Integration

The following sections describe the configuration required on switches and Wireless Controllers to support Cisco ISE functions.

- Enable Your Switch to Support Standard Web Authentication, on page 1
- Define Local Username and Password for Synthetic RADIUS Transactions, on page 2
- Configure NTP Server for Accurate Log and Accounting Timestamps, on page 2
- Command to Enable AAA Functions, on page 2
- RADIUS Server Configuration on the Switch, on page 3
- Enable Switch to Handle RADIUS Change of Authorization (CoA), on page 3
- Enable Device Tracking and DHCP Snooping on Switch Ports, on page 4
- Enable 802.1X Port-Based Authentication for Switch Ports, on page 4
- Enable EAP for Critical Authentications, on page 4
- Throttle AAA Requests Using Recovery Delay, on page 4
- VLAN Definitions Based on Enforcement States, on page 5
- Local (Default) Access List (ACL) Definitions on the Switch, on page 5
- Enable Switch Ports for 802.1X and MAB, on page 6
- Command to Enable 802.1X based on Identity-Based Networking Services, on page 8
- Enable EPM Logging, on page 10
- Enable Switch to Receive SNMP Traps, on page 10
- Enable SNMP v3 Query for Profiling on Switch, on page 10
- Enable MAC Notification Traps for Profiler to Collect, on page 10
- Configure RADIUS Idle-Timeout on the Switch, on page 10
- Wireless Controller Configuration for iOS Supplicant Provisioning, on page 11
- Configure ACLs on Wireless Controllers for MDM Interoperability, on page 11

Enable Your Switch to Support Standard Web Authentication

Ensure that you include the following commands in your switch configuration to enable standard web authentication functions for Cisco ISE, including provisions for URL redirection upon authentication:

```
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.1.2.3
ip http server

! Must enable HTTP/HTTPS for URL-redirection on port 80/443

ip http secure-server
```

Define Local Username and Password for Synthetic RADIUS Transactions

Enter the following command to enable the switch to talk to the Cisco ISE node as though it is the RADIUS server for this network segment:

```
username test-radius password 0 abcde123
```

Configure NTP Server for Accurate Log and Accounting Timestamps

Ensure that you specify the same NTP server on the switch as you have set in Cisco ISE by entering the following command:

```
ntp server <IP_address>|<domain_name>
```

Command to Enable AAA Functions

Enter the following commands on the switch to enable the various AAA functions between the switch and Cisco ISE, including 802.1X and MAB authentication functions:

```
aaa new-model

! Creates an 802.1X port-based authentication method list

aaa authentication dot1x default group radius

! Required for VLAN/ACL assignment

aaa authorization network default group radius

! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius

! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius

!

aaa session-id common
```

```
!

aaa accounting update periodic 1440

! Update AAA accounting information periodically every 1440 minutes

aaa accounting system default start-stop group radius

!
```

RADIUS Server Configuration on the Switch

Configure the switch to interact with Cisco ISE as the RADIUS source server by entering the following commands:

```
!
radius-server <ISE Name>

! ISE Name is the name of the ISE PSN

address ipv4 <ip address> auth-port 1812 acct-port 1813

! IP address is the address of the PSN. This example uses the standard RADIUS ports.

key <passwd>

! passwd is the secret password confiugured in Cisco ISE

exit
```

Note We recommend that you configure a dead-criteria time of 30 seconds with 3 retries to provide longer response times for RADIUS requests that use Active Directory for authentication.

Enable Switch to Handle RADIUS Change of Authorization (CoA)

Specify the settings to ensure the switch can appropriately handle RADIUS CoA behavior and related posture functions on Cisco ISE by entering the following commands:

```
aaa server radius dynamic-author client <ISE-IP> server-key 0 abcde123
```

Note

- Cisco ISE uses port 1700 (Cisco IOS software default) versus RFC default port 3799 for CoA. Existing Cisco Secure ACS 5.x customers may already have this set to port 3799 if they use CoA as part of an existing ACS implementation.
- secret key should be the same as the one configured on Cisco ISE while adding a network device and the IP address should be a PSN IP address.

Enable Device Tracking and DHCP Snooping on Switch Ports

To help provide optional security-oriented functions from Cisco ISE, enable device tracking and DHCP snooping for IP substitution in dynamic ACLs on switch ports by entering the following commands:

```
! Optional
 ip dhcp snooping

! Required!

! Configure Device Tracking Policy!device-tracking policy <DT_POLICY_NAME>no protocol
 ndp tracking enable

! Bind it to interface!interface <interface_id>device-tracking
attach-policy<DT_POLICY_NAME>
```

In RADIUS accounting, the DHCP attributes are not sent by the IOS sensor to Cisco ISE even when DHCP snooping is enabled. In such cases, DHCP snooping should be enabled on the VLAN to make the DHCP active.

Use the following commands to enable DHCP snooping on VLAN:

```
ip dhcp snooping

ip dhcp snooping vlan 1-100
```

Enable 802.1X Port-Based Authentication for Switch Ports

Enter the following commands to turn on 802.1X authentication for switch ports, globally:

```
dot1x system-auth-control
```

Enable EAP for Critical Authentications

To support supplicant authentication requests over the LAN, enable EAP for critical authentications (Inaccessible Authentication Bypass) by entering the following command:

```
dot1x critical eapol
```

Throttle AAA Requests Using Recovery Delay

In the case of a critical authentication recovery, configure the switch to automatically introduce an authentication delay (in milliseconds) to ensure Cisco ISE can launch services again after recovery. Use the following command:

```
authentication critical recovery delay 1000
```

VLAN Definitions Based on Enforcement States

Enter the following commands to define the VLAN names, numbers, and Switch Virtual Interfaces (SVIs) based on known enforcement states in your network. Create the respective VLAN interfaces to enable routing between networks. This can be especially helpful to handle multiple sources of traffic passing over the same network segments from both the endpoints (such as PC, laptop) and the IP phone through which the endpoint is connected to the network, for example:

```
vlan <VLAN_number>
name ACCESS!
vlan <VLAN_number>
name VOICE

!
interface <VLAN_number>
description ACCESS
ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
ip helper-address <Cisco_ISE_IP_address>

!
interface <VLAN_number>
description VOICE
ip address 10.2.3.4 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
```

Local (Default) Access List (ACL) Definitions on the Switch

Enable these functions on older switches (with Cisco IOS software releases earlier than 12.2(55)SE) to ensure Cisco ISE is able to perform the dynamic ACL updates required for authentication and authorization by entering the following commands:

```
ip access-list extended ACL-ALLOW

 permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain
  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal
permit tcp any host <Cisco_ISE_IP_address> eq www

permit tcp any host <Cisco_ISE_IP_address> eq 443

permit tcp any host <Cisco_ISE_IP_address> eq 8443

permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest

  deny ip any any log

!

! The ACL to allow URL-redirection for WebAuth
 ip access-list extended ACL-WEBAUTH-REDIRECT

 permit tcp any any eq www

 permit tcp any any eq 443
```

Note This configuration on the Wireless Controller may increase CPU utilization and raises the risk of system instability. This is an IOS issue and does not adversely affect Cisco ISE.

Enable Switch Ports for 802.1X and MAB

To enable switch ports for 802.1X and MAB:

Step 1 Enter the interface configuration mode for all of the access switch ports:

interface range FastEthernet0/1-8

Step 2 Enable the switch ports for access mode (instead of trunk mode):

switchport mode access

Step 3 Statically configure the access VLAN. This provides local provisioning for the access VLANs and is required for open-mode authentication:

switchport access vlan *<VLAN_number>*

Step 4 Statically configure the voice VLAN:

switchport voice vlan *<VLAN_number>*

Step 5 Enable open-mode authentication. Open mode allows traffic to be bridged onto the data and voice VLANs before authentication is completed. We strongly recommend using a port-based ACL in a production environment to prevent unauthorized access.

Enabling open-mode authentication also allows pre-authentication access before the AAA server response, subject to the port ACL.

authentication open

Step 6 Apply a port-based ACL to determine which traffic should be bridged by default from unauthenticated endpoints onto the access VLAN. Because you should allow all access first and enforce policy later, you should apply ACL-ALLOW to permit all traffic through the switch port. You have already created a default Cisco ISE authorization to allow all traffic for now because we want complete visibility and do not want to impact the existing end-user experience yet.

An ACL must be configured to prepend dynamic ACLs from the AAA server.

ip access-group ACL-ALLOW in

Note Before Cisco IOS software Release 12.2(55)SE on DSBU switches, a port ACL is required for dynamic ACLs from a RADIUS AAA server to be applied. Failure to have a default ACL will result in assigned dynamic ACLs being ignored by the switch. With Cisco IOS software Release 12.2(55)SE, a default ACL will be automatically generated and applied.

Note We are using ACL-ALLOW at this point in the lab because we want to enable 802.1X port-based authentication, but without any impact on the existing network. In a later exercise, we will apply a different ACL-DEFAULT, which blocks undesired traffic for a production environment.

Step 7 Enable Multi-Auth host mode. Multi-Auth is essentially a superset of Multi-Domain Authentication (MDA). MDA only allows a single endpoint in the data domain. When multi-auth is configured, a single authenticated phone is allowed in the voice domain (as with MDA) but an unlimited number of data devices can be authenticated in the data domain.

Allow voice and multiple endpoints on the same physical access port

authentication host-mode multi-auth

Note Multiple data devices (whether virtualized devices or physical devices connected to a hub) behind an IP phone can exacerbate the access ports' physical link-state awareness.

Step 8 Enable various authentication method options with the following commands:

Enable re-authentication:

authentication periodic

Enable re-authentication via RADIUS Session-Timeout:

authentication timer reauthenticate server

authentication event fail action next-method

Configure critical authentication vlan method in case of dead server:

authentication event server dead action reinitialize vlan *<VLAN_number>*

authentication event server alive action reinitialize

Configure IOS Flex-Auth authentication for 802.1X and MAB:

authentication order dot1x mab

authentication priority dot1x mab

Step 9 Enable 802.1X port control on the switchport:

authentication port-control auto

authentication violation restrict

Step 10 Enable MAC Authentication Bypass (MAB):

mab

Step 11 Enable 802.1X on the switchport:

dot1x pae authenticator

Step 12 Set the retransmit period to 10 seconds:

dot1x timeout tx-period *10*

Note The 802.1X tx-period timeout should be set to 10 seconds. Do not change this unless you understand the implications.

Step 13 Enable the portfast feature:

spanning-tree portfast

Command to Enable 802.1X based on Identity-Based Networking Services

The following example shows a control policy that is configured to allow sequential authentication methods using 802.1X, MAB, and web authentication.

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
!


policy-map type control subscriber DOT1XMAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
   30 authorize
  40 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
!
```

The following example shows a control policy that is configured to allow sequential authentication methods using MAB, 802.1X, and web authentication.

```
policy-map type control subscriber MABDOT1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
   20 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class ALL_FAILED do-until-failure
   10 authentication-restart 60
 event authentication-success match-all
  10 class DOT1X do-until-failure
   10 terminate mab
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
```

Applying the service policy on the interface:

```
interface GigabitEthernet1/0/4
 switchport mode access
 device-tracking attach-policy pol1
 ip access-group sample in
 authentication timer reauthenticate server
 access-session port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 dot1x timeout auth-period 10
 spanning-tree portfast
 service-policy type control subscriber DOT1XMAB
```

Enable EPM Logging

Set up standard logging functions on the switch to support possible troubleshooting and recording for Cisco ISE functions:

```
epm logging
```

Enable Switch to Receive SNMP Traps

Ensure the switch can receive SNMP trap transmissions from Cisco ISE over the appropriate VLAN in this network segment:

```
snmp-server community public RO
snmp-server trap-source <VLAN_number>
```

Enable SNMP v3 Query for Profiling on Switch

Configure the switch to ensure SNMP v3 polling takes place as intended to support Cisco ISE profiling services using the following commands. Before that configure the SNMP settings in the Cisco ISE GUI in the **SNMP Settings** window. To view this window, click the **Menu** icon (☰) and choose**Administration** > **Network Resources** > **Network Devices** > **Add | Edit** > **SNMP Settings**.

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group  <group> v3 priv
snmp-server group <group> v3 priv contextvlan-1
```

Note The **snmp-server group** *<group>* **v3 priv context** *vlan-1* command must be configured for each context. The **snmp show context** command lists all the context information.

If the SNMP request times out and there is no connectivity issue, then you can increase the timeout value.

Enable MAC Notification Traps for Profiler to Collect

Configure your switch to transmit the appropriate MAC notification traps so that the Cisco ISE profiler function can collect information on network endpoints:

```
mac address-table notification change
mac address-table notification mac-move
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

Configure RADIUS Idle-Timeout on the Switch

To configure the RADIUS idle-timeout on a switch, use the following command:

```
Switch(config-if)# authentication timer inactivity
```

where *inactivity* is the interval of inactivity in seconds, after which the client activity is considered unauthorized.

In Cisco ISE, you can enable this option for any authorization policies to which such a session inactivity timer should apply. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Wireless Controller Configuration for iOS Supplicant Provisioning

For Single SSID

To support Apple iOS-based devices (iPhone or iPad) switching from one SSID to another on the same wireless access point, configure the Wireless Controller to enable the **FAST SSID change** function. This function helps ensure iOS-based devices can switch between SSIDs quickly.

For Dual SSID BYOD

Fast SSID must be enabled to support dual SSID BYOD. When fast SSID changing is enabled, the Wireless Controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced. For more information about configuring fast SSID on a Cisco Wireless Controller, see the Cisco Wireless Controller Configuration Guide.

Example Wireless Controller Configuration

```
WLC (config)# FAST SSID change
```

You might see the following error message while trying to connect to a wireless network for some of the Apple iOS-based devices:

```
Could not scan for Wireless Networks.
```

You can ignore this error message because this does not affect the authentication of the device.

Configure ACLs on Wireless Controllers for MDM Interoperability

Configure ACLs on the Wireless Controller for use in an authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs must be in the following sequence.

Step 1 Allow all outbound traffic from the server to the client.

Step 2 (Optional) Allow ICMP inbound traffic from the client to the server for troubleshooting.

Step 3 Allow access to the MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.

Step 4 Allow all inbound traffic from the client to the server to Cisco ISE for the web portal and supplicant, and certificate provisioning flows.

Step 5 Allow inbound Domain Name System (DNS) traffic from the client to the server for name resolution.

Step 6 Allow inbound DHCP traffic from the client to the server for IP addresses.

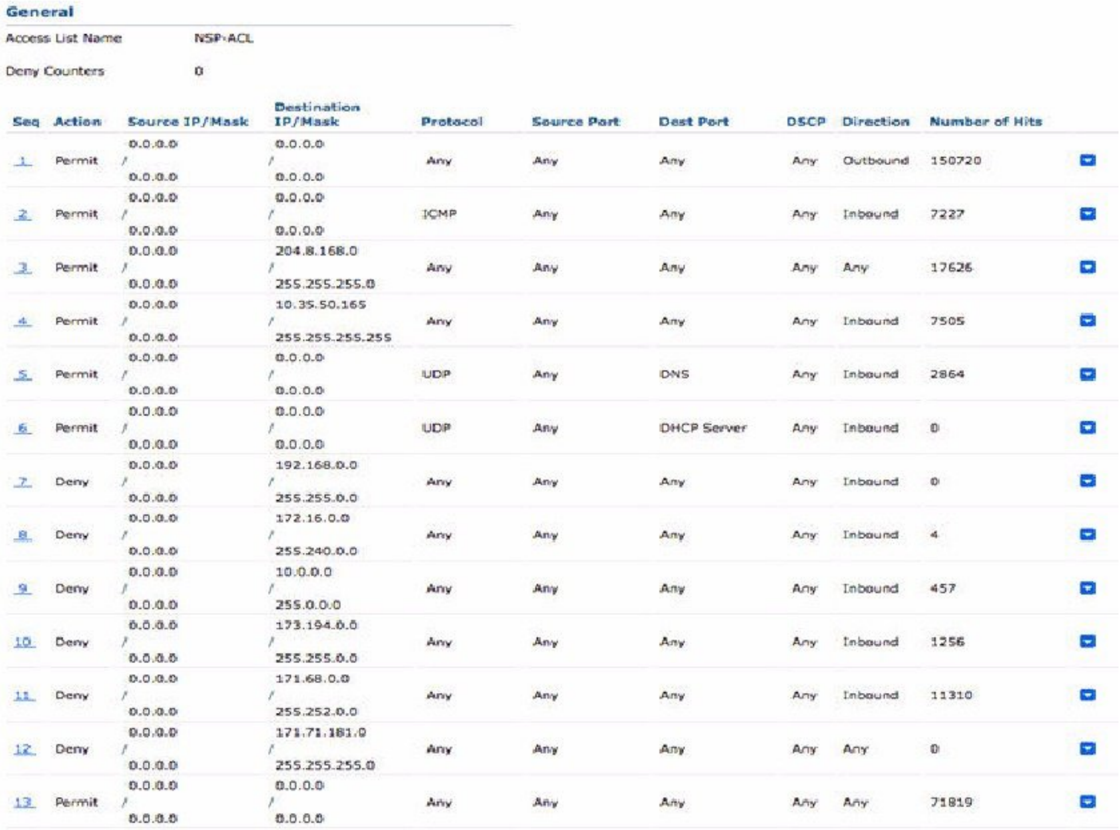
Step 7 Deny all inbound traffic from the client to the server to corporate resources for redirection to Cisco ISE (as per your company policy).

Step 8 (Optional) Permit the rest of the traffic.

Example

The following example shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE IP address is 10.35.50.165, the internal corporate network IP addresses are 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

Figure 1: ACLs for Redirecting Nonregistered Device



General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720	▾
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227	▾
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626	▾
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505	▾
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864	▾
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	▾
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	▾
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4	▾
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457	▾
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256	▾
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310	▾
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0	▾
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819	▾