SE ClearPass Remote Demo
Wireless Guest Self-Registration

Table of Contents

Introduction

This is a step-by-step guide on how to perform the 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. End-Client PC
2. Admin PC
3. Pre-provisioned RAP

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 'Guest Self-Registration', one of the Guest options available in ClearPass.

This type of guest access is usually deployed in a large scale environment where there will be a high number of transient users, and control over who has access is not a priority (Exhibition halls, Stadiums, Conventions etc).

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.

On the Client PC:

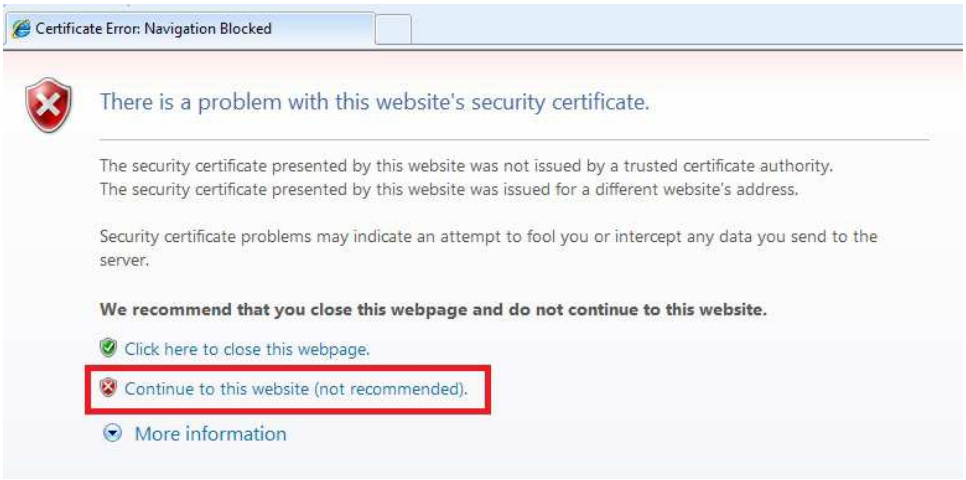
Step 1:
Ensure that if you have previously installed the OnGuard agent that it is no longer running. Connect to the **MDN_Capture_1** SSID:

NB: If using Windows 8.1, you may have your default web browser open straight to the Captive Portal. CLOSE THIS WINDOW. Open a web browser, and follow the instructions below.

The reason is that the redirect at the end of the registration process *may not work* resulting in an error.

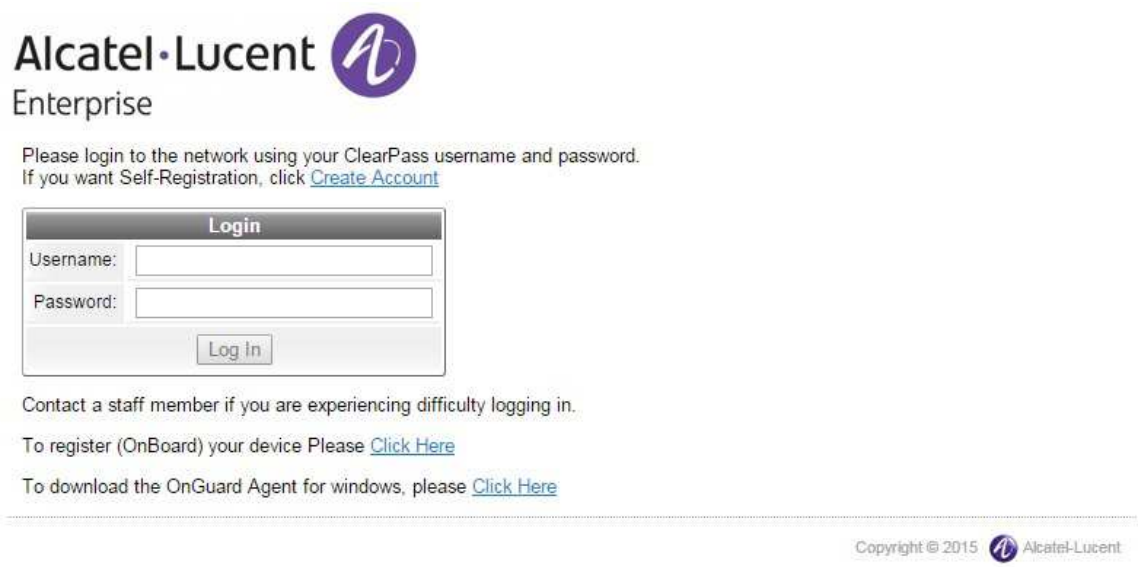
Step 2:
Open web browser and go to a URL:

Step 3: Accept the Certificate warning:



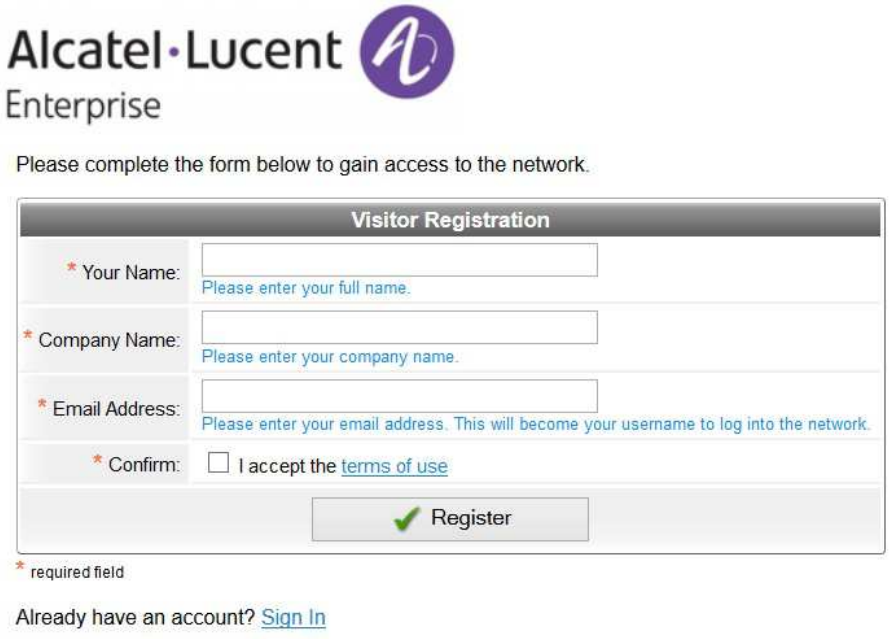
"The reason we have a security certificate warning is because the ClearPass has a self-signed certificate and this PC has not been configured to trust the signing CA. During a production deployment, it is important to have defined or to define a security policy that covers certificates. We can help build this into our offer if necessary."

Step 4:
Arrive at Guest Access Login page:



"The landing page allows us to enter our credentials (if we have already registered and our cache timeout has expired) or click on the 'Create Account link to start the registration process"

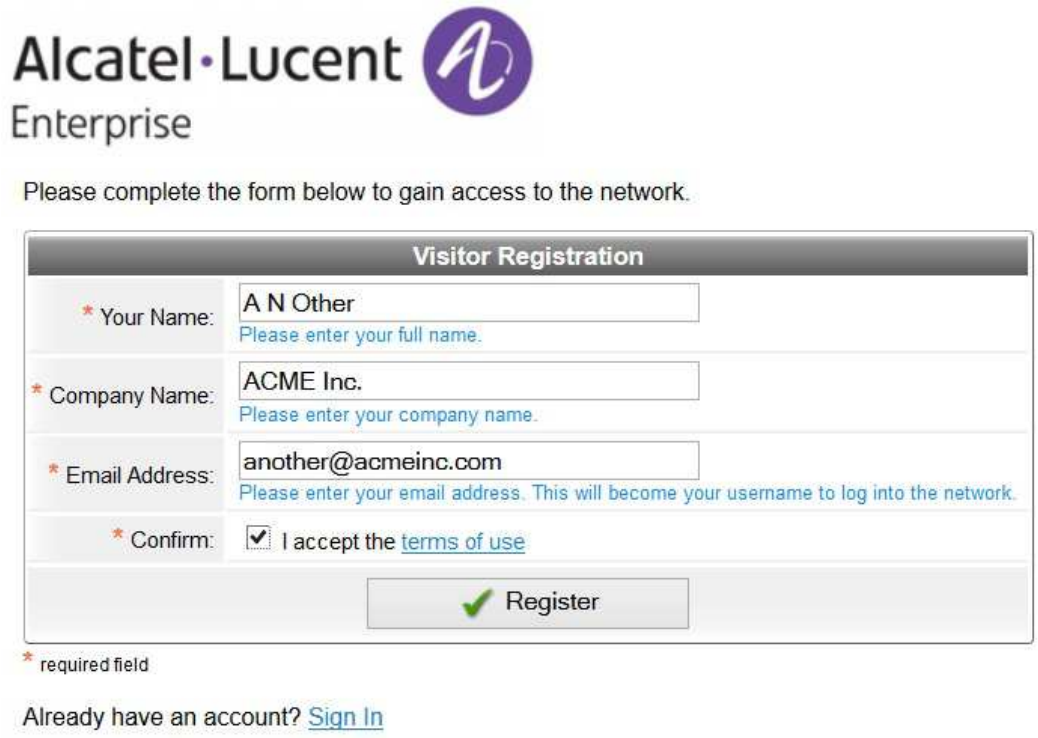
Step 5:
Click on "Create Account" link and arrive at the Self Registration Portal Form:



Insert the following information:

1. Your Name: *(insert anything here)*
2. Company Name: *(insert anything here)*
3. Email Address: *(insert anything here)*
4. Click on the check box to accept the terms and conditions
5. 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).

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

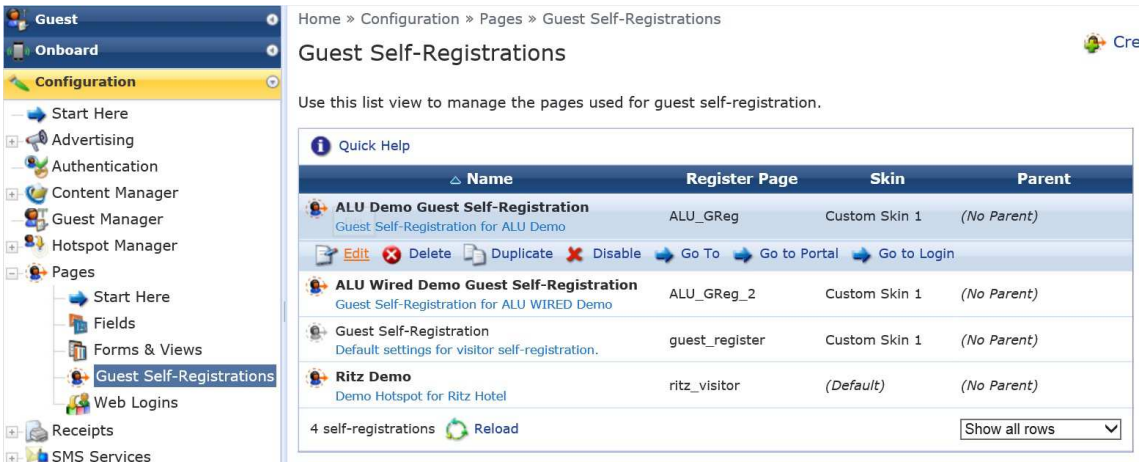
Click on the “ClearPass Guest” application:

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 Demo Guest Self Registration” and click on “Edit”:



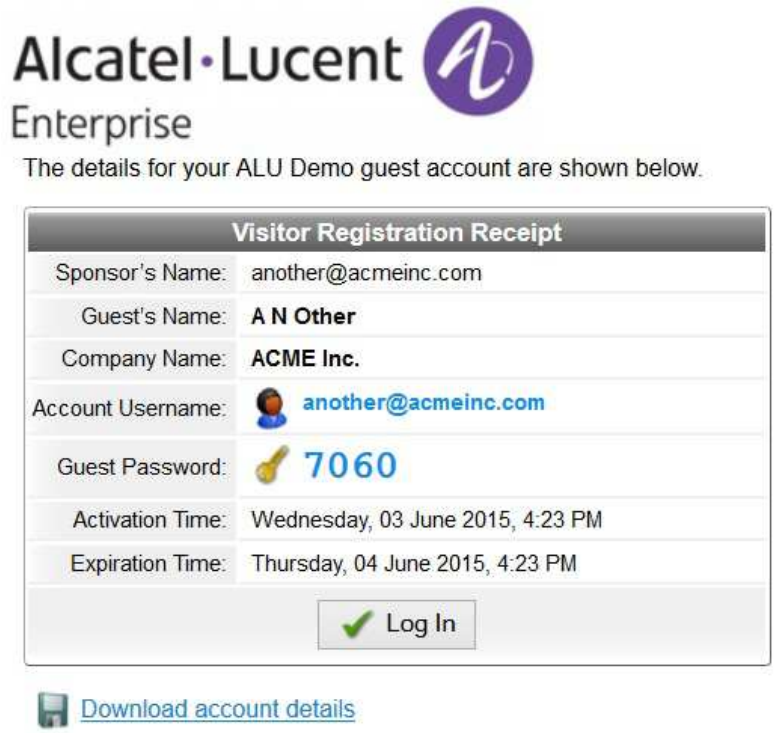
Step 8: The next page is the form page used to customise the different aspects of self registration.

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.

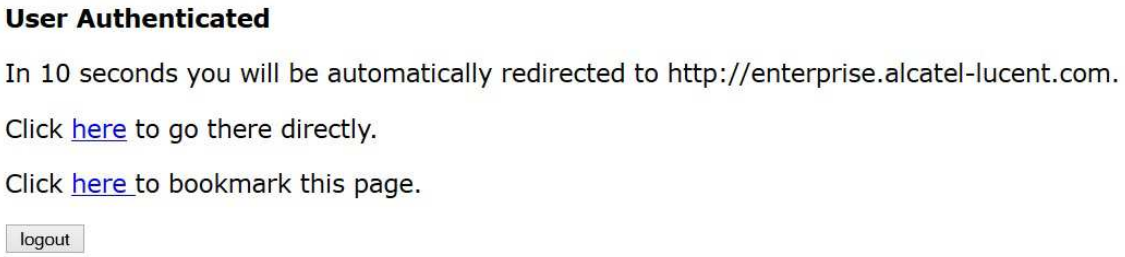
Step 9: On the Client PC on the User Receipt page, click on "**Download Account Details**":



"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 session timeout which forces the user to reauthenticate:

"Having a session timeout protects the user's credentials so that if they are absent from their computer, someone else cannot use the access.

For the purposes of this demo, we have a 1-minute timeout configured allowing us to speed-up the demo. However, in a production environment, this would be set to a higher value 10-20 minutes"

1. Disconnect from **MDN_Capture_1** network.
2. Wait 1 minute.
3. Connect to **MDN_Capture_1**
4. Open web browser and navigate to a URL.

You will be re-directed to the Guest Management page. You can insert the credentials that were saved earlier in **Step 9**, or end the demo.

Contacts

NBE contact for all aspects of the demo platform:

Mike Dann
mike.dann@al-enterprise.com