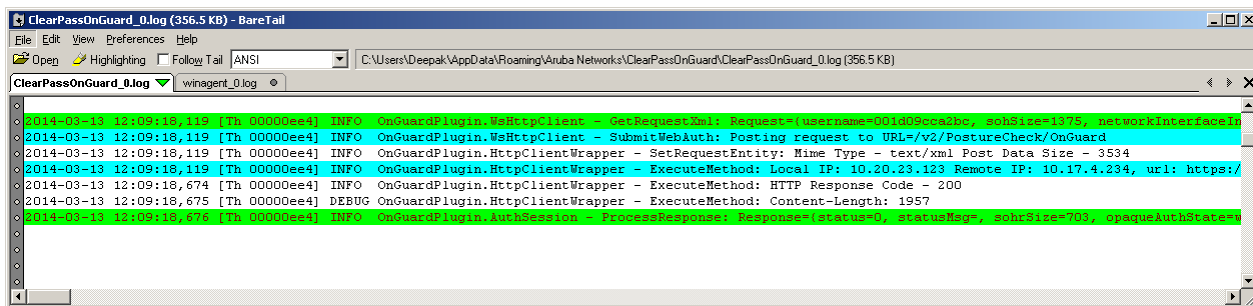
```
2014-03-13 12:09:18,119 [Th 00000ee4] INFO OnGuardPlugin.HttpClientWrapper - SetRequestEntity: Mime Type - text/xml Post Data Size - 3534
```

```
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
```

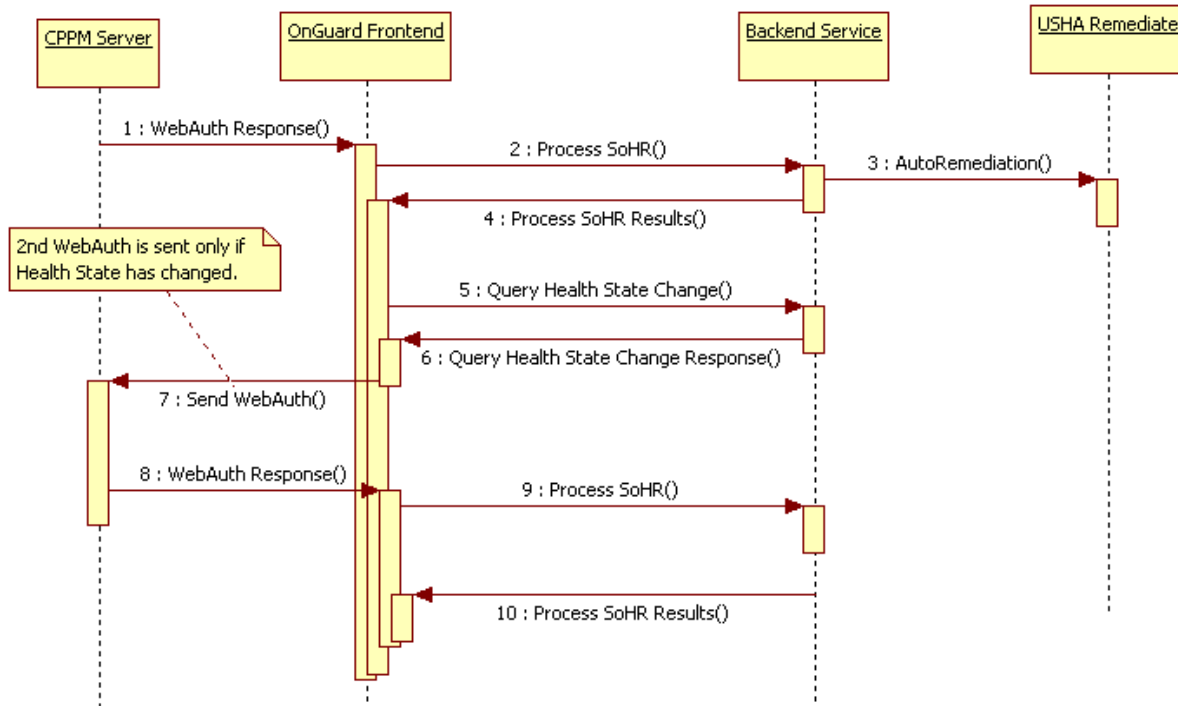
```
2014-03-13 12:09:18,675 [Th 00000ee4] DEBUG OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Content-Length: 1957
```

```
2014-03-13 12:09:18,676 [Th 00000ee4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response={status=0, statusMsg=, sohrSize=703,
opaqueAuthState=wcy1DvZOW8g3h3VKkkyUkg+XB5CeT5CVZzdQPpz3bXgcs3EVeU0VrPIdJKOCzrBT3yZnG3hTNcxXHLIbh5oa0AgpRGYgt9OvfP3QLJEuVQA=,
attributes=[{N=BounceClient V=false}, {N=HealthCheckQuietPeriod V=0}, {N=Message V=Test}, ]}
```

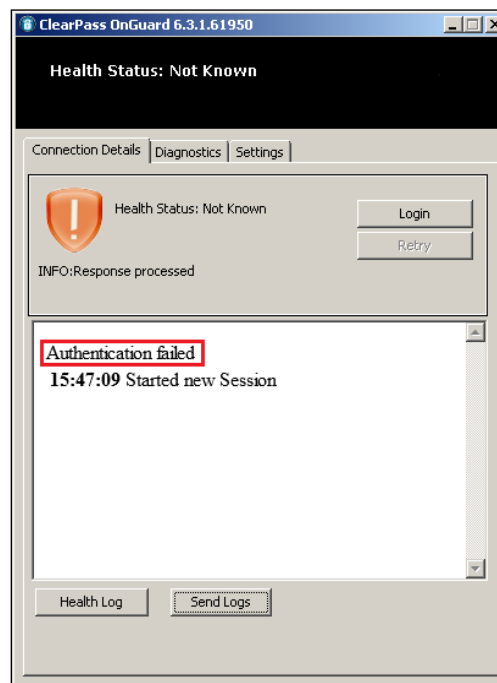


Process WebAuth Response

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

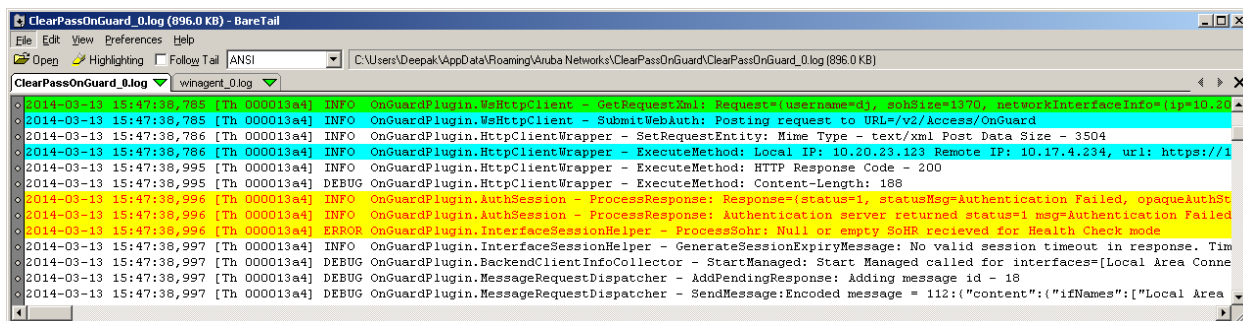
2014-03-13 15:47:38,995 [Th 000013a4] INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200

2014-03-13 15:47:38,996 [Th 000013a4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response={status=1, statusMsg=Authentication Failed,
opaqueAuthState=, attributes=[]}

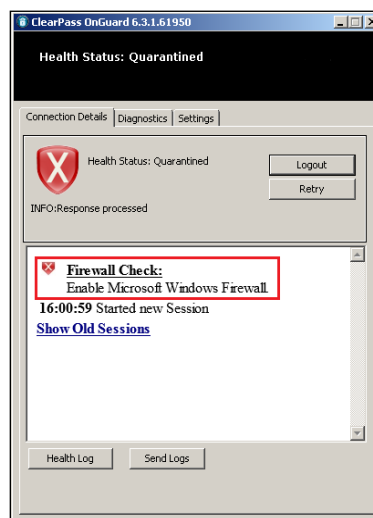
2014-03-13 15:47:38,996 [Th 000013a4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Authentication server returned status=1
msg=Authentication Failed

2014-03-13 15:47:38,996 [Th 000013a4] ERROR OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Null or empty SoHR recieved for Health Check mode

```



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.



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):

```

2014-03-13 12:09:18,676 [Th 00000ee4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response={status=0, statusMsg=, sohrSize=703,
opaqueAuthState=wcy1DvZOW8g3h3VKklyUkg+XB5.....HLlBh5oa0AgpRGYgt9OvfP3QLJEUvQA=, 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: en SoHR:
0x000702bb.....824adff010e044d3b

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":"ProcessSoHRRequest"}}

2014-03-13 12:09:18,680 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request=ProcessSoHRRequest Timeout value (ms) - 300000

!

2014-03-13 12:09:21,725 [Th 00000c60] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
419:{"content":{"healthStatus":false,"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: Healthy - 0
Success - 1

2014-03-13 12:09:21,728 [Th 00000ee4] INFO OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Health response= Success=True Healthy=False
Remediation URL= Msg: Firewall Check:
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: 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
=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] DEBUG OnGuardPlugin.AuthSession - Authenticate: Local Area Connection is Unhealthy.

```

```

ClearPassOnGuard_0.log (347.7 KB) - BareTail
File Edit View Preferences Help
DOpen Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (347.7 KB)
ClearPassOnGuard_0.log winagent_0.log
2014-03-13 12:09:18,678 [Th 00000ee4] INFO OnGuardPlugin.AuthSession - ProcessResponse: Response={status=0, statusMsg:, sohrSize=703, opaqueAuthState=wey
2014-03-13 12:09:18,677 [Th 00000ee4] DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSoHr: Language: en SoHR: 0x000702bb00000137000002b30007001e00000
2014-03-13 12:09:18,679 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 2519:{"content":{"language":"en","remediate":true,"sohr":{"id":18,"name":"ProcessSoHRRRequest"}
2014-03-13 12:09:18,680 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=ProcessSoHRRRequest Tim
.
2014-03-13 12:09:21,725 [Th 00000ee60] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 419:{"content":{"healthStatus":false,"messages":[]},[10,0,70,0,
.
2014-03-13 12:09:21,727 [Th 00000ee4] DEBUG OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: Healthy - 0 Success -
2014-03-13 12:09:21,728 [Th 00000ee4] INFO OnGuardPlugin.InterfaceSessionHelper - ProcessSoHr: Health response: Success=True Healthy=False Remediation URL
Firewall Check: 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: HealthCheckQuietPeriod=0
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] INFO OnGuardPlugin.InterfaceSessionHelper - GenerateSessionExpiryMessage: No valid session timeout in response. Time
2014-03-13 12:09:21,729 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - AddPendingResponse: Adding message id - 16
2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 49:{"id":16,"name":"QueryHealthStateChang
2014-03-13 12:09:21,730 [Th 00000ee4] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=QueryHealthStateChange
.
2014-03-13 12:09:22,356 [Th 00000ee60] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 77:{"content":{"status":false},"id":16,"name":"QueryHealthStateCh
.
2014-03-13 12:09:22,358 [Th 00000ee4] DEBUG OnGuardPlugin.BackendClientInfoCollector - IsHealthStateChanged: QueryHealthStateChange Response =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] DEBUG 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":{"id":18,"name":"ProcessSoHRRRequest"}
1,1,14,4,77,59}},{"id":18,"name":"ProcessSoHRRRequest"}

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|Remediation flag
from ProcessSoHR = 1|Remediation URL =

2014-03-13 16:05:27,172 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing ClearPass Windows Universal
System compressed SoHR

2014-03-13 16:05:27,185 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is
Not_Healthy. Global Remediate Flag - 0

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 - Processing
failed.

2014-03-13 16:05:27,196 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message=Firewall Check:
2014-03-13 16:05:27,196 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message=Enable Microsoft Windows
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":{"healthStatus":false,"messages":[]},[10,0,70,0,....46,0,13,0]],"remediationURL":"","status":true},"id":18,"name":"ProcessSoHRRResponse"}

2014-03-13 16:05:27,216 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentReadEvHandler - Read data =
49:{"id":20,"name":"QueryHealthStateChangeRequest"}

```

```

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.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"}

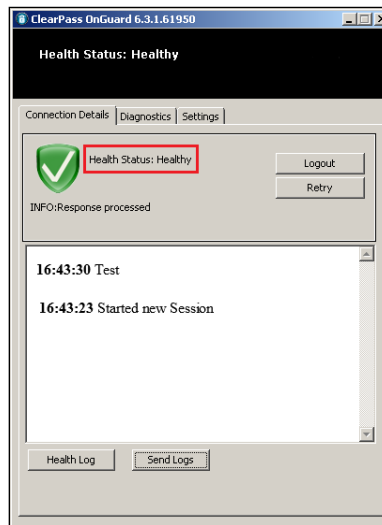
```

```

winagent_0.log (250.2 KB) - BareTail
File Edit View Preferences Help
ClearPassOnGuard_0.log winagent_0.log
2014-03-13 16:05:25,477 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 2519:{"content":{"language":"en","remediate":true,"soh
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|Remediation flag from ProcessSoHR
2014-03-13 16:05:25,497 [Th 00000d38 Evt 04F64030] INFO WinAgent.WinAgentHealthProcessor - ProcessHealthResponse: Remediate Flag - 0
2014-03-13 16:05:27,172 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing ClearPass Windows Universal System compress
2014-03-13 16:05:27,185 [Th 0000019C] INFO WinSHA.SysInfoHealthClassInfoFactory - ProcessHealthResponse: Status of SystemInfo Health Class is Healthy
2014-03-13 16:05:27,185 [Th 0000019C] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Processing Health Class - 0 response succeeded.
2014-03-13 16:05:27,185 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_Healthy. Global
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 Applica
2014-03-13 16:05:27,187 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - GetEnableNotificationAttrValue: Value of EnableNotification attribute of Appli
2014-03-13 16:05:27,187 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Reply from Server contains FirewallUpdateStatus attribute
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 - Processing failed.
2014-03-13 16:05:27,195 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing health response done. Quarantine msg=
2014-03-13 16:05:27,196 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message=
Firewall Check:2014-03-13 16:05:27,196 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message=Enable Microsoft Windows
2014-03-13 16:05:27,197 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=ProcessSoHRRequest
2014-03-13 16:05:27,198 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 419:{"content":{"healthStatus":false,"messages":[
2014-03-13 16:05:27,216 [Th 00000d38 Evt 04F64030] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 49:{"id":20,"name":"QueryHealthStateChangeRequest"}
2014-03-13 16:05:27,217 [Th 00000d38 Evt 04F64030] INFO JavaAgent.WinHealthDataCollector - isHealthStateChanged: Start collecting health info
2014-03-13 16:05:27,217 [Th 00000d38 Evt 04F64030] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Started collecting Health of the Client
2014-03-13 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 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.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":"Qu

```

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=wcy1DvZO.....U9YU8Bk0jrHQ, attributes=[]}

2014-03-13 16:47:54,044 [Th 00001004] DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Language: en SoHR:
0x000701a8000001370002.....8f881c3cbbbed6aba13ed02efafa37f21867fc

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,-96,0.....46,-6,-6,55,-14,24,103,-
4},"id":18,"name":"ProcessSoHRRequest"}}

2014-03-13 16:47:54,045 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request=ProcessSoHRRequest Timeout value (ms) - 300000

2014-03-13 16:47:56,484 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
493:{"content":{"healthStatus":false,"messages":[null,[10,0,70,0,105,0,1.....11,0,110,0,46,0,13,0]],"remediationURL":"","status":true},"id":18,"name":"Pr
ocessSoHRResponse"}

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 Healthy=False
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":"QueryHealthStateChangeRequest"}

2014-03-13 16:47:56,488 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request=QueryHealthStateChangeRequest Timeout value (ms) - 180000

2014-03-13 16:47:56,653 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
76:{"content":{"status":true},"id":20,"name":"QueryHealthStateChangeResponse"}

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=CollectHealthDataRequest Timeout value (ms) - 1200000

2014-03-13 16:47:56,701 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
71:{"content":{"status":true},"id":22,"name":"CollectHealthDataResponse"}

2014-03-13 16:47:56,703 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message =
30:{"id":24,"name":"SoHRequest"}

2014-03-13 16:47:56,703 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=SoHRequest
Timeout value (ms) - 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":24,"name":"SoHResponse"}

!

2014-03-13 16:47:56,725 [Th 00001004] DEBUG OnGuardPlugin.AuthSession - SubmitWebAuthRequest: Authenticating user dj. Retry count=0

!

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://10.17.4.234/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=wcy1DvZOW.....ZU9YU8Bk0}rHQ, attributes=[{N=BounceClient V=false}, {N=HealthCheckQuietPeriod V=0}, {N=Message V=Test}, {}]

2014-03-13 16:47:56,931 [Th 00001004] DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSohr: Language: en SoHR:
0x00070195000001370002018d.....23e01618d606a

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":28,"name":"ProcessSoHRequest"}

2014-03-13 16:47:56,933 [Th 00001004] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request=ProcessSoHRequest Timeout value (ms) - 300000

2014-03-13 16:47:58,546 [Th 0000107c] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
123:{"content":{"healthStatus":true,"messages":[null],"remediationURL":"","status":true},"id":28,"name":"ProcessSoHResponse"}

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

```

[illegible]

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.....6,-6,6,55,-14,24,103,-4]},{"id":18,"name":"ProcessSoHRRRequest"}}

2014-03-13 16:47:55,603 [Th 0000019C] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing ClearPass Windows Universal System compressed SoHR

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

2014-03-13 16:47:55,612 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: 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**

2014-03-13 16:47:56,469 [Th 0000019C] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: **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 application.

2014-03-13 16:47:56,475 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=ProcessSoHRRequest

2014-03-13 16:47:56,475 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 493:{"content":{"healthStatus":false,"messages":[null,[10,0,70,0,.....0,110,0,46,0,13,0]],"remediationURL":"","status":true},"id":18,"name":"ProcessSoHRRResponse"}

```

2014-03-13 16:47:56,494 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data =
49:{"id":20,"name":"QueryHealthStateChangeRequest"}

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=QueryHealthStateChangeRequest

2014-03-13 16:47:56,650 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message =
76:{"content":{"status":true},"id":20,"name":"QueryHealthStateChangeResponse"}

2014-03-13 16:47:56,662 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data =
44:{"id":22,"name":"CollectHealthDataRequest"}

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=CollectHealthDataRequest

2014-03-13 16:47:56,692 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message =
71:{"content":{"status":true},"id":22,"name":"CollectHealthDataResponse"}

2014-03-13 16:47:56,704 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 30:{"id":24,"name":"SoHRequest"}

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":{"soh":{"0,7,3,65,0,0,1,55,0,,,,,,,,,,,,,8,0,1,55,-128,0,4,2,0}},"id":24,"name":"SoHResponse"}

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":"ProcessSoHRequest"}

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

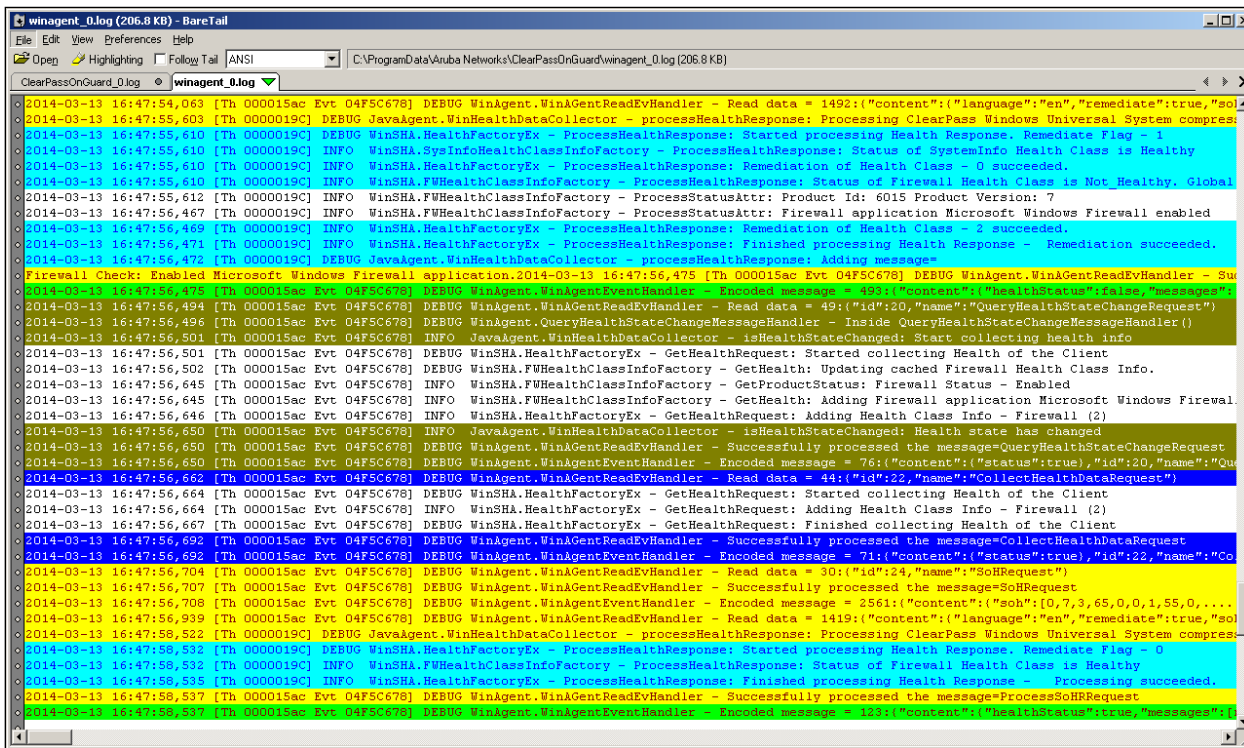
2014-03-13 16:47:58,532 [Th 0000019C] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Healthy

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=ProcessSoHRequest

2014-03-13 16:47:58,537 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message =
123:{"content":{"healthStatus":true,"messages":[null],"remediationURL":"","status":true},"id":28,"name":"ProcessSoHResponse"}

```



```
winagent_0.log (206.8 KB) - Notepad
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (206.8 KB)
ClearPassOnGuard_0.log winagent_0.log
2014-03-13 16:47:54,063 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 1492:{"content":{"language":"en","remediate":true,"so...
2014-03-13 16:47:55,603 [Th 0000019c] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing ClearPass Windows Universal System compres...
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.SysInfoHealthClassInfoFactory - ProcessHealthResponse: Status of SystemInfo Health Class is Healthy
2014-03-13 16:47:55,610 [Th 0000019c] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Remediation of Health Class - 0 succeeded.
2014-03-13 16:47:55,610 [Th 0000019c] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not Healthy. Global
2014-03-13 16:47:55,612 [Th 0000019c] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Product Id: 6015 Product Version: 7
2014-03-13 16:47:55,647 [Th 0000019c] INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Firewall application Microsoft Windows Firewall enabled
2014-03-13 16:47:55,649 [Th 0000019c] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Remediation of Health Class - 2 succeeded.
2014-03-13 16:47:55,671 [Th 0000019c] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - Remediation succeeded.
2014-03-13 16:47:55,672 [Th 0000019c] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Adding message-
Firewall Check: Enabled Microsoft Windows Firewall application.2014-03-13 16:47:55,675 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Su...
2014-03-13 16:47:55,675 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 43:{"content":{"healthStatus":false,"messages":1...
2014-03-13 16:47:55,694 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 49:{"id":20,"name":"QueryHealthStateChangeRequest"}
2014-03-13 16:47:55,696 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.QueryHealthStateChangeMessageHandler - Inside QueryHealthStateChangeMessageHandler()
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO JavaAgent.WinHealthDataCollector - isHealthStateChanged: Start collecting health info
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Started collecting Health of the Client
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.FWHealthClassInfoFactory - GetHealth: Updating cached Firewall Health Class Info.
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO WinSHA.FWHealthClassInfoFactory - GetProductStatus: Firewall Status - Enabled
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO WinSHA.FWHealthClassInfoFactory - GetHealth: Adding Firewall application Microsoft Windows Firewall.
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO WinSHA.FWHealthClassInfoFactory - GetHealth: Adding Health Class Info - Firewall (2)
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO JavaAgent.WinHealthDataCollector - isHealthStateChanged: Health state has changed
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=QueryHealthStateChangeRequest
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 76:{"content":{"status":true,"id":20,"name":"Qu...
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 44:{"id":22,"name":"CollectHealthDataRequest"}
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Started collecting Health of the Client
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO WinSHA.HealthFactoryEx - GetHealthRequest: Adding Health Class Info - Firewall (2)
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - GetHealthRequest: Finished collecting Health of the Client
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=CollectHealthDataRequest
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 71:{"content":{"status":true,"id":22,"name":"Co...
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 30:{"id":24,"name":"SoHRequest"}
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=SoHRequest
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 2561:{"content":{"soh":["0,7,3,65,0,0,1,55,0,...
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 1419:{"content":{"language":"en","remediate":true,"so...
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG JavaAgent.WinHealthDataCollector - processHealthResponse: Processing ClearPass Windows Universal System compres...
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinSHA.HealthFactoryEx - ProcessHealthResponse: Started processing Health Response. Remediate Flag - 0
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Healthy
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] INFO WinSHA.HealthFactoryEx - ProcessHealthResponse: Finished processing Health Response - Processing succeeded.
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=ProcessSoHRequest
2014-03-13 16:47:55,697 [Th 000015ac Evt 04F5C678] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 123:{"content":{"healthStatus":true,"messages":1}}
```

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":"BounceInterfaceRequest"}

2014-03-17 11:57:51,199 [Th 00000e14] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=BounceInterfaceRequest Timeout value (ms) - 180000

!

2014-03-17 11:57:51,646 [Th 000005cc] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"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":"BounceInterfaceResponse"}

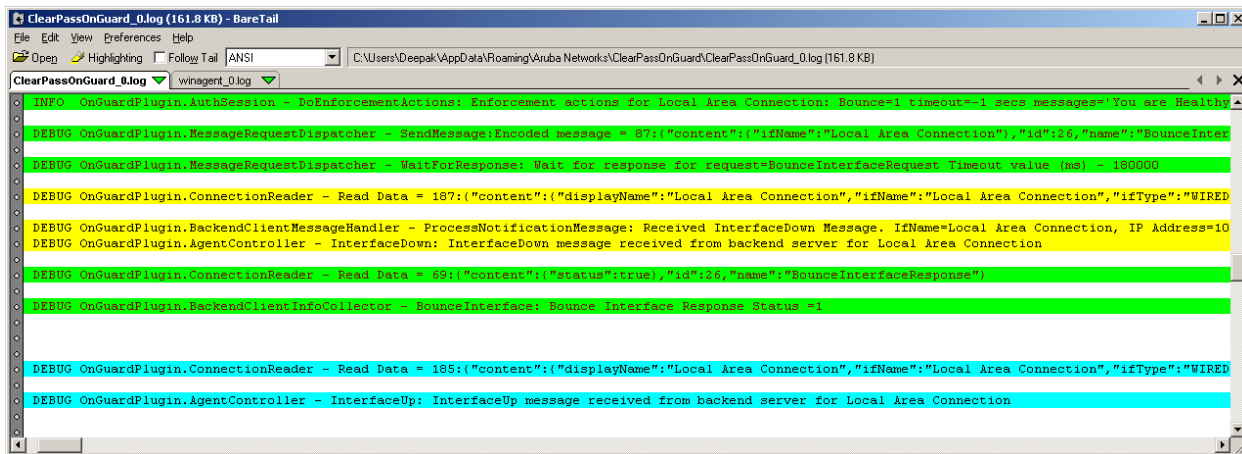
2014-03-17 11:57:57,719 [Th 00000e14] DEBUG OnGuardPlugin.BackendClientInfoCollector - BounceInterface: Bounce Interface Response Status =1

!

2014-03-17 11:57:58,008 [Th 000005cc] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 185:{"content":{"displayName":"Local Area 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":"BounceInterfaceRequest"}

2014-03-17 11:57:51,221 [Th 000000d8 Evt 04DF7530] INFO WinAgent.WinAgentNetworkProcessor - CWinAgentNetworkProcessor::BounceInterface() IfName=Local Area Connection

!

2014-03-17 11:57:51,393 [Th 000000d8 Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection

!

2014-03-17 11:57:51,562 [Th 000000fe0] 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, 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":"Local Area 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 11:57:57,664 [Th 000000d8 Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Successfully enabled(BOUNCE) the Network interface Local Area Connection

2014-03-17 11:57:57,695 [Th 000000d8 Evt 04DF7530] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=BounceInterfaceRequest

2014-03-17 11:57:57,695 [Th 000000d8 Evt 04DF7530] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 69:{"content":{"status":true},"id":26,"name":"BounceInterfaceResponse"}

!

2014-03-17 11:57:57,907 [Th 000000fe0] DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification

!

2014-03-17 11:57:57,935 [Th 000001E0] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration

2014-03-17 11:57:57,935 [Th 000001E0] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0|Current num interfaces=1

!

2014-03-17 11:57:57,935 [Th 000001E0] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123}|mac={00:1d:09:cc:a2:bc}

!

2014-03-17 11:57:57,939 [Th 000001E0] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 185:{"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":7,"name":"InterfaceUp"}

```

```

winagent_0.log (551.0 KB) - BareTail
File Edit View Preferences Help
C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (551.0 KB)
ClearPassOnGuard_0.log winagent_0.log

[Th 000000d8 Evt 04DF7530] DEBUG WinAgent.WinAgentReadEvHandler - Read data = 67:{"content":{"ifName":"Local Area Connection","id":26,"name":"BounceInterfaceRequest"}
[Th 000000d8 Evt 04DF7530] INFO WinAgent.WinAgentNetworkProcessor - CWinAgentNetworkProcessor::BounceInterface() IfName=Local Area Connection
[Th 000000d8 Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection
[Th 000000fe0 Evt 04DF7530] DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification
[Th 000001E0 Evt 04DF7530] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
[Th 000001E0 Evt 04DF7530] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=1|Current num interfaces=0
[Th 000001E0 Evt 04DF7530] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Following interface information, ip={10.20.23.123}|mac={00:1d:09:cc:a2:bc}
[Th 000001E0 Evt 04DF7530] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 187:{"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":7,"name":"InterfaceUp"}
[Th 000001E0 Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Successfully disabled(BOUNCE) the Network interface Local Area Connection
[Th 000001E0 Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Enabling the Network interface Local Area Connection
[Th 000001E0 Evt 04DF7530] INFO WinAgent.WinAgentNetworkControl - Successfully enabled(BOUNCE) the Network interface Local Area Connection
[Th 000001E0 Evt 04DF7530] DEBUG WinAgent.WinAgentReadEvHandler - Successfully processed the message=BounceInterfaceRequest
[Th 000001E0 Evt 04DF7530] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 69:{"content":{"status":true},"id":26,"name":"BounceInterfaceResponse"}
[Th 000001E0 Evt 04DF7530] DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification
[Th 000001E0 Evt 04DF7530] INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
[Th 000001E0 Evt 04DF7530] INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0|Current num interfaces=1
[Th 000001E0 Evt 04DF7530] WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123}|mac={00:1d:09:cc:a2:bc}
[Th 000001E0 Evt 04DF7530] DEBUG WinAgent.WinAgentEventHandler - Encoded message = 185:{"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":7,"name":"InterfaceUp"}

```

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: Trying to establish control channel for Local Area Connection to 10.17.4.234

!

2014-03-17 13:27:09,139 [Th 00000f10] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect from 10.20.23.123 to 10.17.4.234 at 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

!

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 AUTH_SERVER_DISCOVERY (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=AUTH_COMPLETE (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":"KeepAlive"}

2014-03-17 13:27:23,654 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (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=AUTH_COMPLETE (3) (Seconds in this state=15) for Local Area Connection

```



```

2014-03-17 13:27:09,109 [Th 00000f10] INFO OnGuardPlugin.AuthSession - DoEnforceEnforcements: Enforcement actions for Local Area Connection: Remote time
2014-03-17 13:27:09,112 [Th 00000f10] INFO OnGuardPlugin.AuthSession - EstablishControlChannel: Trying to establish control channel for Local Area Connec
.
2014-03-17 13:27:09,139 [Th 00000f10] DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect from 10.20.23.123 to 10.17.4.234 at 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, Por
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 AUTH_SERVER_DISCOVERY (1) to AUTH_COMPLETE (3) after 14
.
2014-03-17 13:27:18,652 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=5
2014-03-17 13:27:18,653 [Th 00000f10] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 42:{"content":"","id":30,"name":"KeepAl
2014-03-17 13:27:18,653 [Th 00000f10] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size - 46 Result - 46
.
2014-03-17 13:27:23,654 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=1
.
2014-03-17 13:27:28,659 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=1
.
2014-03-17 13:27:33,660 [Th 00000f10] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp 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: Trying to connect from 10.20.23.123 to 10.17.4.234 at
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 AUTH_SERVER_DISCOVERY (1) to
AUTH_COMPLETE (3) after 17 seconds

```

```

INFO OnGuardPlugin.AuthSession - EstablishControlChannel: Trying to establish control channel for Local Area Connection to 10.17.4.234
.
DEBUG OnGuardPlugin.ConnectionConnector - Connect: Trying to connect from 10.20.23.123 to 10.17.4.234 at port - 6658
ERROR OnGuardPlugin.ConnectionConnector - Connect: Failed to connect to Remote Server. Error - 10049 (The requested address is not valid in its context.)
ERROR OnGuardPlugin.SocketClient - Connect: BaseClient - Failed to connect. Returned value = -1
ERROR OnGuardPlugin.AuthSession - EstablishControlChannel: Establishing control channel failed for Local Area Connection
.
DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Local Area Connection
INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_SERVER_DISCOVERY (1) to AUTH_COMPLETE (3) after 17 seconds
INFO OnGuardPlugin.AgentController - SetCachedCredentials: Setting cache user credentials dj for interface=Local Area Connection

```

After Establishing Control Channel, the Network Interface is moved from AUTH_SERVER_DISCOVERY to AUTH_COMPLETE state.

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 check 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 14:00:04,602 [Th 000008ac] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=51) for Local Area Connection

2014-03-17 14:00:09,615 [Th 000008ac] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=56) for Local Area Connection

2014-03-17 14:00:14,641 [Th 000008ac] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=61) for Local Area Connection

!

2014-03-17 14:00:18,054 [Th 000008ac] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 69:{"content":{"status":true},"id":9,"name":"NotifyHealthStatusChange"}

!

2014-03-17 14:00:18,055 [Th 000008ac] DEBUG OnGuardPlugin.AgentController - HealthInfoChanged: Health State Changed message received from backend server

!

2014-03-17 14:00:18,056 [Th 000008ac] INFO OnGuardPlugin.InterfaceManager - HandleHealthStateChange: Got HealthStateChange in state=AUTH_COMPLETE (3) for Local Area Connection

!

2014-03-17 14:00:18,057 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:{"id":40,"name":"CollectHealthDataRequest"}

2014-03-17 14:00:18,059 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000
```

```

2014-03-17 14:00:18,098 [Th 00000fac] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
71:{"content":{"status":true},"id":40,"name":"CollectHealthDataResponse"}

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":"SoHRequest"}

2014-03-17 14:00:18,133 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=SoHRequest
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":"SoHResponse"}

!

2014-03-17 14:00:18,174 [Th 000008ac] DEBUG OnGuardPlugin.InterfaceSessionHelper - CollectHealthData: SoH:
0x0007034300000137.....001378000000700080001378000040200

2014-03-17 14:00:18,174 [Th 000008ac] DEBUG OnGuardPlugin.AuthSession - DoSoftReAuth: Local Area Connection: Messages returned by CollectHealth -

!

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 - ProcessSohr: Language: en SoHR:
0x000701a800000137000201a00007.....c6338f881c3cbbcd6aba13ed02efafa37f21867fc

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,-96,0,7,0.....53,-66,-42,-85,-95,62,-48,46,-6,-6,55,-14,24,103,-
4]},"id":44,"name":"ProcessSoHRequest"}

2014-03-17 14:00:18,293 [Th 000008ac] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for
request=ProcessSoHRequest Timeout value (ms) - 300000

2014-03-17 14:00:19,857 [Th 00000fac] DEBUG OnGuardPlugin.ConnectionReader - Read Data =
419:{"content":{"healthStatus":false,"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":"ProcessSoHResponse"}

!

2014-03-17 14:00:19,860 [Th 000008ac] DEBUG OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: Healthy - 0
Success - 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: Moving from AUTH_COMPLETE (3) to
AUTH_SERVER_DISCOVERY (1) after 72 seconds

```

```

ClearPassOnGuard_0.log (243.8 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPass\OnGuard\ClearPassOnGuard_0.log (243.8 KB)
wlogent_0.log ClearPassOnGuard_0.log
INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=51) for Local Area Connection
INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=56) for Local Area Connection
INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=61) for Local Area Connection
DEBUG OnGuardPlugin.ConnectionReader - Read Data = 69:{"content":{"status":true,"id":9,"name":"NotifyHealthStatusChange"}}
DEBUG OnGuardPlugin.AgentController - HealthInfoChanged: Health State Changed message received from backend server
INFO OnGuardPlugin.InterfaceManager - HandleHealthStateChange: Got HealthStateChange in state=AUTH_COMPLETE (3) for Local Area Connection
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Encoded message = 44:{"id":40,"name":"CollectHealthDataRequest"}
DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000
DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:{"content":{"status":true,"id":40,"name":"CollectHealthDataResponse"}}
DEBUG OnGuardPlugin.BackendClientInfoCollector - CollectHealthData: Collect Health Data Response Status = 1
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Encoded message = 30:{"id":42,"name":"SoHRequest"}
DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=SoHRequest Timeout value (ms) - 180000
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":"S
DEBUG OnGuardPlugin.InterfaceSessionHelper - CollectHealthData: SoH: 0x0007034300000137.....0013780000007000800013780000040200
DEBUG OnGuardPlugin.AuthSession - DoSoftReAuth: Local Area Connection: Messages returned by CollectHealth -
INFO OnGuardPlugin.WsHttpClient - Posting request to URL=/v2/PostureReeval/OnGuard
INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: Local IP: 10.20.23.123 Remote IP: 10.17.4.234, url: https://10.17.4.234/networkservices/webauthservi
INFO OnGuardPlugin.HttpClientWrapper - ExecuteMethod: HTTP Response Code - 200
INFO OnGuardPlugin.AuthSession - ProcessSoftReauthResponse: Response=(, sohSize=428)
DEBUG OnGuardPlugin.InterfaceSessionHelper - ProcessSoHr: Language: en SoHR: 0x000701a800000137000201a00007.....c6336f681c3cbbed6aba13ed02efafa3
DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Encoded message = 1493:{"content":{"language":"en","remediate":false,"sohr":{"[0,7,1,-88,0,0,1,55,
DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=ProcessSoHRequest Timeout value (ms) - 300000
DEBUG OnGuardPlugin.ConnectionReader - Read Data = 419:{"content":{"healthStatus":false,"messages":{"[null,[10,0,70,0,108,0,114,0,101,0,119,0,97,0,108,0,108
DEBUG OnGuardPlugin.BackendClientInfoCollector - ProcessHealthResponse: ProcessSoHR Response: Healthy - 0 Success - 1
DEBUG OnGuardPlugin.AuthSession - IsHealthStateChanged: Health state from soft re-auth for Local Area Connection = 3
INFO OnGuardPlugin.AuthSession - IsHealthStateChanged: Status of health evaluation has changed for Local Area Connection. Old state=1 New state=3
INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to 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

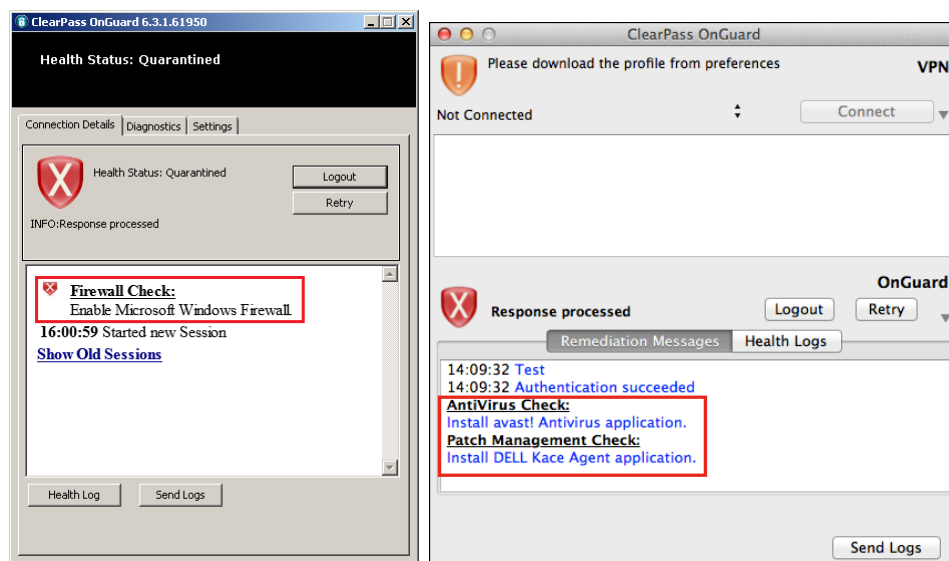
OnGuard Agent can do automatic remediation of unhealthy health classes to make a client compliant, if auto-remediation is enabled.

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 [Health Checks and Auto-Remediation](#) 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

```

```

winagent_0.log (626.4 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (626.4 KB)
winagent_0.log ClearPassOnGuard_0.log winagent_remediate_0.log
INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Status of Firewall Health Class is Not_Healthy. Global Remediate Flag - 1
INFO WinSHA.FWHealthClassInfoFactory - ProcessHealthResponse: Application Microsoft Windows Firewall is Unhealthy.
INFO WinSHA.FWHealthClassInfoFactory - GetEnableRemediationAttrValue: Value of EnableRemediation attribute of Application Microsoft Windows Firewall is 1
INFO WinSHA.FWHealthClassInfoFactory - GetEnableNotificationAttrValue: Value of EnableNotification attribute of Application Microsoft Windows Firewall is 1
INFO WinSHA.FWHealthClassInfoFactory - ProcessStatusAttr: Product Id: 6015 Product Version: 7
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
Open Highlighting Follow Tail ANSI C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_remediate_0.log (3.0 KB)
winagent_0.log ClearPassOnGuard_0.log winagent_remediate_0.log
[MainTh 2020:1920] INFO WinSHARemediate - _tWinMain: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassUSHARemediate.exe -Embedding
[MainTh 2020:1920] INFO WinSHARemediate - _tWinMain: ClearPassUSHARemediate 6.3.1.61950
[MainTh 2020:1920] INFO WinSHARemediate - _tWinMain: Initializing OESIS SDK
[MainTh 2020:1920] INFO WinSHARemediate - _tWinMain: OESIS SDK Version: "3.6.8769.2"
[MainTh 2020:1920] DEBUG WinSHARemediate - SetRTPStatus: Name: Microsoft Security Essentials, ID: 6020, Version: 4.2.0223.0
[MainTh 2020:1920] INFO WinSHARemediate - SetRTPStatus: Enabled real time protection status of Microsoft Security Essentials application
[MainTh 2020:1920] INFO WinSHARemediate - _tWinMain: Uninitializing OESIS SDK

```

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=AUTH_COMPLETE (3) (Seconds in this state=20) for Local Area Connection
!
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 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
!
2014-03-21 11:49:06,826 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Local Area Connection
!
2014-03-21 11:49:06,875 [Th 000003e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
!
2014-03-21 11:49:06,876 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - HandleReconnect: Automatically starting Health check Local Area Connection
!
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:{"id":42,"name":"CollectHealthDataRequest"}
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000
!
2014-03-21 11:49:06,929 [Th 0000138c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:{"content":{"status":true},"id":42,"name":"CollectHealthDataResponse"}
```

```

ClearPassOnGuard_0.log (187.0 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (187.0 KB)
winagent_0.log ClearPassOnGuard_0.log
2014-03-21 11:48:57,147 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=
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 Con
2014-03-21 11:49:00,795 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from AUTH_COMPLETE (3) to RECONNECT_USER (5) after 29 second
2014-03-21 11:49:06,826 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Local
2014-03-21 11:49:06,875 [Th 000003e8] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
2014-03-21 11:49:06,876 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - HandleReconnect: Automatically starting Health check Local Area Connection
2014-03-21 11:49:06,876 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - GetNetworkInterfaceList: Network interfaces list size for Local Area Connect
2014-03-21 11:49:06,878 [Th 000003e8] DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: IsHealthCheckQuietPeriodEnabled() returned false for lo
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.AuthSession - InHealthCheckQuietPeriod: Possible cause - InterfaceType=VPN | Mode=HealthOnly
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.AuthSession - Authenticate: Not In HealthCheckQuietPeriod, Performing Full Auth with health ch
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Encoded message = 44:{"id":42,"name":"CollectHealthDataR
2014-03-21 11:49:06,877 [Th 000003e8] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequ
2014-03-21 11:49:06,929 [Th 0000138c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:{"content":{"status":true},"id":42,"name":"CollectHealthDataR

```

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 Local Area Connection

2014-03-21 11:49:13,488 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from RECONNECT_USER (5) to AUTH_COMPLETE (3) after 12 seconds

```

ClearPassOnGuard_0.log (187.0 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (187.0 KB)
winagent_0.log ClearPassOnGuard_0.log
2014-03-21 11:49:13,488 [Th 000003e8] DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Local Area Connection
2014-03-21 11:49:13,488 [Th 000003e8] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from RECONNECT_USER (5) to AUTH_COMPLETE (3) after 12 sec

```

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
!
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
!
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 Connection
!
2014-03-21 12:11:17,750 [Th 00000218] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 45:{"id":164,"name":"CollectHealthDataRequest"}
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"}

```

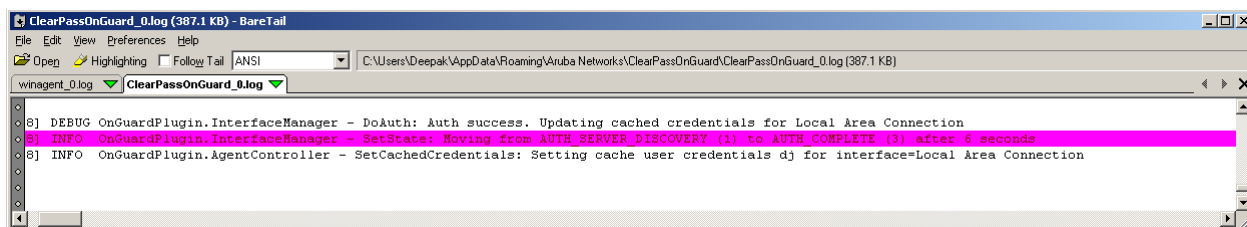
After health checks are complete, the Network Interface is moved from AUTH_SERVER_DISCOVERY to AUTH_COMPLETE state.

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 Logout 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 their 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=AUTH_COMPLETE (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

!

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 - DoLogout: Logout not supported or did not work. Trying bounce 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":"BounceInterfaceRequest"}

2014-03-21 15:11:16,593 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=BounceInterfaceRequest Timeout value (ms) - 180000

2014-03-21 15:11:17,050 [Th 00000d2c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName":"Local Area 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":"BounceInterfaceResponse"}

!

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"}

!

2014-03-21 15:11:21,251 [Th 00000d2c] DEBUG OnGuardPlugin.AgentController - InterfaceUp: InterfaceUp message received from backend server for Local Area Connection

!

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=**

!

2014-03-21 15:12:20,918 [Th 00000140] DEBUG OnGuardPlugin.AgentController - **HandleUserCredentials: Handling User Credentials for Local Area 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**

!

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 - **DoWaitForAuthCredentials: Only health checks required for Local Area Connection**

!

2014-03-21 15:12:20,963 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - **SendMessage: Encoded message = 45:{"id":104,"name":"CollectHealthDataRequest"}**

2014-03-21 15:12:20,964 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - **WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value (ms) - 1200000**

!

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

```

11:09,757 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=225) for Local Area Connection
11:10,572 [Th 5236:3988] INFO OnGuardPlugin.NetworkInterfaceActionListener - Logout: Logout requested Local Area Connection
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
11:14,593 [Th 00000140] DEBUG OnGuardPlugin.InterfaceManager - BounceLogout: Logout not supported or did not work. Trying bounce Local Area Connection
11:14,593 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 87:{"content":{"ifName":"Local Area Connection"},"id":114,"name":"BounceInterfaceRequest","timeout":30}
11:14,593 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=BounceInterfaceRequest Timeout value=30
11:17,050 [Th 0000042c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection"},"id":114,"name":"BounceInterfaceResponse"}
11:17,052 [Th 0000042c] DEBUG OnGuardPlugin.AgentController - InterfaceDown: InterfaceDown message received from backend server for Local Area Connection
11:21,183 [Th 0000042c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 69:{"content":{"status":true},"id":142,"name":"BounceInterfaceResponse"}
11:21,248 [Th 0000042c] DEBUG JsonWrapper.Netstrings - Extracted Netstrings message = {"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection"},"id":142,"name":"BounceInterfaceResponse"}
11:21,251 [Th 0000042c] DEBUG OnGuardPlugin.AgentController - InterfaceUp: InterfaceUp message received from backend server for Local Area Connection
11:21,328 [Th 00000140] DEBUG OnGuardPlugin.AgentController - HandleIfUp: New Interface Up = IfName=Local Area Connection IfType=WIRED DisplayName=Local Area Connection
11:21,328 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - HandleIfUp: Got IfUp in state=LOGGED_OUT (4)
11:21,329 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - HandleIfUp: Notify interface up. Waiting for user action Local Area Connection
12:20,910 [Th 5236:3988] INFO OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Connection Username=
12:20,918 [Th 00000140] DEBUG OnGuardPlugin.AgentController - HandleUserCredentials: Handling User Credentials for Local Area Connection
12:20,919 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from LOGGED_OUT (4) to AUTH_SERVER_DISCOVERY (1) after 70 seconds
12:20,957 [Th 00000140] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
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 seconds
12:20,961 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - DoWaitForAuthCredentials: Only health checks required for Local Area Connection
12:20,963 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 45:{"id":104,"name":"CollectHealthDataRequest"}
12:20,964 [Th 00000140] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=CollectHealthDataRequest Timeout value=30
12:23,153 [Th 0000042c] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 72:{"content":{"status":true},"id":104,"name":"CollectHealthDataResponse"}

```

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):

2014-03-21 15:12:29,477 [Th 00000140] DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Local Area Connection

2014-03-21 15:12:29,477 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from WAIT_FOR_CREDENTIALS (2) to AUTH_COMPLETE (3) after 8 seconds

```

12:29,477 [Th 00000140] DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Local Area Connection
12:29,477 [Th 00000140] INFO OnGuardPlugin.InterfaceManager - SetState: Moving from WAIT_FOR_CREDENTIALS (2) to AUTH_COMPLETE (3) after 8 seconds

```

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 their 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=AUTH_COMPLETE (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

!

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":"BounceInterfaceRequest"}

2014-03-21 13:47:54,235 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=BounceInterfaceRequest Timeout value (ms) - 180000

2014-03-21 13:47:55,546 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection","ifType":"WIRED","ipAddress":"10.20.23.123","macAddress":"001d09cca2bc"},"id":5,"name":"InterfaceDown"}

!

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":"BounceInterfaceResponse"}

!

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":"Local Area 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: New Interface Up = IfName=Local Area Connection 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 - HandleIfUp: Got IfUp in state=LOGGED_OUT (4)

```

2014-03-21 13:48:07,711 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - HandleIfUp: **Notify interface up. Waiting for user action Local Area Connection**

2014-03-21 13:48:07,711 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Local Area Connection

!

2014-03-21 13:48:07,891 [Th 00001504] DEBUG OnGuardPlugin.InterfaceManager - **PickAuthServer: Current domain=default Auth server=10.17.4.234**

!

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 5556:5108] INFO OnGuardPlugin.NetworkInterfaceActionListener - **SetUserAuthInfo: User auth info available for Local Area Connection Username=dj**

!

2014-03-21 13:48:57,598 [Th 00001504] DEBUG OnGuardPlugin.AgentController - **HandleUserCredentials: Handling User Credentials for Local Area Connection**

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 server=10.17.4.234**

!

2014-03-21 13:48:57,651 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:{"id":84,"name":"CollectHealthDataRequest"}

!

2014-03-21 13:48:57,694 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:{"content":{"status":true},"id":84,"name":"CollectHealthDataResponse"}

```
ClearPassOnGuard_0.log (151.9 KB) - Bare Tail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (151.9 KB)
winagent_0.log ClearPassOnGuard_8.log
2014-03-21 13:47:47,016 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH_COMPLETE (3) (Seconds in this state=25)
2014-03-21 13:47:48,215 [Th 5556:5108] INFO OnGuardPlugin.NetworkInterfaceActionListener - Logout: Logout requested Local Area Connection
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 - DeLogout: 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":"BounceInterfaceRequest","status":true},"id":84,"name":"CollectHealthDataRequest"}
2014-03-21 13:47:54,235 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - WaitForResponse: Wait for response for request=BounceInterfaceRequest
2014-03-21 13:47:55,546 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 187:{"content":{"displayName":"Local Area Connection","ifName":"Local Area Connection","id":32,"name":"BounceInterfaceRequest","status":true},"id":84,"name":"CollectHealthDataRequest"}
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 13:48:07,345 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 69:{"content":{"status":true,"id":32,"name":"BounceInterfaceRequest","status":true},"id":84,"name":"CollectHealthDataRequest"}
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":"Local Area Connection","ifName":"Local Area Connection","id":32,"name":"BounceInterfaceRequest","status":true},"id":84,"name":"CollectHealthDataRequest"}
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: New interface up - IfName=Local Area Connection IfType=Wired Display
2014-03-21 13:48:07,710 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - HandleIfUp: Got IfUp in state=LOGGED_OUT (4)
2014-03-21 13:48:07,711 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - HandleIfUp: Notify interface up. Waiting for user action Local Area Connection
2014-03-21 13:48:07,711 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - PerformLoggedOutStateChecks: Determine auth server in logged out state Local Area Connection
2014-03-21 13:48:07,891 [Th 00001504] DEBUG OnGuardPlugin.InterfaceManager - PickAuthServer: Current domain=default Auth server=10.17.4.234
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)
2014-03-21 13:48:57,591 [Th 5556:5108] INFO OnGuardPlugin.NetworkInterfaceActionListener - SetUserAuthInfo: User auth info available for Local Area Connection
2014-03-21 13:48:57,595 [Th 00001504] INFO OnGuardPlugin.AgentController - HandleServerCredentials: Handling User Credentials for Local Area Connection
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 server=10.17.4.234
2014-03-21 13:48:57,651 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage:Encoded message = 44:{"id":84,"name":"CollectHealthDataRequest","status":true,"id":84,"name":"CollectHealthDataRequest"}
2014-03-21 13:48:57,694 [Th 000016b8] DEBUG OnGuardPlugin.ConnectionReader - Read Data = 71:{"content":{"status":true,"id":84,"name":"CollectHealthDataRequest","status":true},"id":84,"name":"CollectHealthDataRequest"}
```

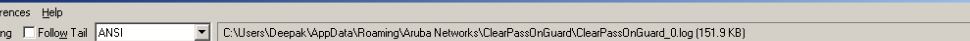
After the health checks are done, the Network Interface is moved from an AUTH_SERVER_DISCOVERY to an AUTH_COMPLETE state.

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 Local Area Connection

2014-03-21 13:49:03,964 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - **SetState: Moving from AUTH_SERVER_DISCOVERY (1) to AUTH COMPLETE (3) after 2 seconds**

2014-03-21 13:49:03,964 [Th 00001504] INFO OnGuardPlugin.AgentController - SetCachedCredentials: Setting cache user credentials dj for interface=Local Area Connection



ClearPassOnGuard_0.log (151.9 KB) - BareTail

File Edit View Preferences Help

Open Highlighting Follow Tail ANSI C:\Users\Deepak\AppData\Roaming\Aruba Networks\ClearPassOnGuard\ClearPassOnGuard_0.log (151.9 KB)

winagent_0.log ClearPassOnGuard_0.log

```

2014-03-21 13:49:03,963 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size = 249 Result = 249
2014-03-21 13:49:03,963 [Th 00001504] DEBUG OnGuardPlugin.InterfaceManager - DoAuth: Auth success. Updating cached credentials for Local Area Connection
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
2014-03-21 13:49:03,964 [Th 00001504] INFO OnGuardPlugin.AgentController - SetCachedCredentials: Setting cache user credentials dj for interface=Local Ar
2014-03-21 13:49:03,964 [Th 00001504] INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue. Waiting for 5000 ms.
2014-03-21 13:49:03,965 [Th 00000764] DEBUG OnGuardPlugin.BaseClient - Run: BaseClient Thread starting
2014-03-21 13:49:08,964 [Th 00001504] INFO OnGuardPlugin.ActionQueue - Dequeue: No pending events in the queue 04205430
2014-03-21 13:49:08,964 [Th 00001504] INFO OnGuardPlugin.InterfaceManager - HandleNoOp: NoOp handling in state=AUTH COMPLETE (3) (Seconds in this state=5
2014-03-21 13:49:08,965 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Encoded message = 43:{"content":"","id":102,"name":"Keep
2014-03-21 13:49:08,965 [Th 00001504] DEBUG OnGuardPlugin.MessageRequestDispatcher - SendMessage: Done sending the data. Size = 47 Result = 47

```

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.

Backend Service Logs (Bounce Network Interface After Logout):

```

2014-03-21 15:56:34,687 [Th 000001F4] INFO WinAgent.WinAgentDisconnectHandler - Disconnect cancel event timedout
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
!
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. Previous num 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=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}

```

```

winagent_0.log (1.6 MB) - BareTail
File Edit View Preferences Help
C:\ProgramData\Aruba Networks\ClearPassOnGuard\winagent_0.log (1.6 MB)
winagent_0.log ClearPassOnGuard_0.log
INFO WinAgent.WinAgentDisconnectHandler - Disconnect cancel event timedout
DEBUG WinAgent.WinAgentNetworkProcessor - TimerCompletionEv: Received TimerCompletionEv with id=0
INFO WinAgent.WinAgentNetworkProcessor - CWinAgentNetworkProcessor::BounceInterface() IfName=Local Area Connection
INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection
DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification
INFO WinAgent.WinAgentNetworkProcessor - Run: Network Interface Change event signalled
INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=1|Current num interfaces=0
WARN 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 WinAgent.WinAgentNetworkControl - Enabling the Network interface Local Area Connection
INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0|Current num interfaces=1
WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123}|mac={00:1d:09:cc:a2:bc}

```

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 =
82:{"content":{"interfaceBounceDelay":3,"now":false,"id":28,"name":"BounceManaged"}

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 - Bouncing the managed network interfaces for
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::BounceInterface() IfName=Local
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 num
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, 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

!

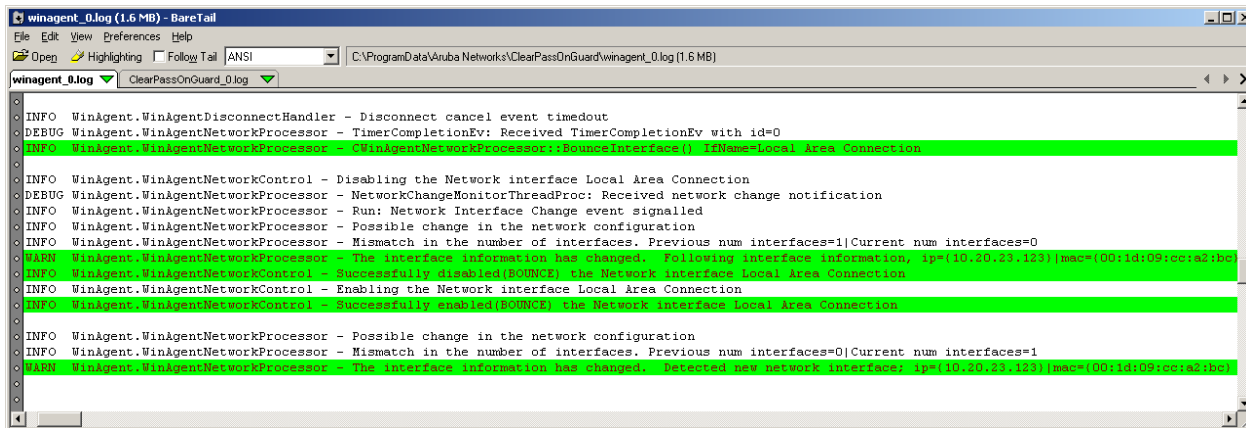
```

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}**



The screenshot shows a log viewer window titled "winagent_0.log (1.6 MB) - BareTail". The log content is as follows:

```
INFO WinAgent.WinAgentDisconnectHandler - Disconnect cancel event timedout
DEBUG WinAgent.WinAgentNetworkProcessor - TimerCompletionEv: Received TimerCompletionEv with id=0
INFO WinAgent.WinAgentNetworkProcessor - (WinAgentNetworkProcessor::BounceInterface) IfName=Local Area Connection
INFO WinAgent.WinAgentNetworkControl - Disabling the Network interface Local Area Connection
DEBUG WinAgent.WinAgentNetworkProcessor - NetworkChangeMonitorThreadProc: Received network change notification
INFO WinAgent.WinAgentNetworkProcessor - Run: Network Interface Change event signalled
INFO WinAgent.WinAgentNetworkProcessor - Possible change in the network configuration
INFO WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=1|Current num interfaces=0
WARN 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 WinAgent.WinAgentNetworkControl - 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 WinAgent.WinAgentNetworkProcessor - Mismatch in the number of interfaces. Previous num interfaces=0|Current num interfaces=1
WARN WinAgent.WinAgentNetworkProcessor - The interface information has changed. Detected new network interface; ip={10.20.23.123}|mac={00:1d:09:cc:a2:bc}
```

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 Networks\ClearPassOnGuard\ClearPassAgentController.exe
2014-02-21	16:38:58:568	2280	9fc	COMAPI	-- START -- COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-21	16:38:58:609	2280	9fc	COMAPI	<<-- SUBMITTED -- COMAPI: Search [ClientId = ClearPass OnGuard 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'"
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 update {BEE25D62-3828-44EF-9B60-502DC4F14C2B}.104 to search 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 result
2014-02-21	16:40:48:426	1028	16c4	Agent	* Added update {348303EC-CCBB-4EB1-88CD-191EF876EFCA}.201 to search result
2014-02-21	16:40:48:427	1028	16c4	Agent	Update {200DFFAD-C01D-49ED-9BA4-80EC7D6EA6F0}.201 is pruned out due to potential supersedence
2014-02-21	16:40:48:427	1028	16c4	Agent	* Added update {B5C84092-6294-4358-86EB-7D743AABD04A}.201 to search result
2014-02-21	16:40:48:427	1028	16c4	Agent	Update {49628BAF-1305-40D2-BBB9-14D852C82B0E}.201 is pruned out due to potential supersedence
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 update {9655393D-1B46-46A2-AC21-C4D1B5E960D1}.202 to search result

2014-02-21	16:40:48:432	1028	16c4	Agent	* Found 63 updates and 10 categories in search; evaluated appl. rules of 1221 out of 2424 deployed entities
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]

```

2014-02-21 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
2014-02-21 16:38:58:568 2280 9fc Misc = Module: C:\Windows\system32\wuapi.dll
2014-02-21 16:38:58:568 2280 9fc COMAPI -----
2014-02-21 16:38:58:568 2280 9fc COMAPI -- START -- COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-21 16:38:58:568 2280 9fc COMAPI -----
2014-02-21 16:38:58:609 2280 9fc COMAPI <<-- SUBMITTED -- COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-21 16:38:58:609 1028 16c4 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 *****
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'"
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 update (BEE25D62-3828-44EF-9B60-502DC4F14C2B).104 to search 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 result
2014-02-21 16:40:48:426 1028 16c4 Agent * Added update (348303EC-CCBB-4EB1-88CD-191EF876EFC).201 to search result
2014-02-21 16:40:48:427 1028 16c4 Agent Update (200DFFAD-C01D-49ED-9BA4-80EC7D6EA6F0).201 is pruned out due to potential supersedence
2014-02-21 16:40:48:427 1028 16c4 Agent * Added update (B5C84092-6294-4358-86EB-7D743AABD04A).201 to search result
2014-02-21 16:40:48:427 1028 16c4 Agent Update (49628BAF-1305-40D2-BBB9-14D852C82B0E).201 is pruned out due to potential supersedence
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 update (9F45C5C2-5497-4E82-9E11-69DB6B9631C3).201 to search result
2014-02-21 16:40:48:431 1028 16c4 Agent * Added update (54D21173-5D5C-441B-8893-C14D1E13D18E).201 to search result
2014-02-21 16:40:48:431 1028 16c4 Agent * Added update (EA312223-9F71-4FC8-B5A8-598175141EF4).203 to search result
2014-02-21 16:40:48:431 1028 16c4 Agent * Added update (71A74817-374C-424D-BD12-E6E3076E0059).204 to search result
2014-02-21 16:40:48:431 1028 16c4 Agent * Added update (9655393D-1B46-46A2-AC21-C4D1B5E960D1).202 to search result
2014-02-21 16:40:48:432 1028 16c4 Agent * Found 63 updates and 10 categories in search; evaluated appl. rules of 1221 out of 2424 deployed entities
2014-02-21 16:40:48:513 1028 16c4 Agent ** END ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]
2014-02-21 16:40:48:513 1028 16c4 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 -----
2014-02-21 16:40:48:835 2280 15cc COMAPI -- END -- COMAPI: Search [ClientId = ClearPass OnGuard Agent]
2014-02-21 16:40:48:835 2280 15cc COMAPI -----

```

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\ClearPassOnGuard\ClearPassAgentController.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	18:27:53:141	1052	113c	Agent	*****
2014-02-22	18:27:53:141	1052	113c	Agent	** START ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]
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-b877473b6441'"
2014-02-22	18:27:53:141	1052	113c	Agent	* ServiceID = {7971F918-A847-4430-9279-4A52D1EFE18D} Third party service
2014-02-22	18:27:53:141	1052	113c	Agent	* Search Scope = {Machine}
2014-02-24	00:55:31:535	1052	134	AU	AU setting next sqm report timeout to 2014-02-24 19:25:31
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	*****
2014-02-24	00:56:25:455	1052	113c	Agent	** END ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]
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]
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.
2014-02-24	00:56:25:564	1648	418	COMAPI	- Updates found = 0
2014-02-24	00:56:25:564	1648	418	COMAPI	- WARNING: Exit code = 0x00000000, Result code = 0x8024001E
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	00:56:25:596	1648	14c	COMAPI	FATAL: Unable to complete asynchronous search. (hr=8024001E)
2014-02-24	00:56:25:611	1052	134	Report	CWERReporter finishing event handling. (00000000)

```

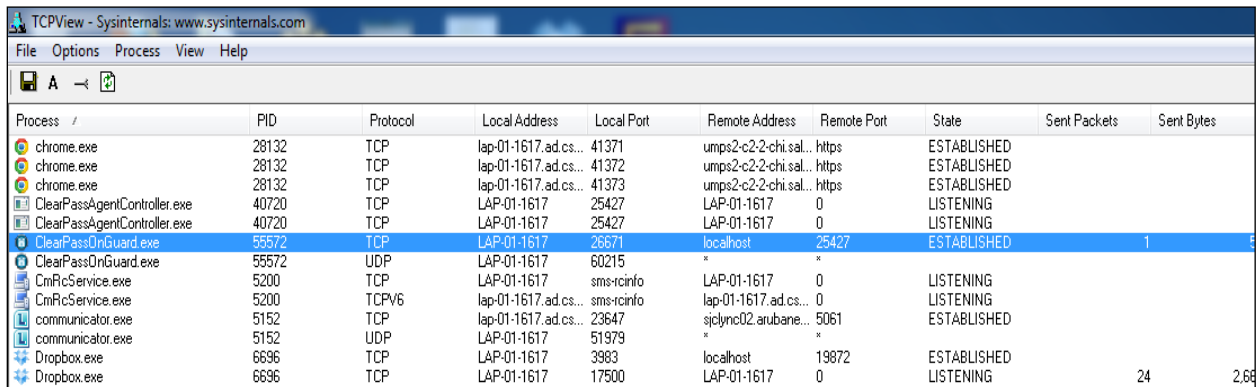
WindowsUpdate.log (1.8 MB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Windows\WindowsUpdate.log (1.8 MB)
winagent_0.log ClearPassOnGuard_0.log winagent_remediate_0.log WindowsUpdate.log
2014-02-22 18:27:53:134 1648 69c Misc ===== Logging initialized (build: 7.6.7600.256, tz: +0530) =====
2014-02-22 18:27:53:134 1648 69c Misc * Process: C:\Program Files\Aruba Networks\ClearPassOnGuard\ClearPassAgentController.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 18:27:53:141 1052 113c Agent *****
2014-02-22 18:27:53:141 1052 113c Agent ** START ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]
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-b877473b6441'"
2014-02-22 18:27:53:141 1052 113c Agent * ServiceID = {7971F918-A847-4430-9279-4A52D1EFE18D} Third party service
2014-02-22 18:27:53:141 1052 113c Agent * Search Scope = {Machine}
2014-02-24 00:55:31:535 1052 134 AU AU setting next sqm report timeout to 2014-02-24 19:25:31
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 = 0x8024000E
2014-02-24 00:56:25:455 1052 113c Agent *****
2014-02-24 00:56:25:455 1052 113c Agent ** END ** Agent: Finding updates [CallerId = ClearPass OnGuard Agent]
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]
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.
2014-02-24 00:56:25:564 1648 418 COMAPI - Updates found = 0
2014-02-24 00:56:25:564 1648 418 COMAPI - WARNING: Exit code = 0x00000000, Result code = 0x8024001E
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 00:56:25:596 1648 14c COMAPI FATAL: Unable to complete asynchronous search. (hr=8024001E)
2014-02-24 00:56:25:611 1052 134 Report CWERReporter finishing event handling. (00000000)
  
```

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>



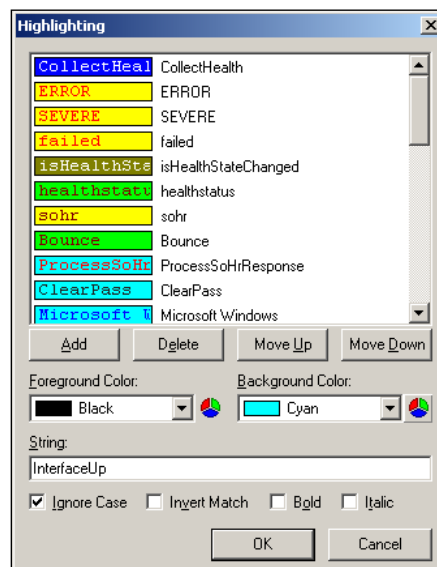
The screenshot shows the TCPView application window with a menu bar (File, Options, Process, View, Help) and a toolbar. Below is a table of active network connections.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes
chrome.exe	28132	TCP	lap-01-1617.ad.cs...	41371	umps2-c2-2-chi.sal..	https	ESTABLISHED		
chrome.exe	28132	TCP	lap-01-1617.ad.cs...	41372	umps2-c2-2-chi.sal..	https	ESTABLISHED		
chrome.exe	28132	TCP	lap-01-1617.ad.cs...	41373	umps2-c2-2-chi.sal..	https	ESTABLISHED		
ClearPassAgentController.exe	40720	TCP	LAP-01-1617	25427	LAP-01-1617	0	LISTENING		
ClearPassAgentController.exe	40720	TCP	LAP-01-1617	25427	LAP-01-1617	0	LISTENING		
ClearPassOnGuard.exe	55572	TCP	LAP-01-1617	26671	localhost	25427	ESTABLISHED	1	
ClearPassOnGuard.exe	55572	UDP	LAP-01-1617	60215	*	*			
CmRcService.exe	5200	TCP	LAP-01-1617	sms-rcinfo	LAP-01-1617	0	LISTENING		
CmRcService.exe	5200	TCPV6	lap-01-1617.ad.cs...	sms-rcinfo	lap-01-1617.ad.cs...	0	LISTENING		
communicator.exe	5152	TCP	lap-01-1617.ad.cs...	23647	sjclync02.arubane...	5061	ESTABLISHED		
communicator.exe	5152	UDP	LAP-01-1617	51979	*	*			
Dropbox.exe	6696	TCP	LAP-01-1617	3983	localhost	19872	ESTABLISHED		
Dropbox.exe	6696	TCP	LAP-01-1617	17500	LAP-01-1617	0	LISTENING	24	2,66

Baretail – Log viewer for Windows.

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

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



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 -
https://arubapedia.arubanetworks.com/arubapedia/images/2/2e/OnGuard_in_a_Cluster.pdf

OnGuard_in_a_Cluster.pdf
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_Evaluation_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_Dissolvable_Agent_Workflow_and_Configuration
7. ClearPass OnGuard Auto-Remediation -
https://arubapedia.arubanetworks.com/arubapedia/index.php/Clearpass_Onguard_Auto-Remediation