Change of Authorization

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

Identity-Based Networking Services supports change of authorization (CoA) commands for session query, reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation.

Feature Information for Change of Authorization

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Change of Authorization

Feature Name	Releases	Feature Information
Change of Authorization	Cisco IOS XE Amsterdam 17.4.1	The Change of Authorization The following commands were introduced by this feature: **show aaa servers**, **show aaa group radius**, **show device-tracking policies**, **show device-tracking database** **show access-session interface** *interface-name*
Change of Authorization	Cisco IOS XE Amsterdam 17.3.1a	The Change of Authorization The following commands were introduced by this feature: **show ip access-lists**, **show ip access-list interface** , **debug epm plugin acl event**, **debug epm plugin acl errors**

Information About Change of Authorization

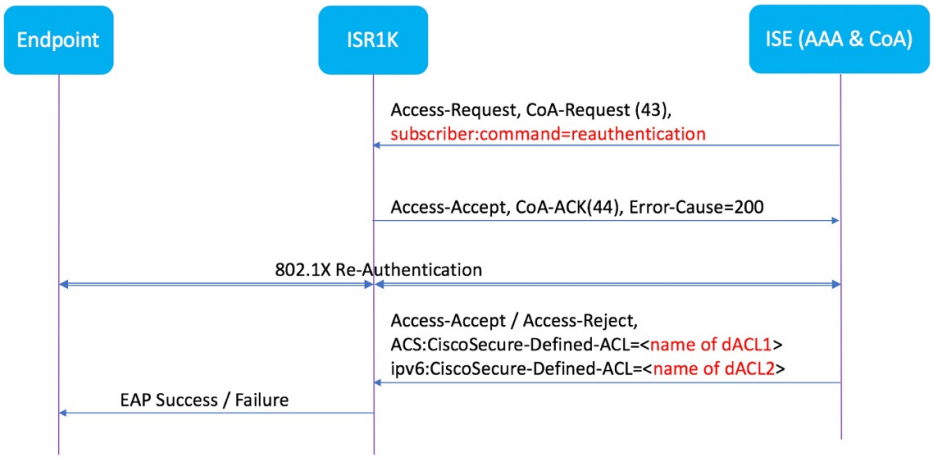
Change of Authorization-Reauthentication Procedure

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. The main steps in this procedure are:

- Authentication
- Posture Assessment
- CoA Re-Authentication
- Network Access Authorization

When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server, such as a Cisco Identity Secure Engine (ISE) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

The RADIUS CoA provides a mechanism to change the attributes of an AAA session after it is authenticated. When policy changed on user or user group in RADIUS server, administrators can initiate RADIUS CoA process from RADIUS server to re-authenticate or re-authorize new policy



By default, the RADIUS interface is enabled on the device. However, some basic configuration is required for the following attributes:

- Security and Password
- Accounting

After posture assessment is succeessful, full network access is pushed down to the device for specific client through CoA re-authentication command based on its compliance state derived from last assessment. It is

optional to enforce downloadable ACLs with Permit-ALL or limited access to certain resources to corresponding clients. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

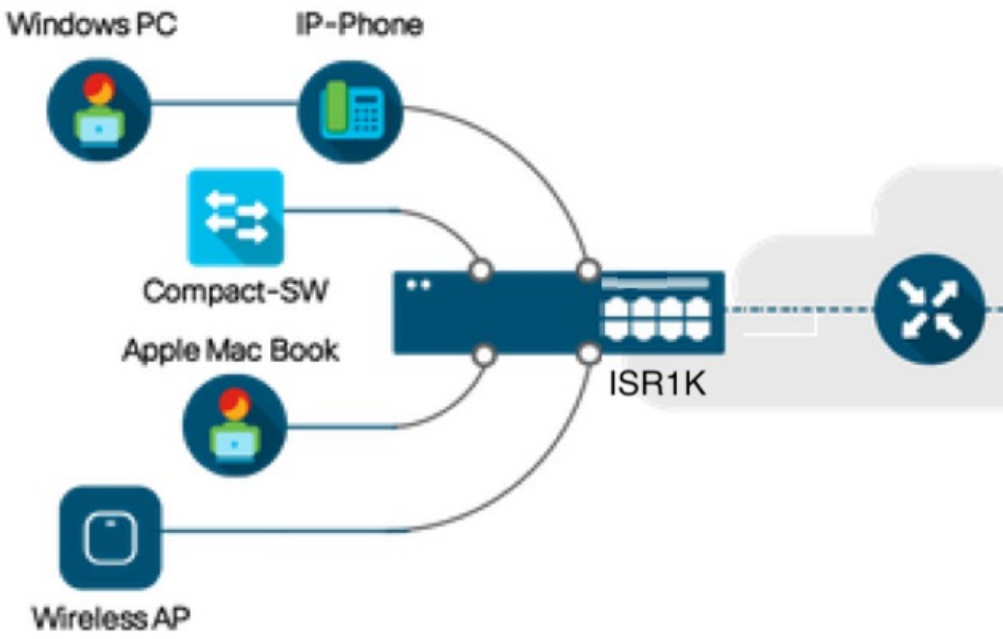
- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

Change of Authorization

Change of Authorization (CoA) is a critical part of a solution to initiate re-authenticate or re-authorization to an endpoint's network access based on its posture assessment result. This feature is integrated with Cisco AnyConnect, version 4.8 and Cisco ISE, version 2.6.

The network topology below shows a typical Cisco 1000 Series Integrated Services Router as a branch router in a network for secure access with ISE and other network services deployed in Campus or Data Center.

Figure 1: Cisco ISR1000 in a Network for Secure Access with ISE and other Network Services



CoA is critical part of the solution to initiate re-authenticate or re-authorization to endpoint's network access based on its posture assessment result. Downloadable ACL is the Target/Purpose of the entire solution. The per-client basis customized security policies are achieved by it.

Restrictions for Change of Authorization

- Only 8 ports SKUs have TCAM to support DACL and Redirect ACL
- xACL can only match exact value(>,<,>=,<= are not supported)

- Switch ASIC TCAM has only 255 entries (IPv4 ACL entries) in total
- No IPv4 option header support, no IP fragment support in ACL packet inspection
- IPv6 is not supported in this feature
- Port ACL is not supported in this feature
- SISF: Only support none-secure device-tracking (tracking policy with security level ‘glean’)
- Multi-auth vlan is not supported on Cisco 1000 Series Integrated Services Routers
- Tracking is not getting replaced by ‘enable tracking‘
- VLAN change does not happen consistently with multiple iterations on client interfaces

How to Configure Change of Authorization

Essential dot1x | SANet Configuration

```
aaa new-model
aaa authentication dot1x default group coa-ise
aaa authorization network default group coa-ise
dot1x system-auth-control
aaa group server radius coa-ise
 server name coa
radius server coa
 address ipv4 10.10.1.10 auth-port 1812 acct-port 1813
 key cisco123
policy-map type control subscriber simple_coa
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
interface gigabitethernet0/0/1
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticator
service-policy type control subscriber simple_coa
```

Configure Change of Authorization

```
aaa server radius dynamic-author
 client
 server-key ******
 auth-type any
 ignore server-key
ip access-list extended redirect_acl
 20 deny udp any eq bootps any
 25 deny udp any eq domain any
 30 deny udp any any eq bootpc
 40 deny udp any eq bootpc any
 50 deny ip any host %{ise.ip}
 60 permit tcp any any eq www
```

```
 70 permit tcp any any eq 443
device-tracking tracking
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
interface 0/0/1
 device-tracking attach-policy tracking_test
```

Configuration Examples for Change of Authorization

Example: Check if the RADIUS Server is Active

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 10.75.28.231, auth-port 1812, acct-port 1813, hostname host
     State: current UP, duration 188755s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 188755s, previous duration 0s
```

Example: Device Tracking Policy

```
Device# show aaa group radius coa3 **** port 1813 new-code
User successfully authenticated
USER ATTRIBUTES
username             0   "coa3"
```

To check if the parameters are enabled:

```
Device# show device-tracking policies
Target               Type  Policy               Feature        Target range
Gi0/1/1              PORT  tracking_test        Device-tracking vlan all
Gi0/1/2              PORT  tracking_test        Device-tracking vlan all
Gi0/1/3              PORT  tracking_test        Device-tracking vlan all
Gi0/1/4              PORT  tracking_test        Device-tracking vlan all
```

To check the SISF table:

```
Device# show device-tracking database
Binding Table has 1 entries, 1 dynamic (limit 100000)
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
Network Address        Link Address       Interface  vlan  prlvl    age    state       Time
 left
ARP 10.11.22.20       0050.5683.3f97      Gi0/1/4     22    0005    11s   REACHABLE
295 s
```

To check if the access-session is authenticated and autorized:

```
Device# show access-session interface gigabitEthernet 0/1/7 detail
            Interface:  GigabitEthernet0/1/7
               IIF-ID:  0x0DB9315A
```

```
       MAC Address:  b496.913d.4f9b
      IPv6 Address:  Unknown
      IPv4 Address:  10.10.22.27
         User-Name:  coa2
         Status:  Authorized
            Domain:  DATA
    Oper host mode:  multi-auth
  Oper control dir:  both
   Session timeout:  N/A
 Common Session ID:  611C4B0A00000053F483D7B0
   Acct Session ID:  Unknown
            Handle:  0x21000049
    Current Policy:  POLICY_COA
Server Policies:  Filter-ID: Filter_ID_COA2
Method status list:  Method           State
                     dot1x           Authc Success
```