APPENDIX C

Switch Configuration Required to Support Cisco ISE Functions

To ensure Cisco ISE is able to interoperate with network switches and functions from Cisco ISE are successful across the network segment, you need to configure network switches with the necessary NTP, RADIUS/AAA, 802.1X, MAB, and other settings for communication with Cisco ISE, according to the following topics:

Enable Your Switch to Support Standard Web Authentication

Ensure you include the following command lines in your switch configuration to enable standard Web Authenticating 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 a Local User Name and Password for Synthetic RADIUS Transactions

Use this function 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 cisco123
```

Set the NTP Server to Ensure Accurate Log and Accounting Timestamps

Be sure to specify the same NTP server as is set in Cisco ISE at **Administration > System > Settings > System Time**.

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

Enable AAA Functions

Use the following command lines 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 5
! Update AAA accounting information periodically every 5 minutes
aaa accounting system default start-stop group radius
!
aaa server radius dynamic-author <cr>
client 10.0.56.17 server-key cisco
! Enables ISE to act as a AAA server when interacting with the client at IP address
10.0.56.17
```

RADIUS Servers Configuration

Configure the switch to interoperate with Cisco ISE acting as the RADIUS source server.

```
!
radius-server attribute 6 on-for-login-auth
! Include RADIUS attribute 8 in every Access-Request
radius-server attribute 8 include-in-access-req
! Include RADIUS attribute 25 in every Access-Request
radius-server attribute 25 access-request include
! Wait 3 x 30 seconds before marking RADIUS server as dead
radius-server dead-criteria time 30 tries 3
!
! Use RFC-standard ports (1812/1813)
radius-server host <Cisco_ISE_IP_address> auth-port 1812 acct-port 1813 test username
test-radius key 0 <RADIUS-KEY>
!
radius-server vsa send accounting
radius-server vsa send authentication
!
! send RADIUS requests from the MANAGEMENT VLAN
ip radius source-interface <VLAN_number>
```

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 RADIUS Change of Authorization (CoA)

Specify the settings here to ensure the switch is able to appropriately handle RADIUS Change of Authorization behavior supporting Posture functions from Cisco ISE.

```
aaa server radius dynamic-author
  client <ISE-IP> server-key 0 cisco123
```

Note Cisco ISE uses port 1700 (IOS 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 are using CoA as part of an existing ACS implementation.

Enable Device Tracking and DHCP Snooping

To help provide optional security-oriented functions from Cisco ISE, you can enable device tracking and DHCP snooping for IP substitution in dynamic ACLs on switch ports.

```
! Optional
ip dhcp snooping
! Required!
ip device tracking
```

Enable 802.1X Port-Based Authentication

This command line turns 802.1X authentication on for switch ports, globally.

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

Use EAP for Critical Authentications

To support supplicant authentication requests over the LAN, enable EAP for critical authentications (Inaccessible Authentication Bypass).

```
dot1x critical eapol
```

Throttle AAA Requests Using Recovery Delay

When a critical authentication recovery event takes place, you can configure the switch to automatically introduce a delay (in seconds) to ensure Cisco ISE is able to launch services again following recovery.

```
authentication critical recovery delay 1000
```

Define VLANs Based on Enforcement States

Use the following command lines to define the VLAN names, numbers, and 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—traffic from both PCs and the IP phone through which the PC is connected to the network, for example.

Note The first IP helper goes to the DHCP server and the second IP helper sends a copy of the DHCP request to the inline posture node for profiling.

```
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>
 ip helper-address <Cisco_ISE_IP_address>
```

Define Local (Default) ACLs on the Switch

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

```
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
 deny ip any host <Cisco_ISE_IP_address>
 permit tcp any any eq www
 permit tcp any any eq 443
 permit tcp any any eq 8443
```

Enable Cisco Security Group Access Switch Ports

To ensure Cisco ISE is able to interoperate with an existing Cisco Security Group Access deployment, use the following procedure to ensure you have enabled all of the functions necessary on the switch.

Step 1 Enter 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 the access VLANs and is required for open-mode authentication.

```
switchport access <VLAN_number>
```

Step 4 Statically configure the voice VLAN:

```
switchport voice <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. Cisco strongly recommends using a port-based ACL in a production environment to prevent unauthorized access.

```
! Enables pre-auth access before AAA response; subject to 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. Since 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 ISE authorization to allow all traffic for now since we want complete visibility and not impact the existing end user experience yet.

```
! An ACL must be configured to prepend dACLs from AAA server.
ip access-group ACL-ALLOW in
```

Note Prior to software versions 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 dACLs being ignored by the switch. With 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 have no 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 + multiple endpoints on 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:

```
! Enable re-authentication
authentication periodic
! Enable re-authentication via RADIUS Session-Timeout
authentication timer reauthenticate server
authentication event fail action next-method
authentication event server dead action authorize <VLAN_number>
authentication event server alive action reinitialize
! IOS Flex-Auth authentication should do 802.1X then MAB
authentication order dot1x mab
authentication priority dot1x mab
```

Step 9 Enable 802.1X port control on the switchport:

```
! Enables port-based authentication on the interface
authentication port-control auto
authentication violation restrict
```

Step 10 Enable MAC Authentication Bypass (MAB):

```
! Enable MAC Authentication Bypass (MAB)
mab
```

Step 11 Enable 802.1X on the switchport

```
! Enables 802.1X authentication on the interface
dot1x pae authenticator
```

Step 12 Set the retransmit period to 10 seconds:

```
dot1x timeout tx-period 10
```

Note The dot1x 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
```

Enable EPM Logging

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

```
epm logging
```

Enable SNMP Traps

Ensure the switch is able to 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

Configure the switch to ensure SNMP v3 polling takes place as intended to support Cisco ISE profiling services. First, configure the SNMP settings in Cisco ISE at **Administration > Network Resources > Network Devices >Add | Edit > SNMP Settings**. See "Table 6-2 Network Devices List Page: SNMP Settings" on page 6-5 for details.

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group <group> v3 priv
snmp-server group <group> v3 priv context vlan-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 is able to 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 the RADIUS Idle-Timeout

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

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

where inactivity is interval of inactivity in seconds, after which 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 from **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. For more information on creating Authorization Policies, see Configuring Permissions for Authorization Profiles, page 17-27.