

Downloadable ACL

DACL är en teknik som tillåter ACL-applisering vid Radius/dot1x-autentisering. Tekniken lämpar sig väl för att implementera klientisolering inom samma subnät närmast användaren.

Själva accesslistan byggs i ISE under Policy > Policy Elements > Authorization > Downloadable ACLs. En ACL kan vara så lätt att den tillåter eller nekar all trafik. Observera att man använder en DACL per protokoll, i händelse av dual-stack behövs två DACL. ACLn byggs enligt IOS-standard, ex:

```
permit icmp any any
deny ip any 192.168.1.0 0.255.255.255
permit ip any any
```

För att DACLn ska användas måste den kopplas mot den Authorization Policy som används i Policy Set:et. Lägg till DACL i Common Tasks enligt skärmdumpen.

image.png

När den här sedan är applicerad i Policy Set:et kan man verifiera att den har blivit tillämpad i show access-session, se exempel:

```
c9300#show access-session interface gigabitEthernet 1/0/3 details
  Interface: GigabitEthernet1/0/3
    IIF-ID: 0x19AE4F44
  MAC Address: aaaa.bbbb.ccc
  IPv6 Address: fe80::aaa:bbbb:cccc:ddd
  IPv4 Address: 192.168.1.1
  User-Name: client
    Status: Authorized
    Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 140BA8C000001D44B98DD61C
  Acct Session ID: Unknown
    Handle: 0x3c000d3d
  Current Policy: POLICY_Gi1/0/3
```

Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Security Policy: Should Secure

Security Status: Link Unsecured

Server Policies:

Vlan Group: Vlan: 1337

ACS ACL: xACSACLx-IP-PERMIT_USER_IPv4-64f82bfd

ACS ACL IPV6: xACSACLx-IPV6-PERMIT_USER_IPv6-664d9894

Method status list:

Method	State
dot1x	Authc Success

Det går även att titta på ACL:en "precis som vanligt", så länge någon port använder sig av den och den därmed är nedladdad.

```
c9300#show ip access-lists xACSACLx-IP-PERMIT_USER_IPv4-64f82bfd
```

```
Extended IP access list xACSACLx-IP-PERMIT_USER_IPv4-64f82bfd
```

```
1 permit icmp any any
```

```
2 deny ip any 192.168.1.0 0.255.255.255
```

```
3 permit ip any any
```

Revision #1

Created 26 April 2025 11:56:39 by Jehrlander

Updated 26 April 2025 11:56:45 by Jehrlander