Check compatibility before using: https://communities.cisco.com/docs/DOC-72932
Device Sensor only supported on specific IOS 15+/ IOS XE 3.6 and up releases

All commands below are under configure terminal
! Begin Global config with Device Sensor
ip domain-name [Domain]
! Test user to verify ISE node availability
! User account does not have to authenticate successfully
username [test user] secret 0 [password]
! HTTPS services are required for URL redirect
! Generate keys before enabling HTTPS
crypto key generate rsa general-keys mod 2048
aaa new-model
! If AAA was not enabled previously
! Enable local switch login authentication and authorization
aaa authentication login default local
aaa authorization exec default local
aaa authentication dot1x default group ISE-RADIUS
aaa authorization network default group ISE-RADIUS
aaa accounting dot1x default start-stop group ISE-RADIUS
aaa accounting network default start-stop group ISE-RADIUS
aaa accounting update newinfo periodic 2880
aaa server radius dynamic-author
  client [ISE1 IP] server-key [RADIUS secret]
  client [ISE2 IP] server-key [RADIUS secret]
aaa session-id common
authentication mac-move permit
epm access-control open
dot1x system-auth-control
dot1x critical eapol
! IP Device Tracking on IOS 15.2(2) or IOS-XE 03.06.00 and above
ip device tracking probe auto-source
! IP Device Tracking on earlier IOS/IOS-XE releases
ip device tracking probe delay 10
! Enable HTTP for redirect
ip http server
! Disable HTTP based admin access to switch
! Don’t enable if you need GUI access or use Prime Infrastructure
ip http active-session-modules none
ip http secure-active-session-modules none
! Limit HTTP connections
ip http max-connections 40

```
! Create the web auth redirect ACL
ip access-list extended ACL_WebAuth
   permit tcp any any eq www
! Create the ACL used for blacklisted devices
ip access-list extended Blackhole
   permit udp any any eq domain-name
   permit udp any eq bootpc any eq bootps
   permit tcp any host [ISE1 IP] eq 8443
   permit tcp any host [ISE2 IP] eq 8443
! Create the low-impact mode ACL applied before RADIUS auth
ip access-list extended ACL_Default
   permit udp any any eq domain-name
   permit udp any eq bootpc any eq bootps
   permit tcp any host [ISE1 IP] eq 8443
   permit tcp any host [ISE2 IP] eq 8443
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 attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
! Define the RADIUS servers and RADIUS group
radius server ISE1
   address ipv4 [ISE1 IP] auth-port 1812 acct-port 1813
   ! Automated tester for IOS 15.2(2) & IOS-XE 03.06.00 and above
   automate-tester username [RADIUS test account] probe-on
   ! Automated tester for earlier IOS/IOS-XE releases
   automate-tester username [RADIUS test account] ignore-acct-port idle-time 10
   key [RADIUS secret]
radius server ISE2
   address ipv4 [ISE2 IP] auth-port 1812 acct-port 1813
   ! Automated tester for IOS 15.2(2) & IOS-XE 03.06.00 and above
   automate-tester username [RADIUS test account] probe-on
   ! Automated tester for earlier IOS/IOS-XE releases
   automate-tester username [RADIUS test account] ignore-acct-port idle-time 10
   key [RADIUS secret]
aaa group server radius ISE-RADIUS
   server name ISE1
   server name ISE2
   deadtime 15
radius-server dead-criteria time 10 tries 3
```

```
ip radius source-interface Loopback0
! DHCP snooping is required for device sensor data to work properly
! Uplink interface must be trusted for DHCP traffic
! This is required if DHCP snooping is enabled. Otherwise, DHCP will fail.
! Use on the Port channel if uplinks are in a port channel
interface [uplink interface]
   ip dhcp snooping trust
ip dhcp snooping
no ip dhcp snooping information option
! VLAN list is comma separated
ip dhcp snooping vlan [1,10,15]
! Enable specific device sensors for profiling
device-sensor filter-list dhcp list dhcp_list
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 dhcp_list
! Enable CDP globally
cdp run
device-sensor filter-list cdp list cdp_list
tlv name device-name
tlv name address-type
tlv name capabilities-type
tlv name platform-type
device-sensor filter-spec cdp include list cdp_list
! Enable LLDP globally
lldp run
device-sensor filter-list lldp list lldp_list
tlv name system-name
tlv name system-description
tlv name system-capabilities
device-sensor filter-spec lldp include list lldp_list
! Send sensor data to ISE and disable local analyzer
device-sensor accounting
device-sensor notify all-changes
no macro auto monitor
access-session template monitor
```

```
# Access port interface configuration

! Use 'authentication host-mode multi-domain' to restrict port to one voice
! and one data device per port
! If port is used by an AP in FlexConnect mode, configure as trunk with allowed VLANs

! Interface config - Monitor Mode
interface GigabitEthernetX/Y
    switchport mode access
    switchport access vlan [id]
    switchport voice vlan [id]
    ! Allow access regardless of RADIUS response
    ! Only used for monitor and low-impact mode
    authentication open
    authentication control-direction in
    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-auth
    authentication violation restrict
    authentication periodic
    authentication timer reauthenticate server
    authentication timer inactivity server dynamic
    mab
    dot1x pae authenticator
    dot1x timeout tx-period 10
    spanning-tree portfast
    ip dhcp snooping limit rate 100
    authentication port-control auto

! Interface config - Low-Impact Mode
interface GigabitEthernetX/Y
    switchport mode access
    switchport access vlan [id]
    switchport voice vlan [id]
    ip access-group ACL_Default in
    ! Allow access regardless of RADIUS response
    ! Only used for monitor and low-impact mode
    authentication open
    authentication control-direction in
    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-auth
    authentication violation restrict
    authentication periodic
    authentication timer reauthenticate server
    authentication timer inactivity server dynamic
    mab
    dot1x pae authenticator
    dot1x timeout tx-period 10
    spanning-tree portfast
    ip dhcp snooping limit rate 100
    authentication port-control auto

! Interface config - Closed Mode
interface GigabitEthernetX/Y
    switchport mode access
    switchport access vlan [id]
    switchport voice vlan [id]
    authentication control-direction in
    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-auth
    authentication violation restrict
    authentication periodic
    authentication timer reauthenticate server
    authentication timer inactivity server dynamic
    mab
    dot1x pae authenticator
    dot1x timeout tx-period 10
    spanning-tree portfast
    ip dhcp snooping limit rate 100
    authentication port-control auto

** Template created by Brad Johnson **
** https://www.ise-support.com **
```