SE ClearPass Remote Demo
Wireless OnGuard

Table of Contents

Introduction

This is a step-by-step guide on how to perform the ClearPass Wireless OnBoard demo, what to show the customer and what to say while doing it.

Assumptions are made that the reader is already familiar with the demo set-up (please refer to "SE ClearPass Remote Demo - Platform Information" document for further details).

CAUTION

DO NOT MAKE ANY CONFIGURATION CHANGES TO THE CLEARPASS SERVER OR THE WIRELESS CONTROLLER. DOING SO WILL CHANGE THE BEHAVIOUR OF THE DEMO SETUP REDERING IT USELESS FOR OTHERS.

Equipment Requirements

1. Wireless Client PC
2. Admin PC (optional)
3. Pre-provisioned RAP (please see "SE ClearPass Remote Demo - Platform Information" documentation for further details)
4. USB Key (see below for more info)

This demo is written for a Windows OS client (XP -> Win8).

The Admin PC is used to show the Controller administration GUI and the changing of the attributed user role, depending on the health state of the client PC.

NB The contents of the ACL's associated with the different roles do not restrict network access. Therefore it is possible to show the Admin side on the client PC.

An explanation, if required:

"This demo shows how we can automatically and dynamically change the user role as a function of the health status of the client PC. We have decided to leave the roles the same as it is not the goal to show how to configure Access Control Lists (ACLs) nor are we showing any ACL contents.

The contents of the role are defined by the Administrator/IT Security Policy. Everyone will have different ideas and requirements.

The main thing to keep in mind is that, even if the desire is to severely restrict network access if a client becomes 'unhealthy', provisions must be made to allow the client to either access a remediation server (depending on the reason for the non-compliance) and to communicate with the CPPM server."

Different Windows OS

The USB key demo works on all flavours of Windows. However, if you are using windows 7 it is possible to perform the demo by substituting the USB requirement with the program 'notepad'.

Instead of inserting a USB key, run 'notepad.exe' in its place.

Overview of the Client Demo

In this demo we want to show to the customer how to protect the network by ensuring that all connected end-points conform to the corporate security policy.

A popularly held opinion regarding a BYOD (Bring Your Own Device) strategy is that the network needs to be 'opened up' to allow access to a (potentially) diverse range of equipment. This is wrong! The opposite is true – the network needs to be *more* secure, giving an enterprise the option and the possibility to allow employees to bring their favoured device on the network.

One part of this strategy is to ensure that equipment connecting to the network adhere, at the very least in part, to the corporate security policy.

This can be enforced by deploying ClearPass OnGuard.

The ClearPass OnGuard agent communicates to the CPPM (ClearPass Policy Manager) the 'health' status of the end-point, which allows the CPPM to take decisions on the type of network access given to the end-point as a function of the end-point's compliance with the pre-defined security policy.

During this demo, we will see how a user can connect to the network, be given a particular 'role' which defines their network access, and see this role change as the end-point becomes out-of-compliance with the security policy.

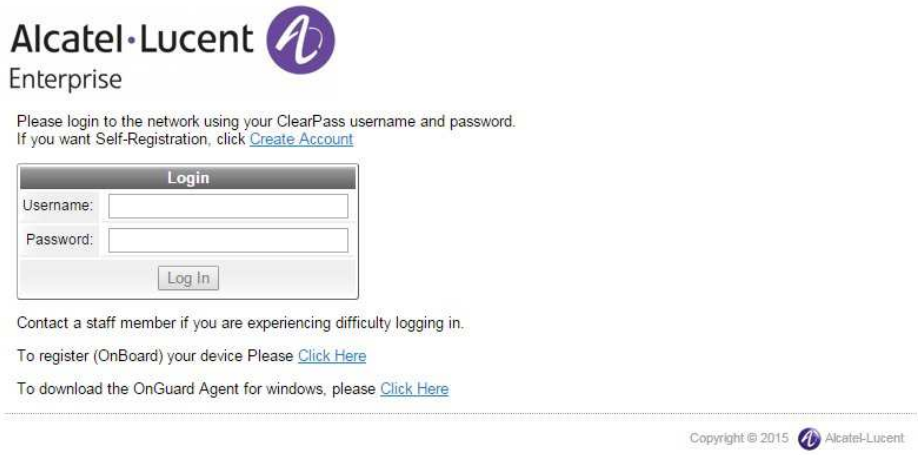
Performing the Demo

Setting up the Client PC:

The Client PC requires the OnGuard agent installed locally. If not already installed, follow these steps:

1. Connect to the MDN_Captive_1 SSID
2. Open a web browser and navigate to a URL
3. Accept any security warnings

4. On the Captive Portal Landing page, at the bottom, there is a link where you can download the OnGuard agent:



5. Install and run the OnGuard Agent.

NB: The version of the OnGuard agent must match the version of the CPPM server. Therefore, if you already have the agent installed on the client PC, ensure that it is the same version as the CPPM server. If in doubt, remove the existing installation, and reinstall using the steps above.

Setting up the Admin PC:

Use the Admin PC to show the change in role given to the client (alternatively, just open a web browser on the client PC after connecting to the MDN_Secure_1 SSID).

Connect to the MDN_OPEN (password: alcatel1) and open a web browser to show the Controller GUI:

https://192.168.8.239:4343

Accept any security warnings, and login as admin:

User: **admin**
Pass: **AlU-966%f**

1. Click on 'Monitoring' at the top of the page.
2. On the left-hand-side under 'WLAN' click on 'MDN_Secure_1'.
3. On the right-hand-side pane, click on 'Clients'.

The demo Steps:

Step 1:
Connect to the **MDN_Secure_1** SSID:

Use the following username/password combination:

Username	Password
local1	**alcatel**

You should see a notice on the bottom right of the screen indicating that the client is 'Healthy':

In addition, if you open the OnGuard Agent, you will see the same message in the Agent's Connection Details page:

Step 2:

Open web browser to show Internet access, to check that you have network connectivity:

Step 3:

On the Admin PC (or client PC if only using 1 PC) show the role given to the user:

Search Results

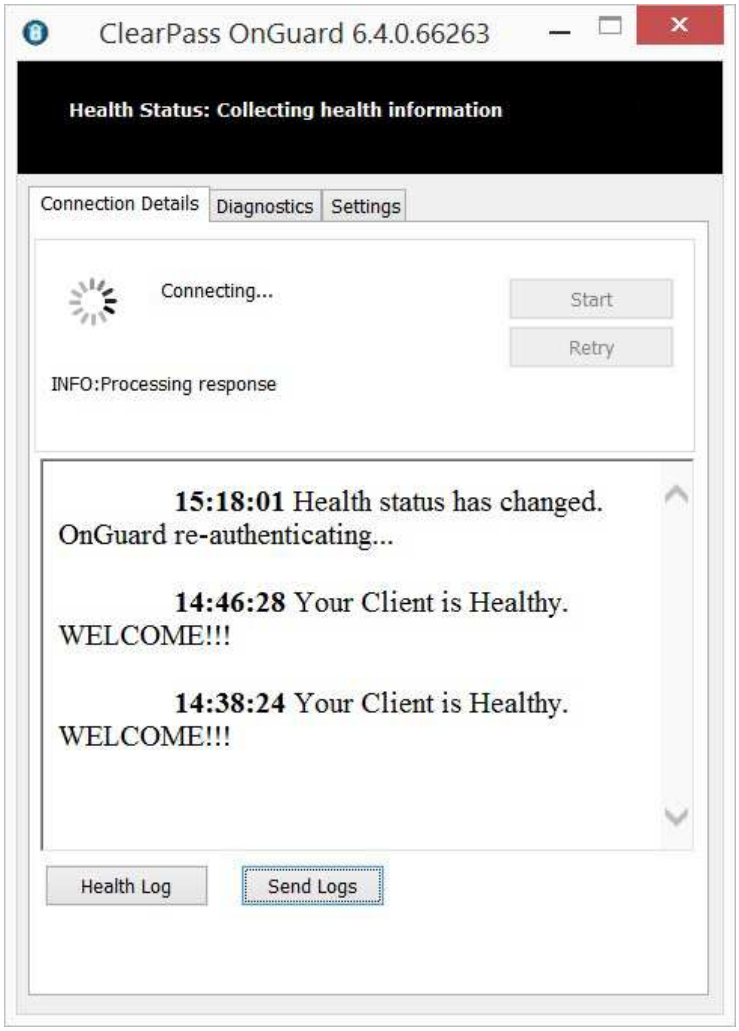
Clients All | IPv4 | IPv6

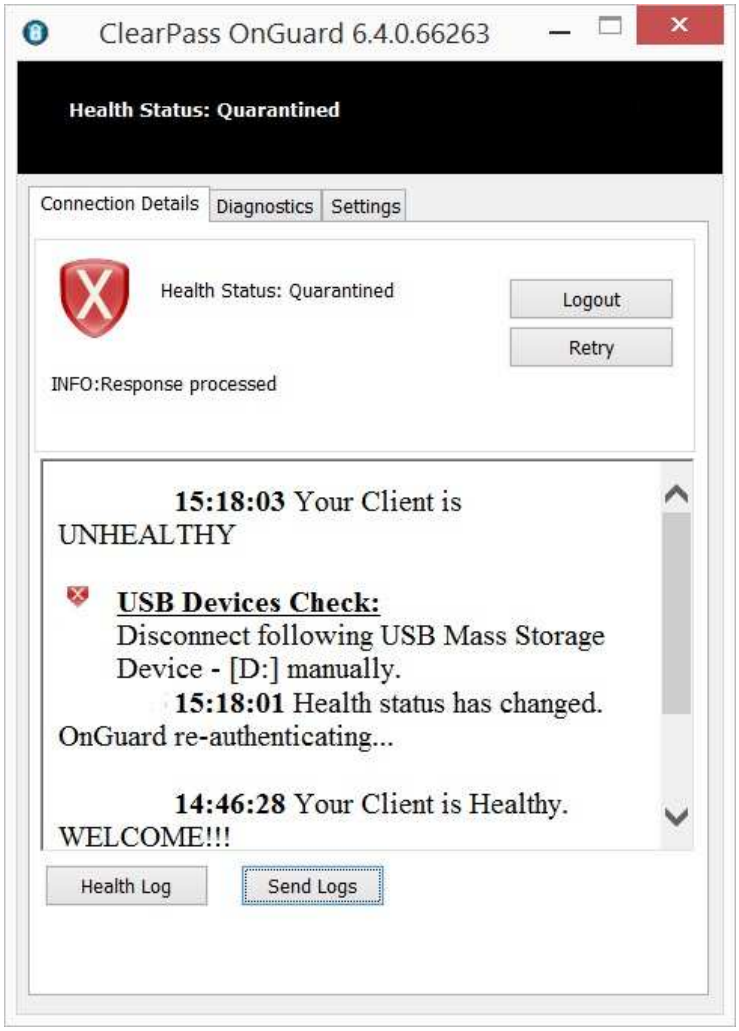
	User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
○	local1	Windows	0c:8b:fd:2e:c7:23	192.168.8.101	byod-presales	802.1x	MDN_Secure_1

"This is the role given to this user while on this network and with a PC that conforms to the security policy."

Step 4:
While the OnGuard Agent is visible, insert a USB key into the client PC.

The OnGuard Agent will, after a few seconds delay (potentially up to 45 seconds...) start to scan the PC and collect a new health report, which it then sends to the CPPM server:





"We can send a message to the user when their PC becomes out-of-compliance, informing them of the problem, and perhaps with instructions on what to do to remedy the problem."

Step 5:

Switch to the Admin view, and show that the client status has changed. It should look something like this:

Search Results

Clients All | IPv4 | IPv6

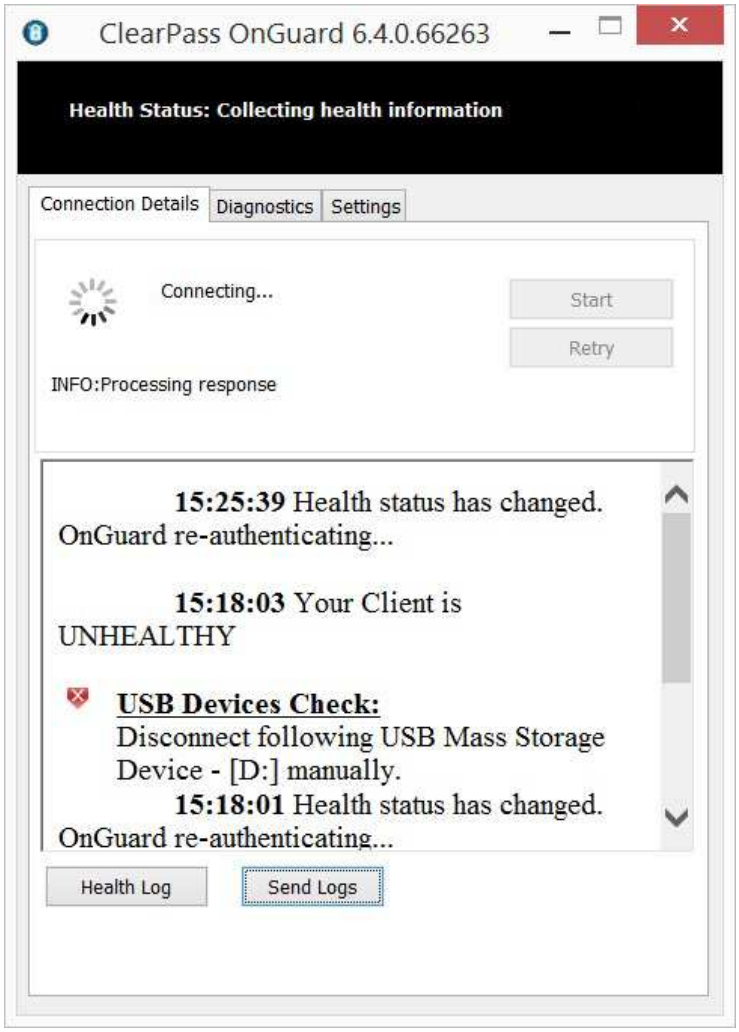
	User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
○	local1	Windows	0c:8b:fd:2e:c7:23	192.168.8.101	byod-unhealthy	802.1x	MDN_Secure_1

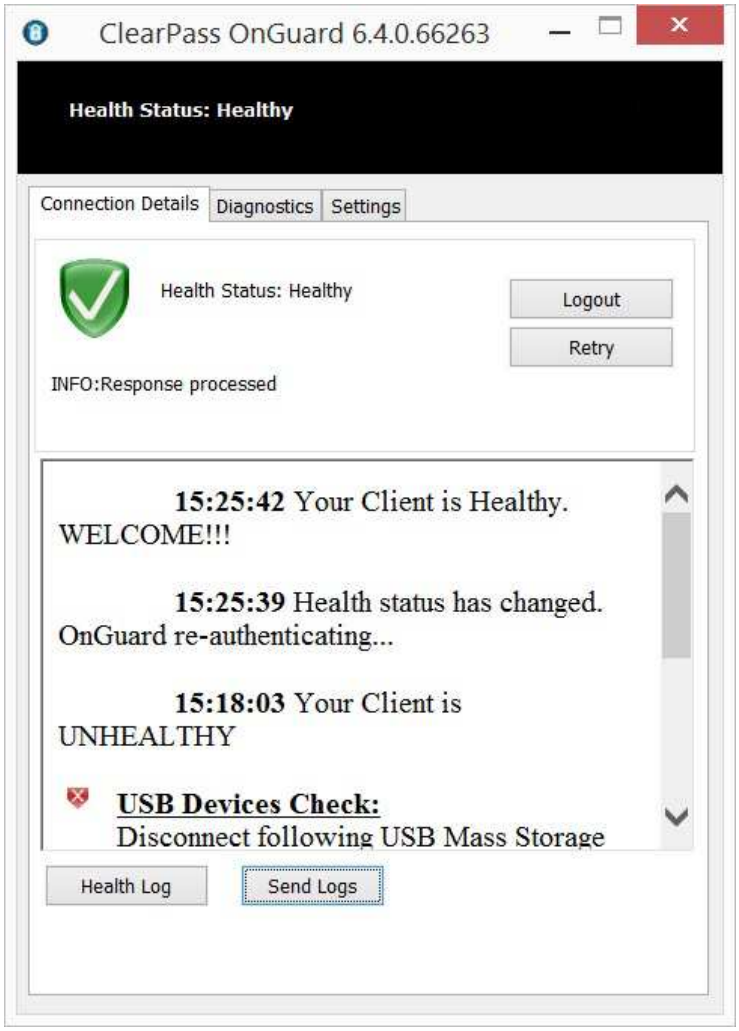
"Here we can see that the role for this user has changed – we now have an 'unhealthy' role. This is done dynamically, without admin intervention and seamlessly for the client."

Step 6:

Remove the USB key from the client PC.

After a short delay, the Agent will detect the change, scan the PC and communicate this to the CPPM server:





"Removing the USB key will trigger a scan of the client and the agent will send this information to the CPPM server, which in turn will send a new role to be given to the user on the Controller.

Step 7:

Show the Admin view again, indicating that the user is once again in their default role:

Search Results

Clients All | IPv4 | IPv6

	User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
○	local1	Windows	0c:8b:fd:2e:c7:23	192.168.8.101	byod-presales	802.1x	MDN_Secure_1

Conclusions and Additional Notes

Remember that if you are not able to use a USB key for whatever reason, that notepad.exe will also trigger a health check and quarantine the client PC (On a Windows 7 PC).

Contacts

NBE contact for all aspects of the demo platform:

Mike Dann
mike.dann@al-enterprise.com