**Switch Software Dependencies**

The switch must support Change of Authorization (CoA) along with [[https://sharepoint.qualcomm.com/_layouts/images/icgen.gif](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html#wp9000135)MAC Authentication Bypass (MAB).](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html#wp9000135) Therefore a minimum version of software is necessary to support the Aruba Clearpass Solution.

|  |  |
| --- | --- |
| **​Switch** | **​Code** |
| ​6500 | ​12.2(33)SXI10 |
| ​4500x/4507/4510 | ​03.04.05.SG.151-2.SG5 |
| ​3750 | ​12.2(55)SE7 |
| ​3560 | ​Not tested, |

**SVI**

In addition to the normal ip-helper necessary for DHCP for the VLAN, another helper needs to be configured to point to the clearpass VIP. The Clearpass server uses this input to profile devices. Clearpass will not serve IP address to the clients.

***Example***

interface Vlan110

description :: User Data VLAN ::

ip helper-address 10.1.1.1

interface vlan400

description :: VoIP Subnet ::

ip helper-address 10.1.1.1

**Global Switch Configuration**

*The configuration below is a global switch config that prepares the switch to leverage Clearpass.*

ip device tracking  
  
ip http server

ip http secure-server

ip http session-module-list disable\_webmgmt NONE

ip http active-session-modules disable\_webmgmt

ip http secure-active-session-modules disable\_webmgmt  
  
aaa group server radius clearpass

server 10.1.1.1 auth-port 1812 acct-port 1813

aaa authentication dot1x default group clearpass

aaa authorization network default group clearpass

aaa accounting dot1x default start-stop group clearpass

radius-server vsa send authentication

radius-server host 10.1.1.1 auth-port 1812 acct-port 1813 key password

dot1x system-auth-control

authentication mac-move permit

aaa server radius dynamic-author

client 10.1.1.1 server-key clearpass

port 3799

auth-type all  
  
ip access-list extended DEFAULT-ACCESS

permit udp any any eq bootps

permit udp any any eq domain

permit tcp any any eq domain

permit tcp any host 10.1.1.1 eq 443

ip access-list extended REDIRECT

deny ip any host 10.1.1.1   
deny udp any any eq domain

permit tcp any any eq www

permit tcp any any eq 443

**Switch Port Configuration**

*The port configuration below needs to be added to the existing port configuration. This configuration activates the Clearpass solution on the individual port.*

**It is recommended to perform a shut/no shut on the port before the port configuration is applied. This will allow DHCP profiling to occur on any VOIP Phone.**

interface GigabitEthernet1/0/1  
description CONF:ON:Room:Port

ip access-group DEFAULT-ACCESS in  
authentication control-direction in

authentication host-mode multi-auth

authentication order mab dot1x

authentication priority mab dot1x

authentication port-control auto

authentication periodic

authentication timer restart 720  
authentication timer reauthenticate server  
dot1x pae authenticator  
dot1x timeout tx-period 60  
dot1x max-reauth-req 10  
 mab

**802.1x Defaults on Cisco Switches**

