Configuring Cisco Wireless LAN Controllers

September 4, 2014

The CMX design guide uses Cisco 5508 Series and Flex 7510 Series Wireless LAN Controllers (WLCs) with version 8.0 code.

To get started, follow the WLC 5508 8.0 configuration design guidelines at: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_010.html.

Note The NTP server should be the same one that you will use for the FastLocate feature with the Wireless Security Module (WSM).

To configure basic guest access with a foreign and anchor controller, follow the design guidelines at: http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2014/CVD-CampusWirelessLANDesignGuide-APR14.pdf.

Once the Wireless LAN Controller has been setup, follow the instructions below to configure a wireless network for Visitor Connect.

WLC Visitor Connect Configuration

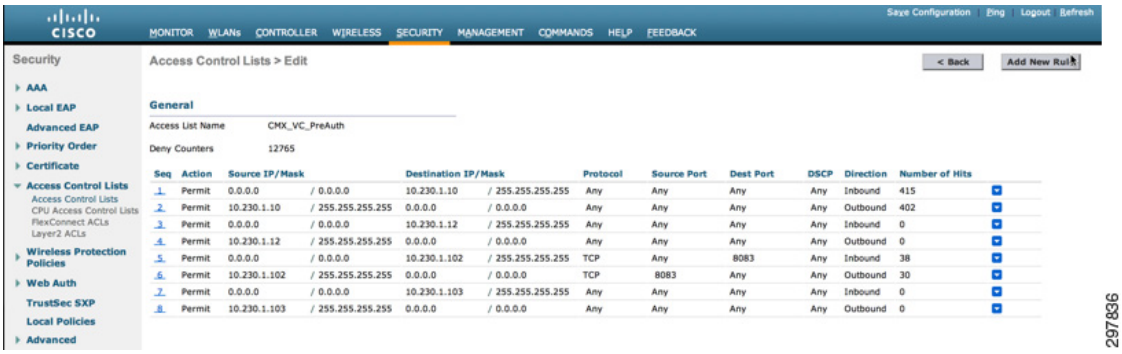
The Visitor Connect configuration on the WLC 5508 consists of two parts:

1. Configuring a pre-authentication ACL on the controller. The pre-authentication ACL causes the wireless LAN controller to redirect all HTTP traffic to the MSE, except traffic which is permitted within the ACL. DNS and DHCP traffic are allowed through in the ACL, as well as traffic destined to the TCP port of the MSE which runs the Visitor Connect service.
2. Configuring Web Passthrough using an external server (pointing to the MSE running CMX Visitor Connect) on the B2C Guest WLAN for Layer 3 security.

Configuring the ACL for CMX Visitor Connect

Configure the pre-authentication ACL on the Cisco 5508 Series WLC, as shown in Figure 23-1.

Figure 23-1 Configure WLC ACL for CMX Visitor Connect



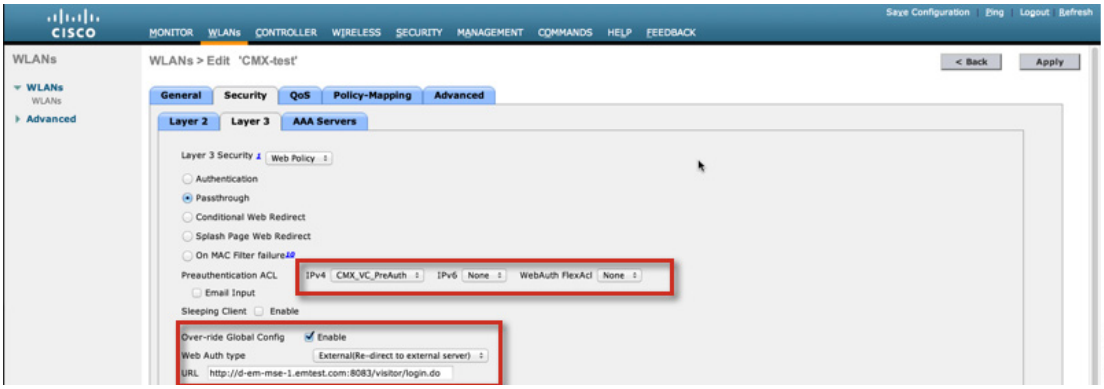
CMX Visitor Connect with Splash Pages & Social Connectors uses port 8083 on the MSE. The example pre-authentication ACL permits (does not redirect) traffic from any host destined for TCP port 8083 of the IP address of the MSE server. Implicitly any traffic not specifically allowed (permitted) is redirected to the MSE running CMX Visitor Connect. This prevents web session traffic already destined for the MSE running CMX Visitor Connect from being re-directed by the wireless LAN controller. In addition DNS and DHCP traffic are typically not redirected via additional access control entries (ACEs) within the pre-authentication ACL.

Note In the design presented in this guide, guest traffic is terminated on a dedicated guest wireless LAN controller sitting on a DMZ segment of an ASA firewall. The ASA firewall security policy should also be configured to only allow guests who are using CMX Visitor Connect to access TCP port 8083 of the MSE which runs CMX Visitor connect.

Configuring the WLAN for Visitor Connect

Figure 23-2 shows an example of the configuration of Web Passthrough using re-direction to an external server for the guest WLAN for CMX Visitor Connect. Additionally, Figure 23-2 shows the application of the pre-authentication ACL to the guest WLAN.

Figure 23-2 Configuring the B2C Guest WLAN for CMX Visitor Connect with Splash Pages



To configure Web Passthrough Using Re-direction for CMX Visitor Connect:

Step 1 On the Security Layer 3 tab, from the drop-down menu next to Layer 3 Security, select **Web Policy**.

Step 2 Select the **Passthrough** checkbox as the type of web policy.

Step 3 Select the name of the IPv4 Pre-authentication ACL configured in the previous section from the drop-down menu next to Pre-authentication ACL.

Step 4 In the drop-down menu next to Web Auth type, select **External** (Re-direct to external server).

Step 5 Configure the External Redirect URL to point to the URL:

http//<IP_Address_or_Name_of_MSE_Server_running_Visitor_Connect>:8083/visitor/login.do

This redirects web traffic to the CMX Visitor Connect service running on TCP port 8083 of the MSE server.

Step 6 Click the **Apply** button at the top right corner of the page to apply and save the changes.

Configuring FastLocate

FastLocate requires WSM modules to be installed on all access points deployed within the site. This section discusses enabling FastLocate directly on a Cisco 5508 Series WLC. Note that you can also use Cisco Prime Infrastructure to enable FastLocate by using templates to enable it on multiple Wireless LAN Controllers.

To configure FastLocate:

Step 1 Ensure that the switches to which the APs with WSM modules will be connected support POE+ or Enhanced POE.

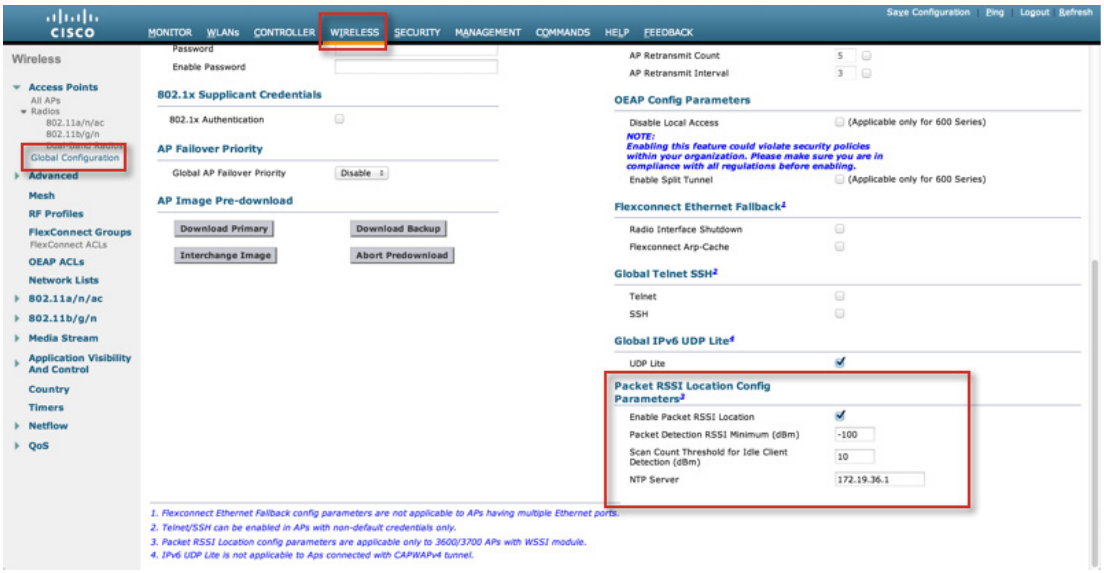
Step 2 Ensure that a valid NTP source has been configured on the WLC.

Step 3 Insert WSM modules into the APs and attach them to POE+ or Enhanced POE switch ports.

Note The reference Installation for the WSM is available at: http://www.cisco.com/c/en/us/support/docs/wireless/aironet-3600-series/115612-Aironet-Access-Point-Module-for-WSSI-Guide-00.html.

Step 4 Establish an HTTPS session to the WLC which controls the APs. Navigate to **Wireless > Access Points > Global Configuration**. Within the Global Configuration page, scroll down to the Packet RSSI Config. Parameters section. An example is shown in Figure 23-3.

Figure 23-3 Configuring FastLocate



Step 5 Click the checkbox next to **Enable Packet RSSI Location**. Leave other details at their default. Configure the IP address of the NTP server that is accessible by the WLC and APs.

Note The Scan Count Threshold for Idle Client Detection (dBM) field represents the number of off-channel scan cycles the AP waits before sending a Block Acknowledgement Request (i.e., BAR) to idle clients. The default value of 10 corresponds to approximately 40-60 seconds, depending on the number of channels in the off-channel scan cycle and whether Cisco CleanAir® has been enabled.

Step 6 Click **Apply** to save the changes and enable FastLocate.

Note FastLocate should be enabled on all WLC. It is possible to do this via Templates using Prime Infrastructure 2.1, however it is not described in this guide.