CMX Security Considerations

September 4, 2014

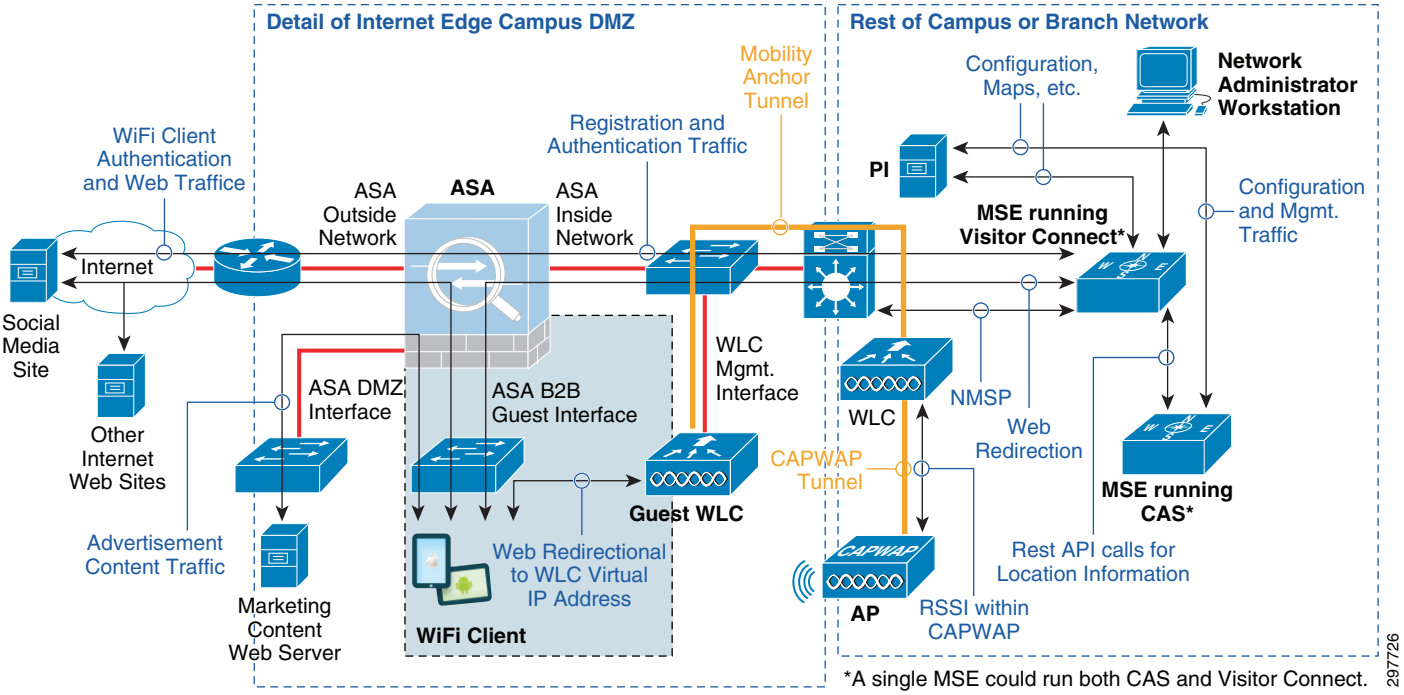
This chapter focuses on traffic isolation for guest wireless access as part of CMX Visitor Connect. Additionally, it discusses Role-Based Access Control (RBAC) for the Mobility Services Engine (MSE) as well as the CMX Connect & Engage service.

Traffic Isolation for CMX Visitor Connect

With CMX Visitor Connect, guests must be allowed to authenticate to the network using credentials from social media sites, such as Facebook, LinkedIn, and Google+. This involves the use of a variation of the OAuth protocol along with the MSE. Hence the MSE which runs CMX Visitor Connect must be reachable by guests. However all other guest traffic (other than DHCP and DNS) should be isolated from the rest of the corporate network. Guests are only allowed to access the Internet in this design.

Figure 5-1 shows at a high-level the hardware and various flows involved in CMX Visitor Connect.

Figure 5-1 Hardware and Information Flows for CMX Visitor Connect



With this design, traffic isolation is primarily achieved via policy configured on the ASA firewall operating as a Layer 3 firewall within the Internet Edge DMZ. Note that virtualization of the network infrastructure is not utilized in this design to isolate guest traffic.

The following interfaces are configured on the ASA firewall for this design example:

- ASA Inside Interface—This has the highest security level. The IP addressing is assumed to be private and part of the enterprise organization for this design. An example policy for the ASA Inside Interface is as follows:
  - Allow all traffic from all devices initiated from any subnet reachable via the ASA Inside Interface to all devices which are reachable via any lower security level interfaces (ASA DMZ Interface, the ASA B2C Guest Interface, and the ASA Outside Interface). The ASA firewall should allow return traffic from any lower security interface back to a higher security interface, as long as the session was initiated from a device on the higher security interface. This allows the necessary connections from the MSE to social media sites for authentication for CMX Visitor Connect.
  - It is assumed for this design that NAT is not used between the ASA Inside Interface and the ASA DMZ Interface or the ASA B2C Guest Interface.
  - It is assumed for this design that NAT is used between the ASA Inside Interface and the ASA Outside Interface since the ASA Outside Interface has a publicly routable IP address.
- ASA Outside Interface—This has the lowest security level. The IP addressing is assumed to be publicly routable in this design. An example policy for the ASA Outside Interface is as follows:
  - Block all traffic from all devices initiated from any subnet reachable via the ASA Outside Interface to all devices which are reachable via any higher security level interfaces (ASA DMZ Interface, the B2C Guest Interface, and the ASA Outside Interface). This effectively blocks any sessions initiated from the Internet from reaching any resources within the corporation, while still allowing return traffic from any sessions initiated from within the corporation out to the Internet.

  - It is assumed that NAT is used between the ASA Outside Interface and the ASA DMZ Interface, the ASA B2C Guest Interface, and the ASA Inside Interface for this design.

- ASA B2C Guest Interface—This has a security level below the ASA Inside Interface and the ASA DMZ Interface, but above the ASA Outside Interface for this design. The IP addressing is assumed to be private and part of the enterprise organization. An example policy for the ASA B2C Guest Interface is as follows:
  - Allow inbound DNS from any device with a source IP address on the ASA B2C Guest Interface subnet to the corporate DNS server located on a subnet available via the ASA Inside Interface.
  - Allow inbound traffic from any device with a source IP address on the ASA B2C Guest Interface subnet destined to TCP port 8083 of the IP address of the MSE which is running CMX Visitor Connect. This is necessary for the redirection of the B2C guest web browser to CMX Visitor Connect running on the MSE during the authentication via social media sites process.
  - Allow inbound traffic from any device with a source IP address on the ASA B2C Guest Interface subnet destined to TCP port 80 (HTTP) of the IP address of the Marketing Content Server which is sitting on the ASA DMZ Interface. This is necessary for allowing the B2C guest browser to access any advertisement content on the Marketing Content Server without allowing the B2C guest device onto the inside of the corporate network. The ability to display advertisement content on the B2C guest device is an optional step in the three-step Visitor Connect process.
  - DHCP should be configured to be relayed by the dedicated Guest WLC to a DHCP server located on the inside of the corporate network. In this configuration, the Mgmt. Interface of the Guest WLC is the source IP address used by the DHCP relay function. Hence the Mgmt. Interface of the Guest WLC needs to have an IP address which is part of the corporate address space reachable via the ASA Inside Interface. In this configuration, the ASA B2C Guest Interface should not need to include an access entry allowing inbound DHCP traffic to the ASA Inside Interface.
  - By default allow all traffic from all devices initiated from any IP address on the ASA B2C Guest Interface subnet to all devices which are reachable via any lower security level interfaces (ASA Outside Interface is the only lower security interface). This allows B2C guests to access the Internet and perform authentication to the social media sites as part of CMX Visitor Connect.
  - It is assumed that NAT is not used between the ASA B2C Guest Interface and the ASA DMZ Interface, or the ASA Inside Interface.
  - It is assumed that NAT is used between the ASA B2C Guest Interface and the ASA Outside Interface since the ASA Outside Interface has a publicly routable IP address.
- ASA DMZ Interface—This has a security level below the ASA Inside Interface, but above the ASA B2C Guest Interface and the ASA Outside Interface. The IP addressing is assumed to be private and part of the Enterprise organization. The ASA DMZ Interface is assumed to house the Marketing Content Web Server. Note that in an actual deployment, the marketing content may be deployed in the cloud and accessible from the Internet, rather than onsite on a DMZ server. Hence this may be optional. An example policy for the ASA DMZ Interface is as follows:
  - By default block all traffic initiated from any device with a source IP address on the ASA DMZ Interface subnet to any other interface. The Marketing Content Web Server is supposed to respond to HTTP requests for marketing content, not generate any requests on its own. This should still allow the Marketing Content Web Server to respond to HTTP requests for content which are initiated from devices on the ASA B2C Guest Interface subnet.
  - It is assumed that NAT is not used between the ASA DMZ Interface and the ASA Inside Interface or the ASA B2C Guest Interface.
  - It is assumed that NAT is used between the ASA DMZ Interface and the ASA Outside Interface since the ASA Outside Interface has a publicly routable IP address.

Note that locking down the ASA firewall such that guests using CMX Visitor Connect can only access TCP port 8083 is a necessary step for securing the overall CMX deployment. The MSE may be running multiple services, including the Context Aware Service (CAS) and CMX Analytics. Hence tight network access control along with role-based access control to the MSE is recommended to minimize chances of unauthorized access to the MSE.

Role-Based Access Control on the MSE

The MSE itself has its own role-based access control (RBAC) separate from the CMX Connect & Engage service. Role-based access control on the MSE controls access to administrative functions on the MSE itself, as well as access to CMX Analytics (both Location and Presence). For role-based access control of the CMX Connect & Engage service, see Role-Based Access Control for the CMX Connect & Engage Service.

Services such as CMX Analytics are intended to be utilized by non-IT personnel. For example, in a retail deployment, store operations managers may need to access the MSE running CMX Analytics to view the dashboard, run reports, or run custom analysis. However IT personnel should be the only ones allowed to modify the configuration of the services running on the MSE and shutdown or restart the MSE. Hence the implementation of role-based access control is considered an essential security measure to mitigate the chances of any accidental or malicious disruption of the services (CMX and/or CAS) provided by the MSE.

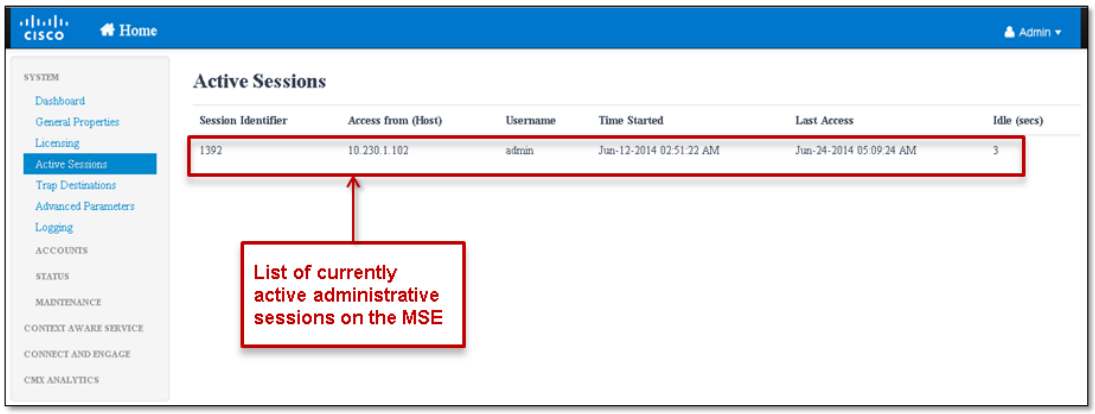
Role-based access control (RBAC) consists of configuring one or more Groups on the MSE with one of the following three access-control privileges—Read Access, Write Access, or Full Access. Individual Users are then created and assigned to one of the Groups. All Groups and Users reside on the local database within the MSE. There is no integration with an external data store, such as an LDAP database or external RADIUS server.

As of MSE version 8.0, it is not recommended to utilize Read Access groups on the MSE. CMX Presence Analytics currently does not participate in Role-Based Access Control (RBAC) on the MSE. Hence any userid which is part of a Read Access group is also able to add/modify/delete CMX Presence Analytics configuration. Note that the use of only Write Access and Full Access groups means that any non-IT personnel who require access to the CMX Analytics dashboard, analytics tab, or reports may also have access to add/modify/delete CMX Analytics (location and presence) configuration. One way to mitigate some of this risk is for IT personnel to download CMX Analytics Reports and email them to non-IT personnel at regular intervals. Alternatively, the list of non-IT personnel—such as store operations managers, marketing executives, etc.—who have direct access to the MSE for CMX Analytics should be kept tightly controlled.

The MSE does support the ability to enforce the choice of a strong password, meaning a minimum length of password which includes capital letters and special characters. The MSE does not provide any mechanism for the end user to change their password after a certain period of time or to change their password at all. Hence the MSE administrator must be responsible for all user accounts and should always choose a strong password when creating user accounts. The MSE does not support the ability to disable a user password after a number of unsuccessful attempts. Hence there is limited ability to guard against unauthorized access to the MSE using a dictionary attack. This makes it all the more critical that the network administrator choose a strong password, especially for user accounts which belong to groups which have Write Access or Full Access.

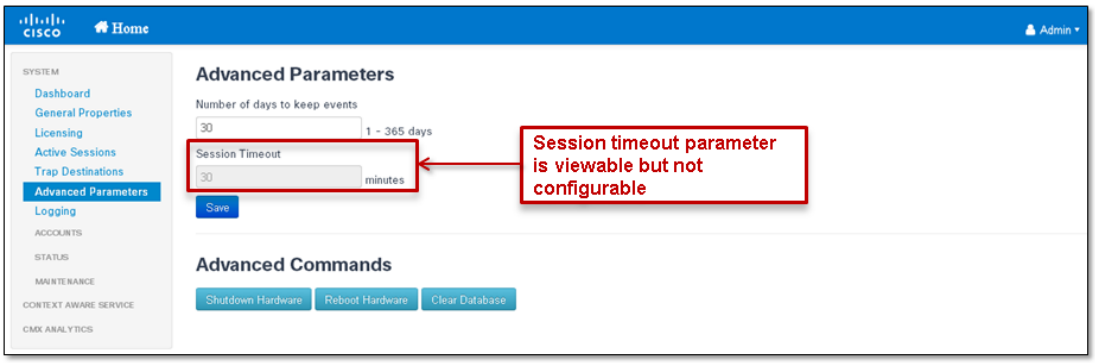
The MSE supports the ability to monitor active sessions. The MSE administrator can view active sessions by selecting the Active Sessions link under the System topic from the MSE Dashboard page. This displays the Active Sessions page, as shown in Figure 5-2.

Figure 5-2 Example of the Active Sessions Page



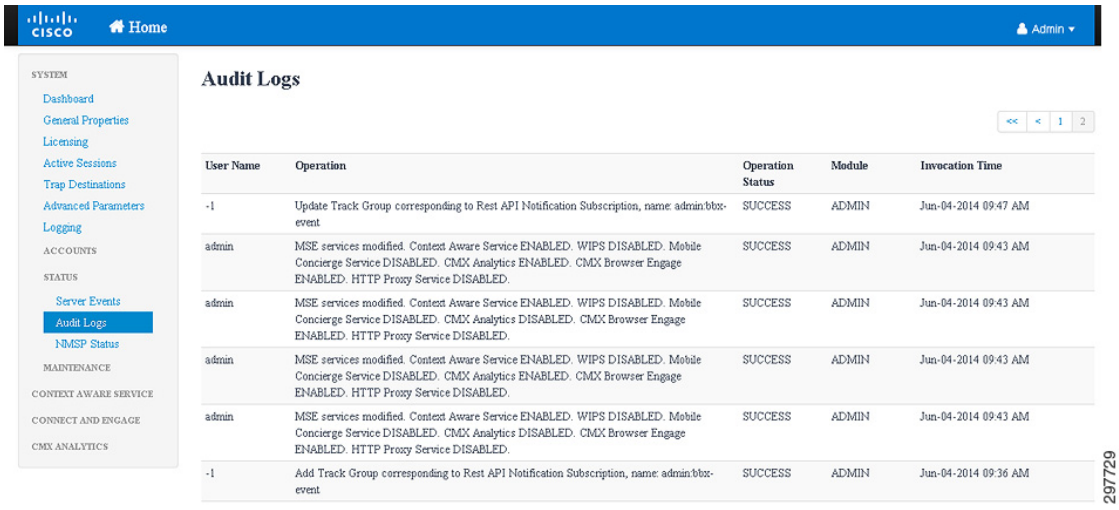
The length of time that a user's session is idle before being logged out of the MSE is set for 30 minutes. This setting is currently viewable under the Advanced Parameters settings, but is not configurable. An example is shown in Figure 5-3.

Figure 5-3 Session Timeout Parameter



The MSE administrator can also view logs to monitor activity of users on the MSE. The MSE administrator can view the logs by selecting the Audit Logs link under the Status topic from the MSE Dashboard page. This displays the Audit Logs page, as shown in Figure 5-4.

Figure 5-4 Example of the Audit Logs Page



The audit logs provide a fairly comprehensive audit trail, showing the specific operation which was performed, the user who performed that operation, whether it was successful or not, and the time when the operation was performed.

Role-Based Access Control for the CMX Connect & Engage Service

The CMX Connect & Engage service (which includes CMX Visitor Connect) has its own role-based access control (RBAC) separate from the MSE itself. For role-based access control on the MSE, see Role-Based Access Control on the MSE.

RBAC on the CMX Connect & Engage service consists of configuring Roles which can perform one or more operations. Individual Users are then created and assigned to one of the Roles. As of MSE version 8.0, all Roles and Users reside on the local database within the CMX Connect & Engage service on the MSE. There is no integration with an external data store, such as an LDAP database or external RADIUS server.

CMX Connect & Engage provides very granular role-based access control (RBAC). Each role can be configured for each of the following 15 operations:

- Accounts—Allows members of the role to create, edit, and delete Accounts. Accounts are associated with different Campaigns and Banners.
- Banner Approver—Allows members of the role to approve Banners.
- Banners—Allows members of the role to create and edit Banners.
- Campaigns—Allows members of the role to create and edit Campaigns.
- Campaign Approver—Allows members of the role to approve Campaigns.
- CMX Mobile—Allows members of the role to access functions found under the Mobile App topic.
- Domain Setup—Allows members of the role to create, edit, and delete domains, which are found under the Settings topic.
- Floor Navigation—Allows members of the role to access Floor Navigation functions found under the Mobile App topic.

- Menu
- Point of Interest—Allows members of the role to create, edit, and delete points of interest.
- Reports
- Roles—Allows members of the role to create, edit, and delete Roles.
- Server Settings—Allows members of the role to access Server Settings functions found under the Settings topic.
- Users—Allows members of the role to create, edit, and delete Users. Users are associated to a particular role for role-based access control.
- Visitor Connect—Allows members of the role to create splash templates and configure social media connectors.

As of software version 8.0, the CMX Connect & Engage service does support the ability to enforce the choice of a strong password—meaning a minimum length of password which includes capital letters and special characters. The CMX Connect & Engage service does not provide any mechanism for the end user to change their password after a certain period of time or to change their password at all. Hence the CMX administrator must be responsible for all user accounts and should always choose a strong password when creating user accounts.

CMX Visitor Connect & Engage does not support the ability to disable a user password after a number of unsuccessful attempts. Hence there is limited ability to guard against unauthorized access to the CMX Connect & Engage service using a dictionary attack. This makes it all the more critical that the network administrator choose a strong password, especially for users who belong to roles such as the Super Admin, who have access to all CMX Connect & Engage operations.