Per-User ACL Support for 802.1X/MAB/Webauth Users

This feature allows per-user ACLs to be downloaded from the Cisco Access Control Server (ACS) as policy enforcement after authentication using IEEE 802.1X, MAB authentication bypass, or 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.

PrerequisitesforPer-UserACLSupportfor802.1X/MAB/Webauth Users

- AAA authentication must be enabled.

- AAA authorization must be enabled by using the **network** keyword to allow interface configuration from the RADIUS server.
- 802.1X authentication must be enabled.
- The user profile and VSAs must be configured on the RADIUS server.

Restrictions for Per-User ACL Support for 802.1X/MAB/Webauth Users

- Per-user Access Control Lists (ACLs) are supported only in single-host mode.
- This feature does not support standard ACLs on the switch port.
- Only one 802.1X-authenticated user is supported on a port. If the multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.
- The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.
- ACLs are not supported on fixed Cisco Integrated Services Routers (ISRs).

Information About Per-User ACL Support for 802.1X/MAB/Webauth Users

802.1X Authentication with Per-User ACLs

Per-user access control lists (ACLs) can be configured to provide different levels of network access and service to an 802.1X-authenticated user. When the RADIUS server authenticates a user that is connected to an 802.1X port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1X port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

Router ACLs and input port ACLs can be confiugured on the same switch. However, a port ACL takes precedence over a router ACL. If an input port ACL is applied to an interface that belongs to a VLAN, the port ACL takes precedence over an input router ACL that is applied to the VLAN interface. Incoming packets received on the port to which a port ACL is applied are filtered by the port ACL. Incoming routed packets received on other ports are filtered by the router ACL. Outgoing routed packets are filtered by the router ACL. To avoid configuration conflicts, the user profiles should be carefully planned and stored on the RADIUS server.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are inacl#<n > for the ingress direction and outacl#<n > for the egress direction. MAB ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It

does not support port ACLs in the egress direction on Layer 2 ports. For more information, see the "Configuring Network Security with ACLs|" module.

The extended ACL syntax style should be used to define the per-user configuration that is stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if the Filter-Id attribute is used, it can point to a standard ACL.

The Filter-Id attribute can be used to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by *.in* for ingress filtering or *.out* for egress filtering. If the RADIUS server does not allow the *.in* or *.out* syntax, the access list is applied to the outbound ACL by default. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and IP extended ACLs).

Only one 802.1X-authenticated user is supported on a port. If the multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

How to Configure Per-User ACL Support for 802.1X/MAB/Webauth Users

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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• 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.
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.

	Command or Action	Purpose
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Save entries in the configuration file.

Configuration Examples for Per-User ACL Support for 802.1X/MAB/Webauth Users

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*
Layer 2 ports	Configuring Network Security with ACLs

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 Per-User ACL Support for 802.1X/MAB/Webauth Users

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 Per-User ACL Support for 802.1X/MAB/Webauth Users

Feature Name	Releases	Feature Information
Per-User ACL Support for 802.1X/MAB/Webauth Users	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	This feature allows per-user ACLs to be downloaded from the Cisco Access Control Server (ACS) as policy enforcement after authentication using IEEE 802.1X, MAB authentication bypass, or web authentication. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.