

This is for Denali or Everest release

Run this at enable prompt, not configure terminal
cts credentials id [device ID] password [password]

All commands below are under configure terminal
! Convert to new style authentication mode to enable C3PL
authentication convert-to new-style

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
! Enable HTTP for redirect
ip http server
! Disable HTTP based admin access to switch
! Don't disable 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

! Global AAA commands
! Enable AAA
aaa new-model
! If AAA was not enabled previously
! Enable local switch login authentication and authorization
aaa session-id common
aaa authentication dot1x default group radius
aaa authorization network default group radius
! AAA Authorization with TrustSec has to use a named list. Default is not allowed.
aaa authorization network ISE-CTS group ISE-RADIUS
cts authorization list ISE-CTS
aaa accounting identity 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
! Include PAN(s) if Policy persona is on a separate node.
! TrustSec configuration is pushed from the PAN.
client [ISE PSN 1 IP] server-key [RADIUS Secret]

```
client [ISE PSN 2 IP] server-key [RADIUS Secret]
```

```
! Global RADIUS commands
```

```
! Define the RADIUS servers (PSN) and RADIUS group
```

```
radius server [ISE PSN 1 name]
```

```
address ipv4 [ISE PSN 1 IP] auth-port 1812 acct-port 1813
```

```
automate-tester username [test user] probe-on
```

```
pac key [RADIUS secret]
```

```
radius server [ISE PSN 2 name]
```

```
address ipv4 [ISE PSN 2 IP] auth-port 1812 acct-port 1813
```

```
automate-tester username [test user] probe-on
```

```
pac key [RADIUS secret]
```

```
aaa group server radius ISE-RADIUS
```

```
server name [ISE PSN 1 name]
```

```
server name [ISE PSN 2 name]
```

```
deadtime 15
```

```
radius-server dead-criteria time 10 tries 3
```

```
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
```

```
! Send RADIUS traffic from management VLAN/IP
```

```
ip radius source-interface vlan [Management VLAN ID]
```

```
! Local ACLs and Service Templates
```

```
! Create the web auth redirect ACL
```

```
ip access-list extended ACL_WebAuth
```

```
deny udp any any eq domain
```

```
deny udp any eq bootpc any eq bootps
```

```
permit tcp any any eq www
```

```
! Create the low-impact mode ACL applied before RADIUS auth
```

```
ip access-list extended ACL_Default
```

```
permit udp any any eq domain
```

```
permit udp any eq bootpc any eq bootps
```

```
permit tcp any host [ISE PSN 1 IP] eq 8443
```

```
permit tcp any host [ISE PSN 2 IP] eq 8443
```

```
! Create ACL used when AAA is down
```

```
ip access-list extended AAA-Down
```

```
permit ip any any
```

```
! Create critical service template for when AAA is down
```

```
service-template CRITICAL
  description Apply when no RADIUS servers are available
  access-group AAA-Down
```

```
! Global 802.1x commands
! Enable 802.1x globally
dot1x system-auth-control
dot1x critical eapol
! Allow session tear down when MAC address detected elsewhere
! Mainly used when non-Cisco devices are moved between Cisco switches
no access-session mac-move deny
```

```
! Enable device sensors
! DHCP snooping is required for device sensor data to work properly
ip dhcp snooping
no ip dhcp snooping information option
! VLAN list is comma separated
ip dhcp snooping vlan [VLANs]
```

```
! 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 notify all-changes
access-session attributes filter-list list sensor_list
cdp
lldp
dhcp
access-session accounting attributes filter-spec include list sensor_list
```

```
! Configure control classes
! Control class for when AAA is down
class-map type control subscriber match-any AAA-Down
    match result-type aaa-timeout
```

```
! Control class for when 802.1x fails for session
class-map type control subscriber match-all Dot1x-Failed
    match method dot1x
    match result-type method dot1x authoritative
```

```
! Configure policy maps
! Policy map applied to all Dot1x/MAB interfaces
policy-map type control subscriber Dot1x-Default
    event session-started match-all
        10 class always do-all
            10 authenticate using dot1x priority 10
            20 authenticate using mab priority 20
    event violation match-all
        10 class always do-all
            10 restrict
    event agent-found match-all
        10 class always do-all
            10 terminate mab
            20 authenticate using dot1x
    event authentication-failure match-all
        10 class AAA-Down do-all
            10 authorize
            20 activate service-template CRITICAL
            30 terminate dot1x
            40 terminate mab
        20 class Dot1x-Failed
            10 authenticate using mab
```

```
! Create IP device tracking policy
device-tracking tracking auto-source
device-tracking policy IP-Tracking
```

```
security-level glean
tracking enable
no protocol udp
```

```
! Enable CTS role based enforcement and SXP
! Enforce CTS on all VLANs or comma separated list
cts role-based enforcement
cts role-based enforcement vlan-list all
cts sxp enable
cts sxp default password [SXP Password]
cts sxp connection peer [ISE PSN 1 IP] password default mode local listener hold-time 0
cts sxp connection peer [ISE PSN 2 IP] password default mode local listener hold-time 0
```

```
! Uplink interface must be trusted for DHCP traffic
! This is required if DHCP snooping is enabled. Otherwise, DHCP will fail.
! If there is a port channel configured for the uplink ports, add to the
! port channel interface configuration instead of the port interface.
interface [uplink interface]
    ip dhcp snooping trust
! Enable CTS authorization and forwarding
    cts manual
! Enable CTS propagation
    propagate sgt
! Set trustworthiness of SGT received on ingress
    policy static sgt [sgt value] trusted
! Disable enforcement on the uplink
    no cts role-based enforcement
```

```
# Access port interface configuration
```

```
! Be sure to remove any switchport port-security settings from the port
! Use "access-session host-mode multi-auth" only if all devices on the port will
! be assigned the same SGT.
! If port is used by an AP in FlexConnect mode, configure as trunk with allowed VLANs
```

```
! Monitor mode
```

```
interface GigabitEthernetX/Y
    switchport mode access
    subscriber aging probe
    service-policy type control subscriber Dot1x-Default
    ! Apply device tracking policy to port if not assigned to VLAN
    device-tracking attach-policy IP-Tracking
    authentication periodic
```

```
authentication timer reauthenticate server
mab
access-session host-mode multi-domain
no access-session closed
dot1x pae authenticator
dot1x timeout tx-period 10
ip dhcp snooping limit rate 100
access-session port-control auto
no switchport port-security
```

! Low-impact mode

```
interface GigabitEthernetX/Y
  switchport mode access
  subscriber aging probe
  service-policy type control subscriber Dot1x-Default
  ! Apply device tracking policy to port if not assigned to VLAN
  device-tracking attach-policy IP-Tracking
  authentication periodic
  authentication timer reauthenticate server
  mab
  ! Limit access with open authentication
  ip access-group ACL_Default in
  access-session host-mode multi-domain
  dot1x pae authenticator
  dot1x timeout tx-period 10
  no access-session closed
  ip dhcp snooping limit rate 100
  access-session port-control auto
  no switchport port-security
```

! Closed mode

```
interface GigabitEthernetX/Y
  switchport mode access
  subscriber aging probe
  service-policy type control subscriber Dot1x-Default
  ! Apply device tracking policy to port if not assigned to VLAN
  device-tracking attach-policy IP-Tracking
  authentication periodic
  authentication timer reauthenticate server
  mab
  access-session host-mode multi-domain
  dot1x pae authenticator
  dot1x timeout tx-period 10
```

```
! Enable closed mode
access-session closed
ip dhcp snooping limit rate 100
access-session port-control auto
no switchport port-security
```

```
# Apply device tracking policy to the VLAN instead of each port
interface [VLAN ID]
```

```
    device-tracking attach-policy IP-Tracking
```

```
** Template created by Brad Johnson **
```

```
** https://www.ise-support.com **
```