Universal Switch Configuration for Cisco Identity Services Engine

Secure Access How-To Guide Series

Author: Hosuk Won

Date: January 2017

Table of Contents

Introduction

What is Cisco Identity Services Engine?

Cisco Identity Services Engine (ISE) is an all-in-one enterprise policy control product that enables comprehensive secure wired, wireless, and Virtual Private Networking (VPN) access.

Cisco ISE offers a centralized control point for comprehensive policy management and enforcement in a single RADIUS-based product. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions. Cisco ISE is an integral component of Cisco Secure Access.

Cisco Secure Access is an advanced Network Access Control and Identity Solution that is integrated into the Network Infrastructure. It is a fully tested, validated solution where all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

Cisco Catalyst Switches

Unlike overlay Network Access Control solutions the Cisco Secure Access utilizes the access layer devices (switches, wireless controllers, and so on) for enforcement. The access device itself now handles functions that were commonly handled by appliances and other overlay devices, such as URL redirection for web authentications.

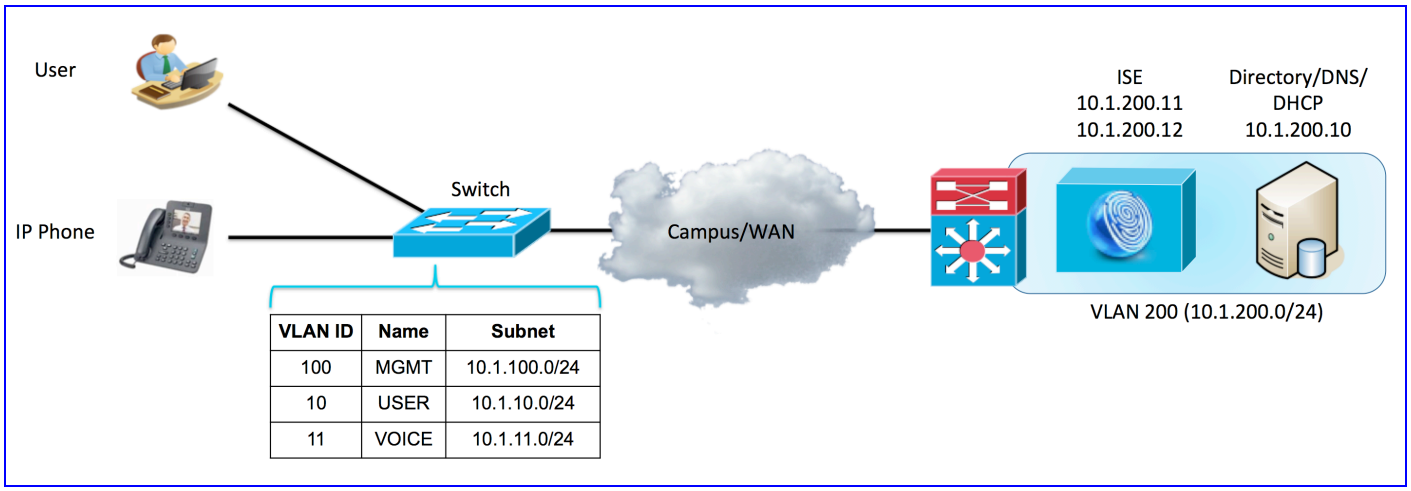
The Cisco Secure Access not only combines standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, it also has many more advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, guest and web authentications services, posture assessments, and integration with leading Mobile Device Management (MDM) vendors for compliance validation of mobile devices before and during network access.

About This Document

This document provides best practice configurations on Cisco Catalyst switches for integrating with Cisco Identity Services Engine. The main section of the document is broken into three parts. Global configuration applies to both monitor/low-impact & closed mode phased deployment. There are two interface configurations provided with first being the monitor/low-impact mode configuration and the second part is closed mode interface configuration. Configuration noted with 'Optional' are ones not essential in terms of ISE integration nonetheless important to address certain user experience. This includes interface behavior during RADIUS server outages as well as dealing with URL redirects for HTTPS traffic.

Following diagram shows the overall layout of the components. There are two access VLANs, ACCESS VLAN for Employee users and VOICE VLAN for IP Phones. MGMT VLAN is used for the switch to communicate with the administrative users and ISE nodes. Although this document doesn't include policy configurations on ISE such as BYOD, Posture Assessment, and profiling configuration provided here allows baseline for such operations.

Figure 1 Components



VLAN ID	Name	Subnet
100	MGMT	10.1.100.0/24
10	USER	10.1.10.0/24
11	VOICE	10.1.11.0/24

Also, in the appendix there are sample configurations that can be copy & pasted into with minimal modification.

Configuration

Global Configuration

In this configuration, two ISE PSN nodes are defined for redundancy. The critical Authorization feature is also used to allow access to the network when none of the ISE nodes are reachable from the switch.

Note: Depending on the IOS & IOS-XE version, some of the commands here may be enabled by default.

Step 1 Basic required commands on the system. Domain name is required when enabling https redirect.

```
SWITCH(config)#ip domain-name EXAMPLE.COM
```

Step 2 (Optional) This 'RADIUS-TEST' account will be used to generate RADIUS test message for ISE.

```
SWITCH(config)#username RADIUS-TEST password 0 PASSWORD
```

Note: The username and password does not need to be a valid account in the Identity Database in ISE. Whether the ISE node sends back ACCESS-ACCEPT for a successful authentication, or ACCESS_REJECT for a failed authentication, the switch considers both responses valid from a live server for RADIUS dead setting. But it is still good to provide a valid account in an external Identity Store, such as MS Active Directory or LDAP, so the switch can test all the way to the back-end Identity Store, and to ensure that the ISE node has connectivity to the external Identity Database.

Step 3 (Optional) Generate keys to be used for HTTPS services

```
SWITCH(config)#crypto key generate rsa general-keys mod 2048
```

Note: Do not run the 'ip http secure-server' command prior to generating the keys. If you perform the commands out of order, the switch automatically generates a certificate with a smaller key size. This certificate can cause undesirable behavior when redirecting HTTPS traffic.

Step 4 Enable AAA.

```
SWITCH(config)#aaa new-model
```

Step 5 Enables network authentication to use defined RADIUS servers.

```
SWITCH(config)#aaa authentication dot1x default group ISE
```

Step 6 Enables network authorization such as url-redirect, dVLAN (Dynamic VLAN), and dACL (Downloadable ACL) for 802.1x authenticated sessions.

```
SWITCH(config)#aaa authorization network default group ISE
```

Step 7 Send accounting information from the NAD to ISE whenever sessions are initiated and stopped.

```
SWITCH(config)#aaa accounting dot1x default start-stop group ISE
```

Step 8 Send accounting updates for new updates and every 2 days so active sessions on the NAD are also maintained on the ISE.

```
SWITCH(config)#aaa accounting update newinfo periodic 2880
```

Note: Interim RADIUS accounting messages are sent to ISE to notify that the sessions are still intact. When ISE fails to receive a RADIUS accounting message for a prolonged period for a given endpoint, ISE removes that session from its session table. ISE does not remove the endpoint from the switch, which creates disconnect between the switch and ISE in terms of which sessions are active. This disconnect can also impact when the endpoint access needs to be reevaluated for any reason. By default, ISE flushes out any sessions without Interim RADIUS accounting messages for 5 days for any authenticated sessions. By sending the periodic RADIUS accounting message to the ISE node less than 5 days, the switch ensures that the sessions are maintained on the ISE. The reason for 2 days here is to provide two updates within 5 days in case one of the RADIUS Accounting packets failed to reach the ISE node.

Step 9 This configures NAD to accept CoA request from ISE. We recommend adding any PSN that this NAD will send requests to for CoA as well. This is required for ISE advanced use cases such as BYOD (NSP), Posture, CWA, and MDM.

```
SWITCH(config)#aaa server radius dynamic-author
SWITCH(config-locsvr-da-radius)# client 10.1.200.11 server-key RADIUS_KEY
SWITCH(config-locsvr-da-radius)# client 10.1.200.12 server-key RADIUS_KEY
```

Step 10 NAD uses a common session ID for a client between different authentication methods. This session ID is used for reporting, CoA, and ISE session management purposes.

```
SWITCH(config)#aaa session-id common
```

Step 11 (Optional) This optional command allows new session on a port when there is an existing session for same MAC address on a different port on the same switch. This is useful when an unmanaged hub or switch is in use, or third-party IP phones are in use by end users.

```
SWITCH(config)#authentication mac-move permit
```

Note: This feature is particularly useful in an environment where unmanaged switch/hubs or 3rd party IP phones are in use. When these types of devices are in use, Catalyst switches are not sufficiently notified when an authenticated device moves from one interface to the other, which could cause the switch to deny access. With this command, the switch can tear down the original session from when the device was first seen, and allow the device to authenticate on a different interface on the same switch. This is not required

for Cisco IP Phones. Cisco IP Phones can use a CDP message to inform the switch when device behind the phone is disconnected, so the switch can effectively remove the session.

Step 12 (Optional) This command allows sessions without dACL to connect to ACL enabled interface with full access.

```
SWITCH(config)#epm access-control open
```

Note: This feature is useful in an environment where mixture of authorization profiles that use dACL and ones that don't. For example, user devices are enforced with dACL to limit access to the network, but no dACL is used on IP phones. When IP Phones are connected, the IP phone is authorized to the voice resources by MAB/802.1X (without dACL). When a user's device is connected to the back of the IP Phone, the switch enforces user device dACL, which applies the ACL at the interface level. This denies IP access to the IP Phone, since the IP Phone lacks dACL for authorization. However, when this command is entered globally, the switch dynamically inserts 'permit ip any any' ACL for any sessions without dACL, including the IP Phone. This is also true for multiple devices connected through an unmanaged hub. If there are multiple devices already connected without dACL, then when a new device with dACL AuthZ is authenticated to the same interface that the unmanaged hub is connected to, then this feature applies 'ip permit any any' ACL to previously connected devices sessions.

Step 13 Enables 802.1x system wide.

```
SWITCH(config)#dot1x system-auth-control
```

Note: When this command is removed it does not disable 802.1X on all the ports, rather the absence of this command would make the switch ignore the EAP frames from the endpoints. If the goal is to disable 802.1X on the ports, use interface range command to remove authentication-related commands.

Step 14 (Optional) Send canned EAPoL Success message to the client when the port fail-open/fail-closes in the event when none of the RADIUS servers are reachable.

```
SWITCH(config)#dot1x critical eapol
```

Note: Critical authentication occurs when none of the configured ISE nodes are reachable to provide authentication services to the switch. When endpoints are authorized based on critical authentication, the endpoint supplicant may restart authentication that impacts user experience, as network connectivity drops during authentication. This feature sends canned EAPoL Success message to the endpoint supplicant so authentication does not restart. Whether the supplicant honors the canned message depends on the supplicant, including supplicant settings, supplicant vendor, and EAP Types.

Step 15 Enable IP device tracking to find out the endpoint IP. This is essential for profiling as well as applying dACL, filter-id, and URL redirect to the session.

```
SWITCH(config)#ip device tracking
```

Step 16 (Optional) If users are seeing duplicate IP message on Windows machines after enabling 'ip device tracking', the following commands can be used to avoid such messages. For switch code running IOS 15.2(2)E & IOS-XE 03.06.00E and above, use following command.

```
SWITCH(config)#ip device tracking probe auto-source
```

Note: For previous versions of IOS code, run the following command.

```
SWITCH(config)#ip device tracking probe delay 10
```

Note: If the preceding command does not resolve the issue and the switch is configured with SVI for endpoint VLANs then following command can be used to address duplicate IP message issue.

```
SWITCH(config)#ip device tracting probe use-svi
```

Step 17 Create VLANs.

```
SWITCH(config)#vlan 10
SWITCH(config-vlan)# name USER

SWITCH(config)#vlan 11
SWITCH(config-vlan)# name VOICE

SWITCH(config)#vlan 100
SWITCH(config-vlan)# name MGMT
```

Step 18 SVI configuration for user VLAN

```
SWITCH(config)#interface 10
SWITCH(config-if)# ip address 10.1.10.1 255.255.255.0
```

Step 19 Send DHCP packets to the DHCP server

```
SWITCH(config-if)# ip helper-address 10.1.200.10
```

Step 20 (Optional) Send DHCP packets to ISE for profiling purpose.

```
SWITCH(config-if)#ip helper-address 10.1.200.11
```

Note: Recommended to send to just one of the ISE nodes instead of multiple nodes to reduce replication traffic between ISE nodes. Also, if device sensor is used then recommended not forwarding DHCP using 'helper-address' at the same time as it results in duplicate profiling information, which potentially increases replication traffic between ISE nodes.

Step 21 SVI configuration for voice VLAN.

```
SWITCH(config)#interface 11
SWITCH(config-if)#ip address 10.1.11.1 255.255.255.0
SWITCH(config-if)#ip helper-address 10.1.200.10
SWITCH(config-if)#! ip helper-address 10.1.200.11
```

Step 22 SVI configuration for management VLAN.

```
SWITCH(config)#interface 100
SWITCH(config-if)#ip address 10.1.100.1 255.255.255.0
```

Step 23 This is required to use http redirect feature of the switch.

```
SWITCH(config)#ip http server
```

Step 24 (Optional) This is required to use https redirect feature of the switch.

```
SWITCH(config)#ip http secure-server
```

Note: Utilizing HTTPS redirect impacts CPU on the switch and is recommended to monitor the performance before enabling it on high-density switches.

Step 25 (Optional) Configure the following to disable http based admin access to the switch while still allowing URL-Redirect to work.

```
SWITCH(config)#ip http active-session-modules none
SWITCH(config)#ip http secure-active-session-modules none
```

Step 26 (Optional) This impacts how many concurrent URL-Redirect sessions can be present. On a high-density access switch, this value may need to be increased if multiple users are going to be using URL-Redirect simultaneously. The default and maximum value may be different based on the code version and the platform. On 3560CG platform running 15.2(2)E3, the default is 16 and maximum is 48.

```
SWITCH(config)#ip http max-connections 48
```

Note: Not available on older version of IOS.

Step 27 This ACL defines which traffic is redirected to ISE during CWA, BYOD, and Posture. Any traffic that is permitted per ACL is redirected. Implicit deny prevents other traffic types from being redirected. We recommended that you specify only HTTP (and HTTPS) here to be permitted since this traffic gets pushed to the switch CPU. If additional access control is needed in conjunction with the redirect ACL, then we recommend using dACL in conjunction with the redirect ACL.

```
SWITCH(config)#ip access-list extended ACL_WEBAUTH_REDIRECT
SWITCH(config-ext-nacl)#permit tcp any any eq www
SWITCH(config-ext-nacl)#permit tcp any any eq 443
```

Note: The ACL name referenced above is identical to the default redirect ACL name used in fresh ISE 2.0 installation. If different name is desired, make sure you update both the switch and the ISE Authorization Profile with new redirect ACL name.

Step 28 This ACL defines which traffic is redirected to ISE for black listed devices. Any traffic that is permitted per ACL gets redirected. Implicit deny prevents other traffic types from being redirected. We recommend that you specify only HTTP (and HTTPS) here to be permitted as this traffic gets pushed to the switch CPU. If additional access control is needed in conjunction with the redirect ACL, we recommend using dACL in conjunction with the redirect ACL.

```
SWITCH(config)#ip access-list extended BLACKHOLE
SWITCH(config-ext-nacl)#permit tcp any any eq www
SWITCH(config-ext-nacl)#permit tcp any any eq 443
```

Note: The ACL name referenced above is identical to the default redirect ACL name used in fresh ISE 2.0 installation. If different name is desired, make sure to update both the switch and the ISE Authorization Profile with new redirect ACL name.

Step 29 ACL to apply prior to RADIUS authentication. This is required when using open mode or low-impact mode of phased deployment for wired access

```
SWITCH(config)#ip access-list extended ACL-DEFAULT
SWITCH(config-ext-nacl)#permit udp any any eq domain
SWITCH(config-ext-nacl)#permit udp any eq bootpc any eq bootps
SWITCH(config-ext-nacl)#deny ip any any
```

Note: In the low-impact mode deployment, this ACL is in effect when the interface goes into critical auth state. That means that when an endpoint is trying to connect while none of the ISE nodes are reachable, and the endpoint is placed in critical VLAN configured per interface configuration, the endpoint is still restricted to this ACL during critical state.

Step 30 Configure the NAD to send any defined Vendor Specific Attribute (VSA) to ISE during authentication requests and accounting updates

```
SWITCH(config)#radius-server vsa send authentication
SWITCH(config)#radius-server vsa send accounting
```

Step 31 Send additional attribute to RADIUS server (Required for ISE).

```
SWITCH(config)#radius-server attribute 6 on-for-login-auth
SWITCH(config)#radius-server attribute 8 include-in-access-req
SWITCH(config)#radius-server attribute 25 access-request include
```

Step 32 Add ISE PSN as RADIUS server

```
SWITCH(config)#radius server ISE01
SWITCH(config-radius-server)#address ipv4 10.1.200.11
```

Step 33 Define method and username for testing RADIUS status on switch code running IOS 15.2(2)E & IOS-XE 03.06.00E and above. This command sends RADIUS test messages to the server only when the RADIUS server is marked dead per dead criteria. The probe will be sent when the deadtime expires and more frequently if the RADIUS server is still unresponsive. This command is useful in a large organization with high number of NADs as probes are not being sent constantly. This command and the next command are mutually exclusive.

```
SWITCH(config-radius-server)# automate-tester username RADIUS-TEST probe-on
```

Note: The following command is supported on previous versions of IOS. This command sends RADIUS test messages to the server at a configured interval, regardless of server status. If the deployment has a large number of NADs, we recommend that you increase the interval of the probe, to limit the impact on the RADIUS server. When increasing the idle-time value, the global deadtime value should also be increased so probe idle-time is less than deadtime. This ensures that endpoints authorized into critical states are not reinitialized only to be authorized back to critical state when the deadtime expires. Here the value is set to 10 minutes (Default is 60 minutes).

```
SWITCH(config-radius-server)# automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
```

Note: These probe messages will be visible on ISE RADIUS Livelog along with regular user authentication events. On ISE, collection filters can be configured to filter out probe messages so only user authentication events are visible in the Livelog.

Step 34 Set RADIUS key.

```
SWITCH(config-radius-server)#key RADIUS_KEY
```

Step 35 Configure additional ISE PSN as RADIUS server.

```
SWITCH(config)#radius server ISE02
SWITCH(config-radius-server)#address ipv4 10.1.200.12
SWITCH(config-radius-server)#automate-tester username RADIUS-TEST probe-on
SWITCH(config-radius-server)#! automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
SWITCH(config-radius-server)#key RADIUS_KEY
```

Step 36 Add RADIUS server group to be referenced in the AAA directive

```
SWITCH(config)#aaa group server radius ISE
SWITCH(config-sg-radius)#server name ISE01
SWITCH(config-sg-radius)#server name ISE02
```

Step 37 Define how long it takes the NAD to mark the RADIUS server dead when the server fails to respond. In an environment where there is a single ISE node defined as RADIUS server, it also defines how long the NAD will leave the port in fail-open/fail-closed (Critical) state, assuming interface configuration is configured to reinitialize after servers are back online. If all the ISE nodes are back in service, the switch will revert back to the first ISE node in the list. In this example, the value is set to 15 minutes.

```
SWITCH(config-sg-radius)#deadtime 15
```

Note: This value should be higher than idle-time set for any of the RADIUS probes configured previously. Instead of defining the deadtime in the RADIUS server group, it can also be configured globally using 'radius-server deadtime 15' command.

Step 38 Set RADIUS dead criteria to mark server dead.

```
SWITCH(config)#radius-server dead-criteria time 10 tries 3
```

Step 39 (Optional) Defines which interface the RADIUS requests will source from.

```
SWITCH(config)#ip radius source-interface vlan 100
```

Note: Although Management SVI is used in above example, it is recommended to utilize loopback interface so the source IP of the RADIUS request is guaranteed to arrive from same source IP in case there are multiple paths to the RADIUS server.

Step 40 (Optional) Used for profiling. This allows ISE to poll CDP/LLDP/ARP table from the NAD. If device sensor feature is used, then recommended not to use SNMP at the same time to reduce duplicate profiling data

```
SWITCH(config)#snmp-server community SNMP_COMMUNITY_STRING RO
```

Note: Aside from custom SNMP community string, it is also recommended to use ACL to only allow ISE nodes and management server to have access to the switch via SNMP.

Step 41 (Optional) Enable DHCP snooping to gather DHCP information from the clients for profiling purpose using device sensor. This is recommended method of collecting DHCP information as opposed to using 'ip helper-address' command

```
SWITCH(config)#ip dhcp snooping
```

Note: If static IP addresses are used for endpoints, skip this step.

Step 42 (Optional) Enable DHCP snooping on the VLANs that endpoints will reside

```
SWITCH(config)#ip dhcp snooping vlan 10, 11
```

Note: If static IP addresses are used for endpoints, skip this step.

Step 43 (Optional) Enable device sensor for DHCP

```
SWITCH(config)#device-sensor filter-list dhcp list TLV-DHCP
SWITCH(config-sensor-dhcplist)#option name host-name
SWITCH(config-sensor-dhcplist)#option name requested-address
```

```
SWITCH(config-sensor-dhcplist)#option name parameter-request-list
SWITCH(config-sensor-dhcplist)#option name class-identifier
SWITCH(config-sensor-dhcplist)#option name client-identifier
SWITCH(config)#device-sensor filter-spec dhcp include list TLV-DHCP
```

Step 44 (Optional) Enable CDP globally.

```
SWITCH(config)#cdp run
```

Step 45 (Optional) Enable device sensor for CDP

```
SWITCH(config)#device-sensor filter-list cdp list TLV-CDP
SWITCH(config-sensor-cdplist)#tlv name device-name
SWITCH(config-sensor-cdplist)#tlv name address-type
SWITCH(config-sensor-cdplist)#tlv name capabilities-type
SWITCH(config-sensor-cdplist)#tlv name platform-type
SWITCH(config)#device-sensor filter-spec cdp include list TLV-CDP
```

Step 46 (Optional) Enable LLDP globally

```
SWITCH(config)#lldp run
```

Step 47 (Optional) Enable device sensor for LLDP.

```
SWITCH(config)#device-sensor filter-list lldp list TLV-LLDP
SWITCH(config-sensor-lldplist)#tlv name system-name
SWITCH(config-sensor-lldplist)#tlv name system-description
SWITCH(config)#device-sensor filter-spec lldp include list TLV-LLDP
```

Step 48 (Optional) Enable sensor data to be sent in RADIUS accounting including all changes

```
SWITCH(config)#device-sensor accounting
SWITCH(config)#device-sensor notify all-changes
```

Step 49 (Optional) Disable local analyzer to prevent duplicate updates from being sent to ISE

```
SWITCH(config)#no macro auto monitor
SWITCH(config)#access-session template monitor
```

Note: Due to CSCvc76593 the IP device Tracking needs to be disabled from all trunked interfaces.

```
SWITCH(config-if)#ip device tracking maximum 0
```

Step 50 End configuration mode and save configuration

```
SWITCH(config)#end
SWITCH#write memory
Building configuration…
[OK]
SWITCH#
```

Interface Level Configuration (Monitor Mode / Low-Impact Mode Configuration)

Following interface configuration enables 'authentication open' directive that is the key command for Monitor Mode and Low-Impact Mode configuration. Main difference between the two modes is existence of port ACL or not. Typically for Monitor mode, the portal ACL is not applied whereas for Low-Impact mode the ACL is applied to limit traffic to DHCP, DNS, and some cases TFTP. This configuration utilizes 'authentication host-mode multi-auth' which allows unlimited number of hosts on a single interface that is allowed per switching platform.

Step 1 Start interface configuration mode

```
SWITCH(config)#interface GigabitEthernetX/Y
SWITCH(config-if)#description ACCESS (Multi-Auth w/ Low-Impact Mode)
```

Step 2 Make port to access mode. Without this command the interface will not take 'authentication' related commands

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 10
SWITCH(config-if)#switchport voice vlan 11
```

Step 3 (Optional) Enable CDP & LLDP for device sensor (Should be enabled by default)

```
SWITCH(config-if)#cdp enable
SWITCH(config-if)#lldp receive
```

Step 4 Apply Pre-Auth ACL for low-impact mode

```
SWITCH(config-if)#ip access-group ACL-DEFAULT in
```

Step 5 Allows network access regardless of RADIUS response. This will need to be combined with the ACL above to control how much access is given for a device that fails the authentication

```
SWITCH(config-if)#authentication open
```

Note: The preceding command allows access prior to authentication, and if authentication fails (RADIUS sends back ACCESS-REJECT). However, if the RADIUS server sends back ACCESS-ACCEPT along with an authorization attribute, such as dVLAN and dACL, the authorization will be enforced for the

session. This means that if the dACL provides limited access to the network, regardless of 'authentication open' directive, the endpoint will have limited access per dACL.

Step 6 (Optional) Allows broadcast traffic in from the network to the unauthenticated port. This assists with WoL (Wake on LAN) process, so the network management server can wake the clients up on demand. It also assists in MAB process for certain types of devices that doesn't generate much traffic on its own without network request from another host.

```
SWITCH(config-if)#authentication control-direction in
```

Step 7 Allows port to move to MAB after 802.1x authentication fails

```
SWITCH(config-if)#authentication event fail action next-method
```

Step 8 (Optional) Allows port to fail-open/fail close when no RADIUS servers are available during authentication. If the port needs to fail-open, then assign same VLAN as access VLAN. If the port needs to fail-close, then assign dummy VLAN without SVI. This only impacts devices connecting while none of the RADIUS servers are reachable. Devices already connected prior to this event will not be impacted. Note that the DEFAULT-ACL is still in effect on this port which may impact the user experience for the user trying to authenticate while none of the ISE nodes configured on the switch are available.

```
SWITCH(config-if)#authentication event server dead action reinitialize vlan 10
```

Note: The VLAN ID can be any VLAN that is defined on the local switch. In the event that none of the ISE nodes are available and if Fail-Open is desired in such condition then recommended to set this to the same VLAN ID as regular user VLAN. On the other hand, if Fail-Close is desired then this can be set to a VLAN ID without SVI.

Step 9 (Optional) Allows voice device to be authorized to assigned voice VLAN when none of the RADIUS servers are available.

```
SWITCH(config-if)#authentication event server dead action authorize voice
```

Step 10 (Optional) When the RADIUS servers are reachable, the port reinitializes which will reauthenticate each endpoints on the interface. This command can be omitted if desired behavior is to leave the port fail-open/fail-closed even after the server is reachable again

```
SWITCH(config-if)#authentication event server alive action reinitialize
```

Step 11 Puts the port into multi-auth mode, which allows one voice device and unlimited data devices. Depending on the switching platform, the port may be forced to the same VLAN for all data endpoints or multiple VLANs

```
SWITCH(config-if)#authentication host-mode multi-auth
```

Step 12 (Optional) You can configure an 802.1x port so that it shuts down, generates a syslog error, or discards packets from a new device when a device connects to an 802.1x-enable port the maximum number of allowed about devices have been authenticated on the port. The default setting is 'shutdown' where the port err-disables when the condition is met. 'restrict' allows the port to stay up but log the incident. Typically, this is not an issue on a multi-auth port as it allows multiple devices on the same interface, however, if two or more voice devices are connected or the interface is in multi-domain or single-host mode, the port could be in violation

```
SWITCH(config-if)#authentication violation restrict
```

Step 13 (Optional) Enable reauthentication & inactivity timer for the port. This command is needed whether the values is statically assigned on the port or derived from the RADIUS server.

```
SWITCH(config-if)#authentication periodic
```

Step 14 (Optional) Allows reauthenticate timer interval (Session timer) to be downloaded to the switch from the RADIUS server

```
SWITCH(config-if)#authentication timer reauthenticate server
```

Note: Attribute 27 (Session-Timeout) and 29 (Terminate-Action) can be set on the Radius server. With Attribute 28 value of 'RADIUS-Request', the session is reauthenticate. Setting it to 'Default' terminates the session and forces a restart. When no values are sent from the RADIUS server, no reauthentication timer is applied for the session.

Step 15 (Optional) Allow inactivity timer interval to be downloaded to the switch from the RADIUS server. The 'dynamic' keyword instructs the NAD to send out ARP-Probe before removing the session to make sure the device is indeed disconnected.

```
SWITCH(config-if)#authentication timer inactivity server dynamic
```

Note: From the RADIUS server, Attribute 28 (Idle-Timeout) can set this. When no values are sent from the RADIUS server, no idle-timeout timer is applied for the session. Depending on the platform and the IOS version, this command may not be available.

Step 16 Enable MAC (MAC Authentication Bypass) on the port

```
SWITCH(config-if)#mab
```

Step 17 Trim down the interval for EAPoL Identity Request frames from the switch. When combined with retry value, this brings the time to wait for guest access to the network to 30 seconds. The default value for tx-period is 30 seconds, which brings the total wait time for guest devices to 90 seconds. When the wait time is 90 seconds, many devices give up on trying to obtain ip address from the network. We recommend that you start at 10 seconds, and trim down to lower value to enhance guest user experience, as required.

```
SWITCH(config-if)#dot1x timeout tx-period 10
```

Note: This value has less impact when the 'authentication open' directive is used on the interface, as the port is already open for network access prior to 802.1x authentication.

Step 18 Enable Spanning-Tree portfast for access port.

```
SWITCH(config-if)#spanning-tree portfast
```

Step 19 Following commands essentially enables 802.1x on the port. We recommend that you run these commands last, after rest of the 802.1x commands are entered.

```
SWITCH(config-if)#authentication port-control auto
SWITCH(config-if)#dot1x pae authenticator
```

Interface Level Configuration (Closed Mode Configuration)

The following interface configuration is Closed Mode configuration. In this mode, the endpoint cannot pass any traffic until the endpoint successfully authenticates via 802.1X or MAB. Although not required, this configuration utilizes 'authentication host-mode multi-domain', which allows single voice device and single data device on a single interface.

Step 1 Start interface configuration mode.

```
SWITCH(config)#interface GigabitEthernetX/Y
SWITCH(config-if)#description ACCESS (Multi-Domain w/ Closed Mode)
```

Step 2 Make port to access mode. Without this command, the interface will not take 'authentication' related commands.

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 10
SWITCH(config-if)#switchport voice vlan 11
```

Step 3 (Optional) Enable CDP & LLDP for device sensor (Should be enabled by default)

```
SWITCH(config-if)#cdp enable
SWITCH(config-if)#lldp receive
```

Step 4 (Optional) Allows broadcast traffic in from the network to the unauthenticated port. This assists with WoL process, so the network management server can wake the clients up on demand. It also assists in MAB process for certain types of devices that doesn't generate much traffic on its own without network request from another host.

```
SWITCH(config-if)#authentication control-direction in
```

Step 5 Allows port to move to MAB after 802.1x authentication fails.

```
SWITCH(config-if)#authentication event fail action next-method
```

Step 6 (Optional) Allows the port to fail-open/fail close when no RADIUS servers are available during authentication. If the port needs to fail-open, then assign same VLAN as access VLAN. If the port needs to fail-close, then assign dummy VLAN without SVI. This only impacts devices connecting when none of the RADIUS servers are reachable. Devices already connected prior to this event will not be impacted. Note that the DEFAULT-ACL is still in effect on this port

```
SWITCH(config-if)#authentication event server dead action authorize
```

Note: VLAN ID can be specified at the end of the command to designate the VLAN ID when Critical event occurs. When omitted it will use the VLAN specified in the 'switchport access vlan' command.

Step 7 (Optional) Allows voice device to be authorized to assigned voice VLAN when none of the RADIUS servers are available.

```
SWITCH(config-if)#authentication event server dead action authorize voice
```

Step 8 (Optional) When the RADIUS servers are reachable, the port reinitializes, which reauthenticates each endpoint on the interface. This command can be omitted if the desired behavior is to leave the port fail-open/fail-closed even after the server is reachable.

```
SWITCH(config-if)#authentication event server alive action reinitialize
```

Step 9 Puts the port into multi-domain mode, which allows one voice device and one data devices.

```
SWITCH(config-if)#authentication host-mode multi-domain
```

Step 10 (Optional) You can configure an 802.1x port to shut down, generate a syslog error, or discard packets when a new device connects to an 802.1x-enabled port and the maximum number of allowed about devices have been authenticated on that port. The default setting is 'shutdown' where the port err-disables when the condition is met. 'restrict' allows the port to stay up and log the incident. Typically, this is not an issue on a multi-auth port as it allows multiple devices on the same interface, however, if two or more voice devices are connected, the port could be in violation.

```
SWITCH(config-if)#authentication violation restrict
```

Step 11 (Optional) Enable reauthentication & inactivity timer for the port. This command is needed whether the values is statically assigned on the port or derived from the RADIUS server.

```
SWITCH(config-if)#authentication periodic
```

Step 12 (Optional) Allows the reauthenticate timer interval (Session timer) to be downloaded to the switch from the RADIUS server.

```
SWITCH(config-if)#authentication timer reauthenticate server
```

Step 13 (Optional) Allows the inactivity timer interval to be downloaded to the switch from the RADIUS server. The 'dynamic' keyword instructs the NAD to send out an ARP-Probe before removing the session to make sure the device is indeed disconnected.

```
SWITCH(config-if)#authentication timer inactivity server dynamic
```

Note: From the RADIUS server, Attribute 28 (Idle-Timeout) can set this. When no values are sent from the RADIUS server, no idle-timeout timer is applied for the session. Depending on the platform and the IOS version, this command may not be available.

Step 14 Enables MAC (MAC Authentication Bypass) on the port.

```
SWITCH(config-if)#mab
```

Step 15 Trims down the interval for EAPoL Identity Request frame from the switch. When combined with retry value, this brings the time to wait for guest access network to 30 seconds. The default value for tx-period is 30 seconds, which brings the total wait time for guest devices to 90 seconds. Many devices stop trying to obtain an ip address from the network before 90 seconds. We recommend starting at 10 seconds, and trimming down to a lower value to enhance guest user experience, as required.

```
SWITCH(config-if)#dot1x timeout tx-period 10
```

Step 16 Enable Spanning-Tree portfast for the access port.

```
SWITCH(config-if)#spanning-tree portfast
```

Step 17 Following commands essentially enables 802.1x on the port. We recommend that you run these commands last, after rest of the 802.1x commands are entered.

```
SWITCH(config-if)#authentication port-control auto
SWITCH(config-if)#dot1x pae authenticator
```

Appendix A: Sample Configuration

Global Configuration with device sensor

```
ip domain-name EXAMPLE.COM
username RADIUS-TEST password 0 PASSWORD
crypto key generate rsa general-keys mod 2048
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting update newinfo periodic 2880
aaa server radius dynamic-author
 client 10.1.200.11 server-key RADIUS_KEY
 client 10.1.200.12 server-key RADIUS_KEY
aaa session-id common
dot1x system-auth-control
dot1x critical eapol
ip device tracking
vlan 10
 name USER
vlan 11
 name VOICE
vlan 100
 name MGMT
interface 10
 ip address 10.1.10.1 255.255.255.0
ip helper-address 10.1.200.10
interface 11
 ip address 10.1.11.1 255.255.255.0
ip helper-address 10.1.200.10
interface 100
 ip address 10.1.100.1 255.255.255.0
ip http server
ip access-list extended ACL_WEBAUTH_REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended ACL-DEFAULT
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny   ip any any
radius-server vsa send authentication
radius-server vsa send accounting
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius server ISE01
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST probe-on
 # For IOS & IOS-XE without 'probe-on' feature use following command instead
 ! automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
 key RADIUS_KEY
radius server ISE02
 address ipv4 10.1.200.12
 automate-tester username RADIUS-TEST probe-on
 # For IOS & IOS-XE without 'probe-on' feature use following command instead
 ! automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
 key RADIUS_KEY
aaa group server radius ISE
 server name ISE01
 server name ISE02
 deadtime 15
radius-server dead-criteria time 10 tries 3
```

```
ip radius source-interface vlan 100
device-sensor filter-list dhcp list TLV-DHCP
 option name host-name
 option name requested-address
 option name parameter-request-list
 option name class-identifier
 option name client-identifier
device-sensor filter-spec dhcp include list TLV-DHCP
cdp run
device-sensor filter-list cdp list TLV-CDP
 tlv name device-name
 tlv name address-type
 tlv name capabilities-type
 tlv name platform-type
device-sensor filter-spec cdp include list TLV-CDP
lldp run
device-sensor filter-list lldp list TLV-LLDP
 tlv name system-name
 tlv name system-description
device-sensor filter-spec lldp include list TLV-LLDP
device-sensor accounting
device-sensor notify all-changes
no macro auto monitor
access-session template monitor
end
write memory
```

Global Configuration without device sensor

```
ip domain-name EXAMPLE.COM
username RADIUS-TEST password 0 PASSWORD
crypto key generate rsa general-keys mod 2048
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting update newinfo periodic 2880
aaa server radius dynamic-author
 client 10.1.200.11 server-key RADIUS_KEY
 client 10.1.200.12 server-key RADIUS_KEY
aaa session-id common
dot1x system-auth-control
dot1x critical eapol
ip device tracking
vlan 10
 name USER
vlan 11
 name VOICE
vlan 100
 name MGMT
interface 10
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
interface 11
 ip address 10.1.11.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
interface 100
 ip address 10.1.100.1 255.255.255.0
ip http server
ip access-list extended ACL_WEBAUTH_REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE
 permit tcp any any eq www
```

```
 permit tcp any any eq 443
ip access-list extended ACL-DEFAULT
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny   ip any any
radius-server vsa send authentication
radius-server vsa send accounting
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius server ISE01
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
 key RADIUS_KEY
radius server ISE02
 address ipv4 10.1.200.12
 automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
 key RADIUS_KEY
aaa group server radius ISE
 server name ISE01
 server name ISE02
 deadtime 15
radius-server dead-criteria time 10 tries 3
ip radius source-interface vlan 100
snmp-server community SNMP_COMMUNITY_STRING RO
ip dhcp snooping
ip dhcp snooping vlan 10, 11
end
write memory
```

Interface Level Configuration for Trunked interfaces (Uplink ports)

```
description Trunk (Uplink)
switchport mode trunk
ip device tracking maximum 0
```

Interface Level Configuration for Low-Impact Mode

```
description ACCESS (Multi-Auth w/ Low-Impact Mode)
switchport mode access
switchport access vlan 10
switchport voice vlan 11
ip access-group ACL-DEFAULT in
authentication open
authentication event fail action next-method
authentication event server dead action reinitialize vlan 10
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
mab
authentication violation restrict
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
dot1x timeout tx-period 10
spanning-tree portfast
authentication port-control auto
dot1x pae authenticator
```

Interface Level Configuration for Closed Mode

```
description ACCESS (Closed Mode)
switchport mode access
switchport access vlan 10
switchport voice vlan 11
authentication event fail action next-method
authentication event server dead action authorize
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-domain
mab
authentication violation restrict
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
dot1x timeout tx-period 10
spanning-tree portfast
authentication port-control auto
dot1x pae authenticator
```