IEEE 802.1X with ACL Assignments

The IEEE 802.1X with ACL Assignments feature allows you to download access control lists (ACLs), and to redirect URLs from a RADIUS server to the switch, during 802.1X authentication or MAC authentication bypass of the host. It also allows you to download ACLs during web authentication.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Prerequisites for IEEE 802.1X with ACL Assignments

- You must configure a static ACL on the interface to support Cisco Discovery Protocol (CDP) bypass, because the auth-default-ACL does not support CDP bypass in single host mode.
- If you use a custom logo with web authentication and it is stored on an external server, the port ACL must allow access to the external server before authentication. You must either configure a static port ACL or change the auth-default-ACL to provide appropriate access to the external server.

Restrictions for IEEE 802.1X with ACL Assignments

- ACLs are not supported on fixed Cisco Integrated Services Routers (ISRs).
- This feature does not support standard ACLs on the switch port.

Information About IEEE 802.1X with ACL Assignments

Overview of 802.1X Authentication with Downloadable ACLs and Redirect URLs

You can download ACLs and redirect URLs from a RADIUS server to the switch during 802.1X authentication or MAC authentication bypass of the host. You can also download ACLs during web authentication.

Note A downloadable ACL is also referred to as a dACL.

If more than one host is authenticated and the host is in single-host, MDA, or multiple-authentication mode, the switch changes the source address of the ACL to the host IP address.

You can apply the ACLs and redirect URLs to all devices that are connected to the 802.1X-enabled port.

If no ACLs are downloaded during 802.1X authentication, the switch applies the static default ACL on the port to the host. On a voice VLAN port that is configured in multiple-authentication or MDA mode, the switch applies the ACL only to the phone as part of the authorization policies.

Beginning with Cisco IOS Release 12.2(55)SE, if there is no static ACL on a port, a dynamic auth-default-ACL is created, and policies are enforced before dACLs are downloaded and applied.

Note The auth-default-ACL does not appear in the running configuration.

The auth-default-ACL is created when at least one host with an authorization policy is detected on the port. The auth-default-ACL is removed from the port when the last authenticated session ends. You can configure the auth-default-ACL by using the **ip access-list extended auth-default-acl** global configuration command.

Note The auth-default-ACL does not support Cisco Discovery Protocol (CDP) bypass in single host mode. You must configure a static ACL on the interface to support CDP bypass.

The 802.1X and MAC authentication methods support two authentication modes, *open* and *closed* . If there is no static ACL on a port in *closed* authentication mode:

- An auth-default-ACL is created.
- The auth-default-ACL allows only DHCP traffic until policies are enforced.
- When the first host authenticates, the authorization policy is applied without IP address insertion.

- When a second host is detected, the policies for the first host are refreshed, and policies for the first and subsequent sessions are enforced with IP address insertion.

If there is no static ACL on a port in *open* authentication mode:

- An auth-default-ACL-OPEN is created and allows all traffic.
- Policies are enforced with IP address insertion to prevent security breaches.
- Web authentication is subject to the auth-default-ACL-OPEN.

To control access for hosts with no authorization policy, you can configure a directive. The supported values for the directive are *open* and *default* . When you configure the *open* directive, all traffic is allowed. The *default* directive subjects traffic to the access provided by the port. You can configure the directive in the user profile on the AAA server or on the switch. To configure the directive on the AAA server, use the **authz-directive =<open/default>** global command. To configure the directive on the switch, use the **epm access-control open** global configuration command.

Note The default value of the directive is *default*.

If a host falls back to web authentication on a port without a configured ACL:

- If the port is in open authentication mode, the auth-default-ACL-OPEN is created.
- If the port is in closed authentication mode, the auth-default-ACL is created.

The access control entries (ACEs) in the fallback ACL are converted to per-user entries. If the configured fallback profile does not include a fallback ACL, the host is subject to the auth-default-ACL that is associated with the port.

Note If you use a custom logo with web authentication and it is stored on an external server, the port ACL must allow access to the external server before authentication. You must either configure a static port ACL or change the auth-default-ACL to provide appropriate access to the external server.

Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL

The switch uses these *cisco-av-pair* VSAs:

- url-redirect is the HTTP to HTTPS URL.
- url-redirect-acl is the switch ACL name or number.

The switch uses the Cisco Secure-Defined-ACL attribute-value pair to intercept an HTTP or HTTPS request from the endpoint device. The switch then forwards the client web browser to the specified redirect address. The url-redirect attribute-value pair on the Cisco Secure ACS contains the URL to which the web browser is redirected. The url-redirect-acl attribute-value pair contains the name or number of an ACL that specifies the HTTP or HTTPS traffic to redirect. Traffic that matches a permit ACE in the ACL is redirected.

Note Define the URL redirect ACL and the default port ACL on the switch.

If a redirect URL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs

You can set the CiscoSecure-Defined-ACL attribute-value pair on the Cisco Secure ACS with the RADIUS cisco-av-pair vendor-specific attributes (VSAs). This pair specifies the names of the downloadable ACLs on the Cisco Secure ACS with the #ACL#-IP-name-number attribute.

- The name is the ACL name.
- The number is the version number (for example, 3f783768).

If a downloadable ACL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host-access-policy to the switch, it applies the policy to traffic from the host connected to a switch port. If the policy does not apply, the switch applies the default ACL. If the Cisco Secure ACS sends the switch a downloadable ACL, this ACL takes precedence over the default ACL that is configured on the switch port. However, if the switch receives a host access policy from the Cisco Secure ACS but the default ACL is not configured, authorization failure is declared.

How to Configure IEEE 802.1X with ACL Assignments

Configuring Downloadable ACLs

To configure a switch to accept downloadable ACLs or redirect URLs from the RADIUS server during authentication of an attached host, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip device tracking**
4. **aaa new-model**
5. **aaa authorization network default group radius**
6. **radius-server vsa send authentication**
7. **interface** *interface-id*
8. **ip access-group** *acl-id* **in**
9. end
10. **show running-config interface***interface-id*
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted .
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Enables the IP device tracking table.
Step 4	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 5	**aaa authorization network default group radius** **Example:** `Switch(config)# aaa authorization network default group radius`	Sets the authorization method. To remove the authorization method, use the **no aaa authorization network default group radius** command.

	Command or Action	Purpose
Step 6	**radius-server vsa send authentication** **Example:** `Switch(config)# radius-server vsa send autentication`	Configures the network access server.
Step 7	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode.
Step 8	**ip access-group** *acl-id* **in** **Example:** `Switch(config-if)# ip access-group 99 in`	Configures the default ACL on the port in the input direction. **Note** The ACL ID is an access list name or number.
Step 9	end	`Switch(config-if)# end` Returns to Privileged EXEC mode.
Step 10	**show running-config interface***interface-id* **Example:** `Switch# show running-config interface interface-id`	Displays the specific interface configuration for verification.
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Save entries in the configuration file.

Configuration Examples for IEEE 802.1X with ACL Assignments

Example: Configuring a Switch for a Downloadable Policy

The following example shows how to configure a switch for a downloadable policy:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface fastEthernet 2/13
Switch(config-if)# ip access-group default_acl in
```

```
Switch(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Authentication commands	*Cisco IOS Security Command Reference Commands A to C*
IPsec	*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 15.0*
RADIUS	"Configuring RADIUS" module.
Standalone MAB Support	*Standalone MAB Support*

Standards and RFCs

Standard/RFC	Title
IEEE 802.1X protocol	—
RFC 3580	*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*

MIBs

MIB	MIBs Link
• CISCO–AUTH–FRAMEWORK–MIB • CISCO–MAB–AUTH–BYPASS–MIB • CISCO–PAE–MIB • IEEE8021–PAE–MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IEEE 802.1X with ACL Assignments

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: IEEE 802.1X with ACL Assignments

Feature Name	Releases	Feature Information
IEEE 802.1X with ACL Assignments	15.2(2)T	The IEEE 802.1X with ACL Assignments feature provides the means to download ACLs, and to redirect URLs from a RADIUS server to the switch, during 802.1X authentication or MAC authentication bypass of the host. It also provides the means to download ACLs during web authentication.