SE ClearPass Remote Demo
Wired Guest Self-Registration

Table of Contents

Introduction

This is a step-by-step guide on how to perform the Wired Guest Self-Registration Access 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. Wired Client PC (Windows)
2. Admin PC (Wired or Wireless) with an SSH client (e.g. putty)
3. Pre-provisioned RAP (see the 'SE ClearPass Remote Demo - Platform Information' documentation for details on how to provision the RAP)
4. OS6850E or OS6855 running AOS6.4.6R01 or later

Having 2 PCs is not mandatory but is strongly recommended. Switching between an 'end-user' view and 'admin' view will break-up the demo's flow and having the possibility of showing what's happening on the administration side while performing the client actions will significantly improve the audience's demonstration experience.

This demo script was written using 'Windows 7' as the Client PC OS. Warnings and options may differ if using another version of windows.

Performing the Demo

This demo shows 'Wired Guest Self-Registration', one of the Guest options available in ClearPass.

In a wired context, this type of access would be used in meeting rooms or where a wireless access is not possible or available.

We still have control over what sort of information is required to be given before network access is granted. This can be used in conjunction with URL proxies or filters to log URL activity, a legal requirement in some countries.

However, in a wired context this might not be as important, as the 'owner' of the access port (the Enterprise) can decide who has access in that physical access to the port is required to plug-in the cable.

The demo flow is summarised as follows:

1. Setup the Client PC
2. Connect the Client PC to the switch
3. Launch a web browser
4. Get redirected to a captive portal
5. Click on the Self-Registration Link
6. Fill-in the form
7. Download the login details
8. Access the Internet

Setting up the Wired Environment

Please refer to 'SE ClearPass Remote Demo - Platform Information' document for information relating to the switch setup.

Setting up the Client PC

Ensure that if the wired auto configuration service is running (i.e. you have the 'Authentication' tab visible in the Ethernet properties) that authentication is *unchecked*.

The port on the switch is configured so that if it detects a non-supplicant, it will redirect the user to the Captive Portal; otherwise the port will expect an 802.1x challenge.

On the Client PC:

Step 1:
Connect the client PC to port 3 or 5 on the switch

NB: WINDOWS 8.1 Clients:
(On Windows 8.1, you may have your default browser open. If after accepting the certificate warnings you do not get redirected to the Captive Portal, close the browser, open another one and go to an HTTP:// web site – avoid HTTPS://

Additionally, if you have installed the OnGuard Agent, you may have a second browser page appear after the OnGuard Agent communicates with the CPPM server (the CoA packet received by the switch may force a reset of the session – as if you had plugged in the cable a second time)). Exit the OnGuard Agent.

Step 2:
Open web browser and go to a URL:

Step 3:
Accept any Certificate warnings

"The reason we have a security certificate warning is because the ClearPass server has a self-signed certificate. In a production environment, it is very important to have a security policy that covers certificates. We can help build this into our offer if necessary."

Step 4:
Arrive at the Captive Portal landing page:

"Our Captive Portal has links to the Self-Registration process at the top, a link to download the OnGuard Agent (detailed in another demo) and a link to the OnBoard process (detailed in another demo)."

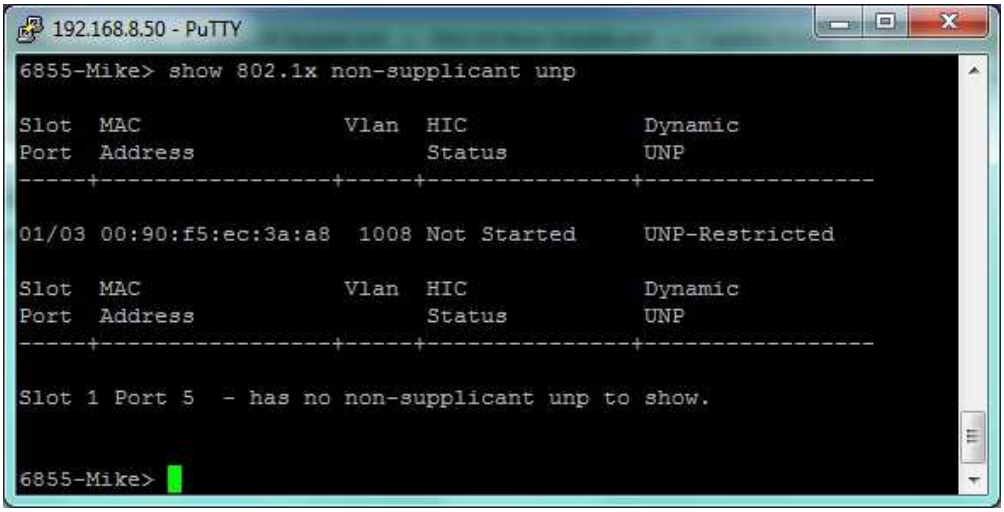
On the Admin PC:

Show the UNP given to the user by connecting to the switch via SSH:

Username	Password
admin	**switch**

And issue the following command:

```
> show 802.1x non-supplicant unp
```

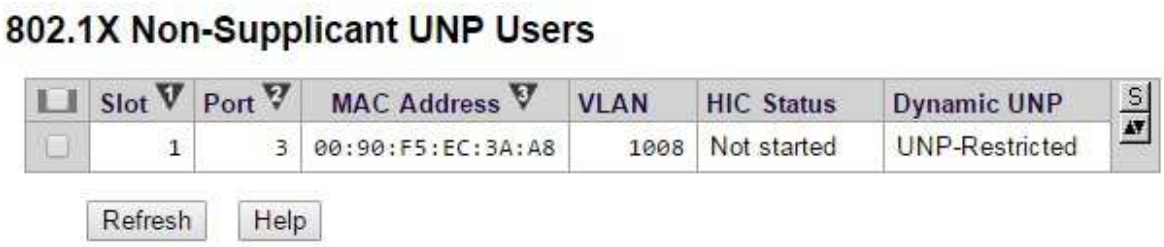


Alternatively, you can show the same information via the Webview GUI. Open a web browser (NOT IE!) and go the https address of your switch. Accept any warnings, and login with the same credentials as above.

Navigate to the following page:

Security -> Access Guardian -> 802.1x Non-Supplicant -> UNP

You should see that the user on port 1/3 has a dynamic NP of UNP-Restricted:

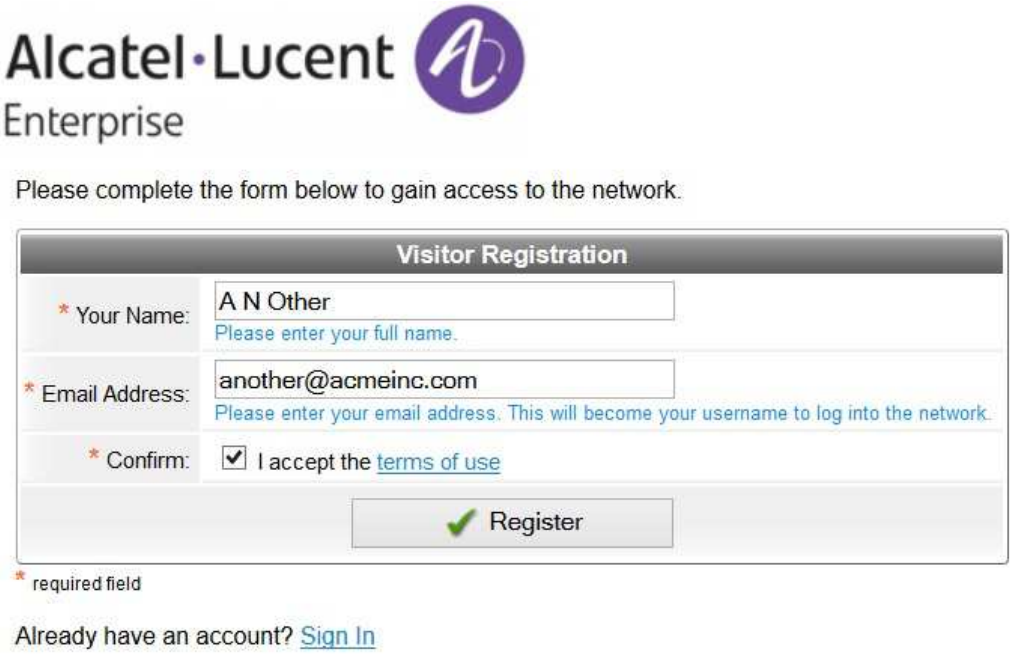


Step 5:
Click on "Create Account" link and arrive at the Self Registration Portal Form:

Insert the following information:

1. Your Name: *(insert anything here)*
2. Email Address: *(insert anything conforming to an e-mail syntax)*
3. Click on the check box to accept the terms and conditions
4. Click on "Register"

"The form we see can be customised to add other information that you would like the user to enter"



Step 6:
On the Admin PC, connect to the **MDN_OPEN** SSID (password: alcatel1) or connect to port 7 on the switch.

Go to the following address: `http://192.168.111.100` ignore any certificate warning.

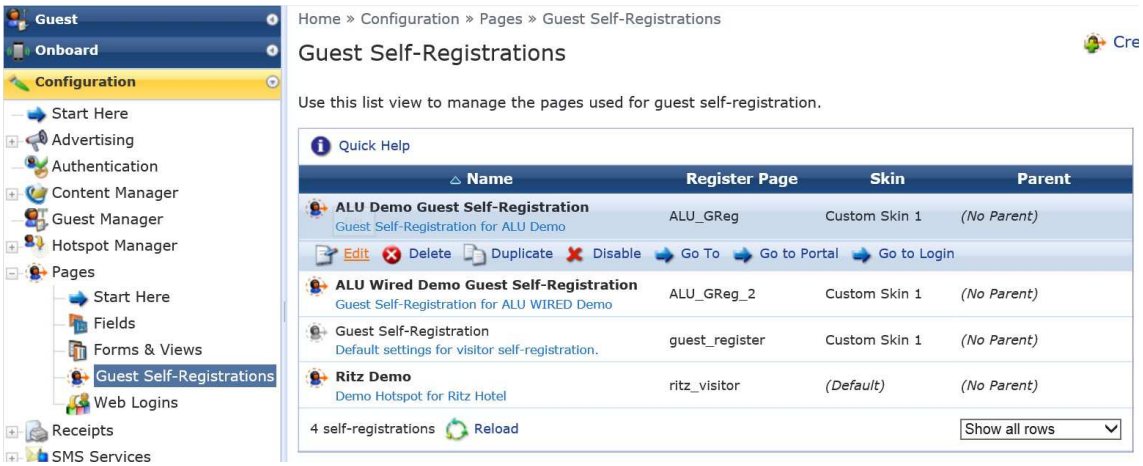
Click on the "ClearPass Guest" application:

Login to the CPPM with the following credentials:

Username: **`admin`**
Password: **`eTIPS123`**

Step 7:
In the new page, navigate to “Configuration -> Pages -> Guest Self Registrations”.

On the right-hand-side, select “**ALU Wired Demo Guest Self-Registration**” and click on “Edit”:



Step 8: The next page is the form page used to customise the different aspects of self registration.

Explain the following to the customer:

"This page gives us access to the different options of the Guest Self Registration module.
Here we can choose skins, what information is required to gain network access, a redirect URL (if desired) and so on."

Continue with this page if required.

Step 9: On the Client PC on the User Receipt page, click on "**Download Account Details**":

"We have the option of sending the user's details via SMS (by integrating with an existing SMSC service – not provided by ClearPass) or via e-mail using the company's e-mail service. Here we download the details into a text document which we can save on our local machine."

Once downloaded, click on **Log In**.

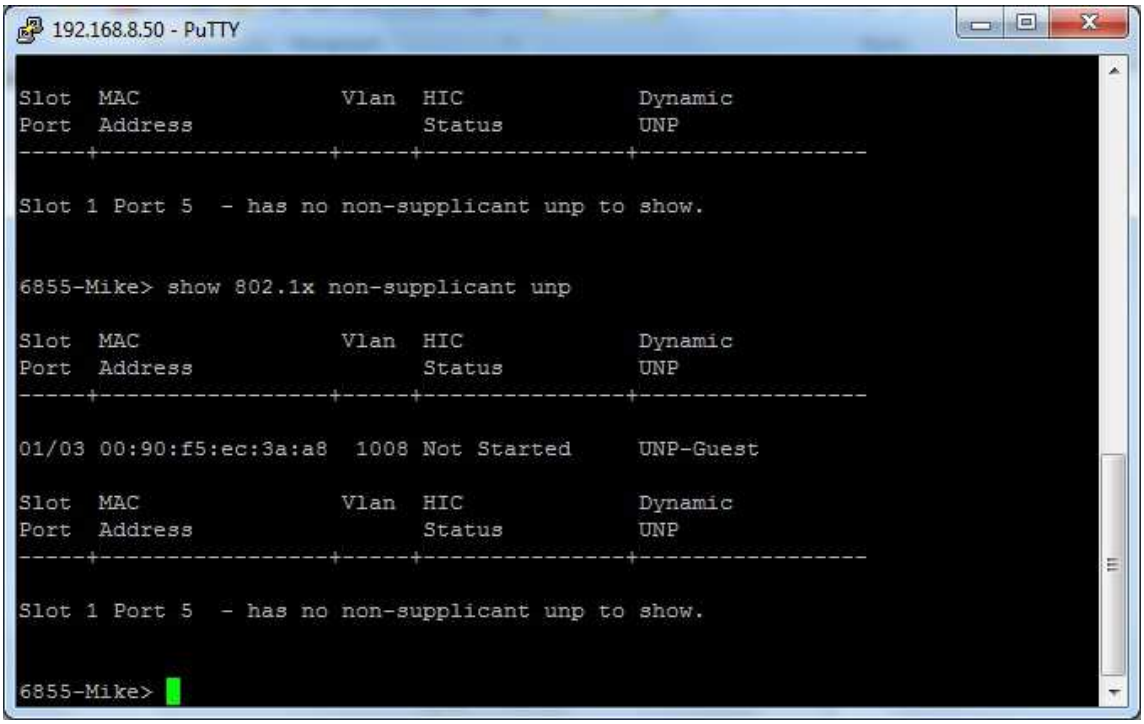
A redirect page informing the user that they have been authenticated:

You will be redirected to ALE's Internet homepage.

Step 10:
Show the new UNP given to an authenticated guest user:

SSH to the switch and issue the command:

```
> show 802.1x non-supplicant unp
```

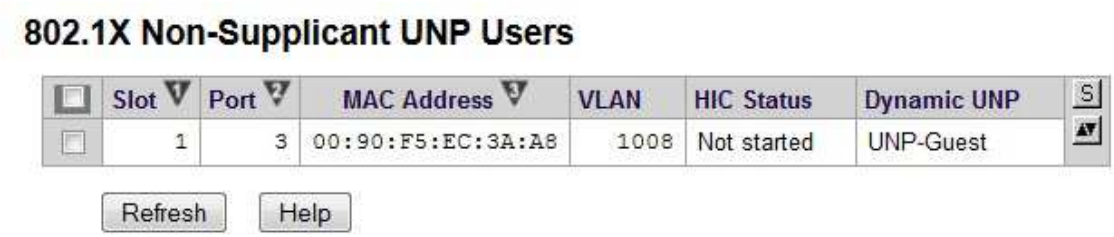


Alternatively, you can show the same information via the webview GUI. Open a web browser (NOT IE!) and go the https address of your switch. Accept any warnings, and login with the same credentials as above.

Navigate to the following page:

Security -> Access Guardian -> 802.1x Non-Supplicant -> UNP

You should see that the user on port 1/3 has a dynamic NP of UNP-Restricted:



"Notice that the Dynamic UNP for the newly created user is now UNP-Guest. We have dynamically changed the UNP allowing the user those rights we deem correct for that type of access."

Contacts

NBE contact for all aspects of the demo platform:

Mike Dann
mike.dann@al-enterprise.com