Downloadable ACL

Downloadable ACLs

A downloadable ACL is a type of access control list that

- restricts network access to users or devices based on predefined criteria
- is specified as a list of Access Control Entries (ACEs), and
- can be maintained centrally in Cisco ISE and downloaded to controllers.

Supporting reference information

You can easily maintain and update ACLs in Cisco ISE.

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

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

ACLs are applied to each controller on a per-wireless-client basis.

Typically, you can configure ACLs in a controller itself. However, you can also configure ACLs on a connected Cisco ISE server and download them to the controller when a wireless client connects.

These ACLs are referred to as downloadable ACLs, per-user Dynamic ACLs, or dACLs.

You can easily maintain downloadable ACLs because they define or update ACLs in Cisco ISE and can be downloaded to all applicable controllers.

(In Cisco IOS-XE 17.8 and earlier releases, you must configure the name in Cisco ISE and define the ACL individually on each controller.)

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.

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. 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. The dACL feature is supported only in a centralized controller with Local mode APs. **Note** The dACL feature is not supported in RLAN environments.

Scale considerations for downloadable ACL

This table provides the ACL scale numbers for controllers.

ACL Scale for Controllers

- 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.

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.

Restrictions for downloadable ACL

Restrictions on dACL usage

These restrictions apply to downloadable ACLs (dACL):

- dACL does not support FlexConnect local switching.
- You can use IPv6 dACLs only in Cisco ISE 3.0 or later.
- You can use the dACL feature only in a centralized controller that uses Local mode Access Points.

Note The dACL feature is not supported in RLAN environments.

Configuring dACL name and definition in Cisco ISE

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

Configure dACL in a controller (CLI)

Before you begin

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

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the wireless profile policy.

Example:

```
Device(config)# wireless profile policy policy-profile-name
```

Step 3 Configure AAA override to apply policies coming from the Cisco ISE servers.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Step 4 Enable the profile policy.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Configure explicit authorization server list (CLI)

Deploy an explicit authorization server list for network authorization.

This configuration is used to set up RADIUS servers for network authorization in a Cisco device.

Before you begin

Ensure you have the necessary RADIUS server details and access to the device.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Specify the RADIUS server name.

Example:

```
Device(config)# radius server server-name
```

Step 3 Specify the RADIUS server parameters.

Example:

```
Device(config-radius-server)# address ipv4 ip-address
```

Step 4 Specify the authorization and encryption key used between the device and the RADIUS server.

Example:

```
Device(config-radius-server)# pac key key
```

Step 5 Return to the configuration mode.

Example:

```
Device(config-radius-server)# exit
```

Step 6 Create a RADIUS server-group identification.

Example:

```
Device(config)# aaa group server radius server-group-name
```

server-group-name refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.

Step 7 Create an authorization method list for web-based authorization.

Example:

```
Device(config)# aaa authorization network authorization-list group server-group-name
```

You must use the already created authorization method list.

Step 8 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The explicit authorization server list is now configured and ready for use.

Verify dACL configuration

To verify the dACL, use this 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 this 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 this command:

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