# Downloadable ACL



## Feature History for Downloadable ACL

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

***Table 1: Feature History for Downloadable ACL***

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Dublin 17.10.1 | Downloadable ACL | The Downloadable ACL (dACL) feature defines and updates access control lists (ACLs) in one place (Cisco ISE) and allows ACL download to all the applicable controllers.<br><br>In Cisco IOS-XE 17.8 and earlier releases, you had to configure the name in Cisco ISE and define the ACL individually in each of the controllers.<br><br>The dACL feature is supported only in a centralized controller with Local mode Access Points.<br><br>**Note** The dACL feature is not supported in RLAN environments. |

# Information About Downloadable ACL

ACLs are used to restrict network access to some users or devices based on predefined criteria. These criteria are specified as a list of Access Control Entries (ACEs).

Each ACE has a matching condition based on packet header fields as follows:

- IP addresses
- ports
- protocols
- combination of IP addresses, ports, and protocols
- Result (permit or deny)

ACLs are applied to a controller on a per wireless client basis. Typically, you can configure ACLs in a controller itself. However, you can also configure ACLs to a connected Cisco ISE server and download them to the controller when a wireless client joins. Such ACLs are referred to as downloadable ACLs, per-user Dynamic ACLs, or dACLs.

Downloadable ACLs are easy to maintain because they define or update ACLs in Cisco ISE and can be downloaded to all the applicable controllers. (In Cisco IOS-XE 17.8 and earlier releases, you had to configure the name in Cisco ISE and define the ACL individually in each of the controllers.)

## Scale Considerations for Downloadable ACL

The following table provides the ACL scale numbers for controllers.

***Table 2: ACL Scale for Controllers***

| Controllers | ACL Scale |
|---|---|
| Cisco Catalyst 9800-40 Wireless Controller (small or medium) | Supports 128 ACLs with 128 ACEs. |
| Cisco Catalyst 9800-80 Wireless Controller (large) | Supports 256 ACLs and 256 ACEs. |

# Guidelines and Restrictions for Downloadable ACL

- dACL does not support FlexConnect local switching.
- IPv6 dACLs are supported only in Cisco ISE 3.0 or a later release.
- The dACL feature is supported only in a centralized controller with Local mode Access Points.

**Note** The dACL feature is not supported in RLAN environments.

# Configuring dACL Name and Definition in Cisco ISE

Before you configure a dACL in a controller, you must configure the dACL name and definition in Cisco ISE. For more information, see Configure Per-User Dynamic Access Control Lists in ISE.

# Configuring dACL in a Controller (CLI)

### Before you begin

- You should have configured the RADIUS server.
- You should have configured the **aaa-override** command in the policy profile. For more information, see **Configuring AAA for Local Authentication (CLI)**.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wireless profile policy** *policy-profile-name*<br>**Example:**<br>`Device(config)# wireless profile policy named-policy-profile_4` | Configures the wireless profile policy. |
| **Step 3** | **aaa-override**<br>**Example:**<br>`Device(config-wireless-policy)# aaa-override` | Configures AAA override to apply policies coming from the Cisco ISE servers. |
| **Step 4** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)# no shutdown` | Enables the profile policy. |

# Configuring Explicit Authorization Server List (CLI)

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **radius server** *server-name*<br>**Example:**<br>`Device(config)# radius server Test-SERVER2` | Specifies the RADIUS server name. |
| **Step 3** | **address ipv4** *ip-address*<br>**Example:**<br>`Device(config-radius-server)# address ipv4 124.3.52.62` | Specifies the RADIUS server parameters. |
| **Step 4** | **pac key** *key*<br>**Example:**<br>`Device(config-radius-server)# pack key cisco` | Specify the authorization and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server. |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-radius-server)# exit` | Returns to the configuration mode. |
| **Step 6** | **aaa group server radius** *server-group-name*<br>**Example:**<br>`Device(config)# aaa group server radius authz-server-group` | Creates a radius server-group identification.<br>**Note** *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters. |
| **Step 7** | **aaa authorization network** *authorization-list* **group** *server-group-name*<br>**Example:**<br>`Device(config)# aaa authorization network authZlist group authz-server-group` | Creates an authorization method list for web-based authorization.<br>**Note** You must use the already created authorization method list. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

# Verifying dACL Configuration

To verify the dACL, use the following command:

```
Device# show wireless client mac-address <client_mac> detail
Local Policies:
   Service Template : wlan_svc_named-policy-profile_1_local (priority 254)
    VLAN             : 16
    Absolute-Timer   : 1800
  Server Policies:
    ACS ACL          : xACSACLx-IP-tftpv4_2-62de6299
    ACS ACL          : xACSACLx-IPV6-tftpv6_2-62de8087
  Resultant Policies:
    ACS ACL          : xACSACLx-IP-tftpv4_2-62de6299
    ACS ACL          : xACSACLx-IPV6-tftpv6_2-62de8087
    VLAN Name        : VLAN0016
    VLAN             : 16
    Absolute-Timer   : 1800
```

To verify dACLs, use the following commands:

```
Device# show ip access-lists xACSACLx-IP-tftpv4_2-62de6299
Extended IP access list xACSACLx-IP-tftpv4_2-62de6299
    1 deny ip any host 9.8.29.13
    2 permit ip any any (58 matches)
```

```
Device# show ipv6 access-list xACSACLx-IPV6-tftpv6_2-62de8087
IPv6 access list xACSACLx-IPV6-tftpv6_2-62de8087
    deny ipv6 any host 2001:9:8:29:3AAD:A27A:973A:97CC sequence 1
    permit ipv6 any any (2 matches) sequence 2
```

To view all the downloaded dACLs, use the following command:

```
Device# show ip access-lists
```