Configuring NAC

This chapter describes how to configure Network Admission Control (NAC) on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information"chapter or the Feature History table in this chapter.

Information About NAC

NAC allows you to check endpoint devices for security compliancy and vulnerability before these devices are allowed access to the network. This security compliancy check is referred to as *posture validation*. Posture validation allows you to prevent the spread of worms, viruses, and other rogue applications across the network.

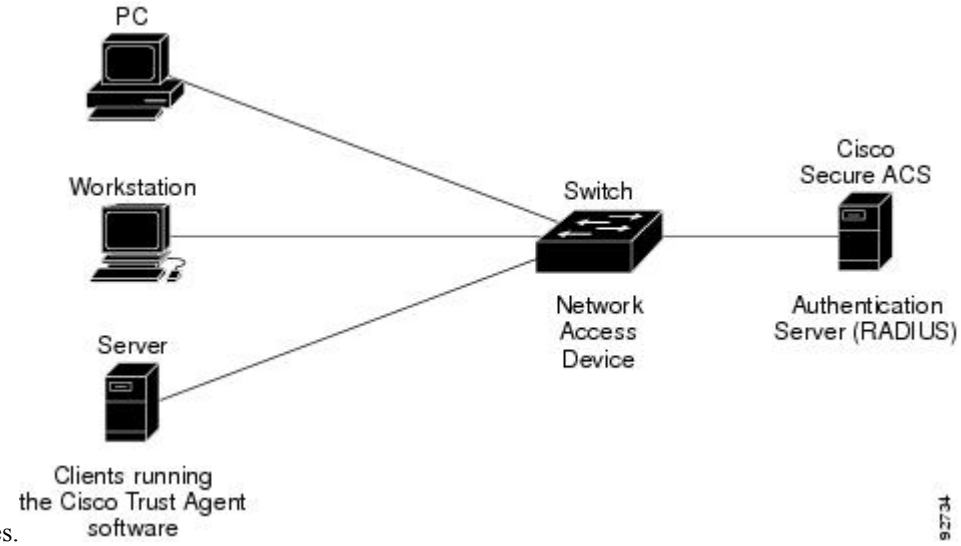
NAC validates that the posture or state of endpoint devices complies with security policies before the devices can access protected areas of the network. For devices that comply with the security policies, NAC allows access to protected services in the network. For devices that do not comply with security policies, NAC allows access to the network only for remediation, when the posture of the device is checked again.

NAC Device Roles

NAC assigns roles to the devices in the network.

Figure 1: Posture Validation Devices

This figure shows an example of a network with the NAC device



roles.

NAC supports the following roles for network devices:

Endpoint device

Systems or clients on the network such as a PC, workstation, or server that is connected to a Cisco NX-OS device access port through a direct connection. The endpoint device, which is running the Cisco Trust Agent software, requests access to the LAN and switch services and responds to requests from the switch. Endpoint devices are potential sources of virus infections, and NAC must validate their antivirus statuses before granting network access.

Note The Cisco Trust Agent software is also referred to as the *posture agent* or the *antivirus client*. For more information on Cisco Trust Agent software, go to the following URL:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

Network access device (NAD)

Cisco NX-OS device that provides validation services and policy enforcement at the network edge and controls the physical access to the network based on the access policy of the client. The NAD relays Extensible Authentication Protocol (EAP) messages between the endpoints and the authentication server.

The NAD queries for posture credentials whenever it detects a new connection to the network. When the endpoint device has a posture agent (PA) installed, the NAD performs an in-band posture validation. The NAD acts as a relay agent between the endpoint device and AAA server for all messages in the posture validation exchange. If the NAD does not find a PA, the NAD performs an out-of-band posture validation through an audit server.

The NAD queries for posture credentials whenever it detects a new connection to the network. When the endpoint device has a posture agent (PA) installed, the NAD performs an in-band posture validation.

The NAD acts as a relay agent between the endpoint device and AAA server for all messages in the posture validation exchange. If the NAD does not find a PA, the NAD performs an out-of-band posture validation through an audit server.

The NAD controls which hosts have access to network destinations through that device based on a network access profile received from the AAA server once the posture validation exchange completes (whether in-band or out-of-band). The access profile can be one of the following forms:

- VLAN or private VLAN.
- Access control lists (ACLs) determine what type of traffic for which destinations are reachable for this host in addition to any default access that is provided to all hosts independent of the NAC process (for example, access to the Dynamic Host Configuration Protocol [DHCP] server, remediation server, audit server).

The NAD triggers the posture validation process at the following times:

- When a new session starts.
- When the revalidation timer expires.
- When you enter a system administrator command.
- When the posture agent indicates that the posture has changed (only for an endpoint device with a posture agent).

For Cisco NX-OS devices, the encapsulation information in the Extensible Authentication Protocol (EAP) messages is based on the User Datagram Protocol (UDP). When using UDP, the Cisco NX-OS device uses EAP over UDP (EAPoUDP or EoU) frames.

Authentication server
Server that performs the actual validation of the client. The authentication server validates the antivirus status of the client, determines the access policy, and notifies the NAD if the client is authorized to access the LAN and NAD services. Because the NAD acts as the proxy, the EAP message exchange between the NAD and authentication server is transparent to the NAD.

The Cisco NX-OS device supports the Cisco Secure Access Control Server (ACS) Version 4.0 or later with RADIUS, authentication, authorization, and accounting (AAA), and EAP extensions.

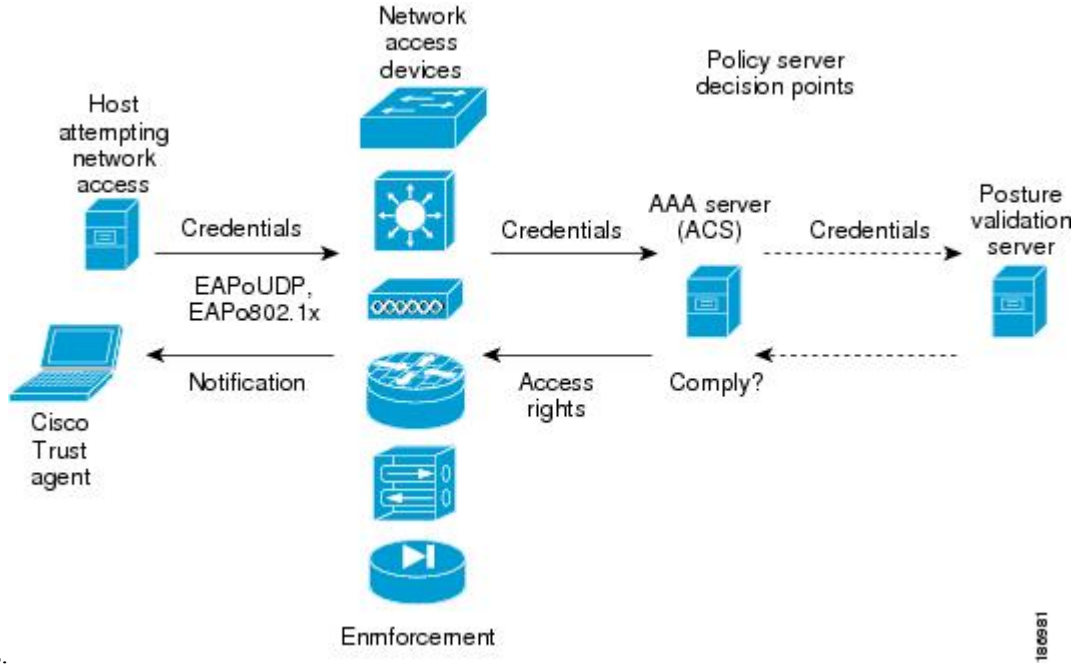
Posture validation server
Third-party server that acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules. The posture validation server receives requests from an authentication server.

NAC Posture Validation

Posture validation occurs when a NAC-enabled NAD detects an endpoint device that is attempting to connect or use its network resources. When the NAD detects a new endpoint device, it requests the network access profile for the endpoint device from an AAA server (such as the Cisco Secure ACS).

Figure 2: NAC Endpoint Device Posture Validation

This figure shows the NAC endpoint device posture validation



process.

The AAA server determines if the endpoint device has a posture agent installed. If the endpoint device has a posture agent (such as the Cisco Trust Agent), the AAA server requests the endpoint device for posture information via the NAD. The endpoint device responds to the AAA server with a set of posture credentials. The AAA server then validates the posture information locally or delegates the posture validation decisions to one or more external posture validation servers.

If the endpoint device does not have a posture agent, the AAA server may request an audit server to collect posture information from the device through other means (for example, fingerprinting and port scanning). The AAA server also asks the audit server to validate that information and return a posture validation decision.

The AAA server aggregates the posture validation results from these sources and makes an authorization decision that is based on whether the endpoint device complies with the network policy. The AAA server determines the network access profile for the endpoint device and sends the profile to the NAD for enforcement of the endpoint device authorization.

The examination of endpoint device credentials by the AAA server can result in one or more application posture tokens (APTs). An APT represents a compliance check for a given vendor's application. The AAA server aggregates all APTs from the posture validation servers into a single system posture token (SPT) that represents the overall compliance of the endpoint device. The value SPT is based on the worst APT from the set of APTs. Both APTs and SPTs are represented using the following predefined tokens:

Healthy
The endpoint device complies with the posture policy so no restrictions are placed on this device.

Checkup
The endpoint device is within policy but does not have the latest software; an update is recommended.

Transition
The endpoint device is in the process of having its posture checked and is given interim access pending a result from a complete posture validation. A transition result may occur when a host is booting and complete posture information is not available, or when complete audit results are not available.

Quarantine
The endpoint device is out of compliance and must be restricted to a quarantine network for remediation. This device is not actively placing a threat on other endpoint devices but is vulnerable to attack or infection and must be updated as soon as possible.

Infected
The endpoint device is an active threat to other endpoint devices; network access must be severely restricted and the endpoint device must be placed into remediation or denied all network access to the endpoint device.

Unknown
The AAA server cannot determine the posture credentials of the endpoint device. You need to determine the integrity of the endpoint device so that proper posture credentials can be attained and assessed for network access authorization.

IP Device Tracking

The IP device tracking allows endpoint devices to remain connected to the network if the AAA server is not available. Typical deployments of NAC use Cisco Secure ACS to validate the client posture and to pass policies back to the NAD.

IP device tracking provides the following benefits:

- While AAA is unavailable, the endpoint device still has connectivity to the network, although it may be restricted.
- When the AAA server is available again, a user can be revalidated and the user's policies can be downloaded from the ACS.

Note When the AAA server is down, the NAD applies the IP device tracking policy only if there is no existing policy associated with the host. Typically, during revalidation when the AAA server goes down, the NAD retains the current policies used for the endpoint device.

NAC LPIP

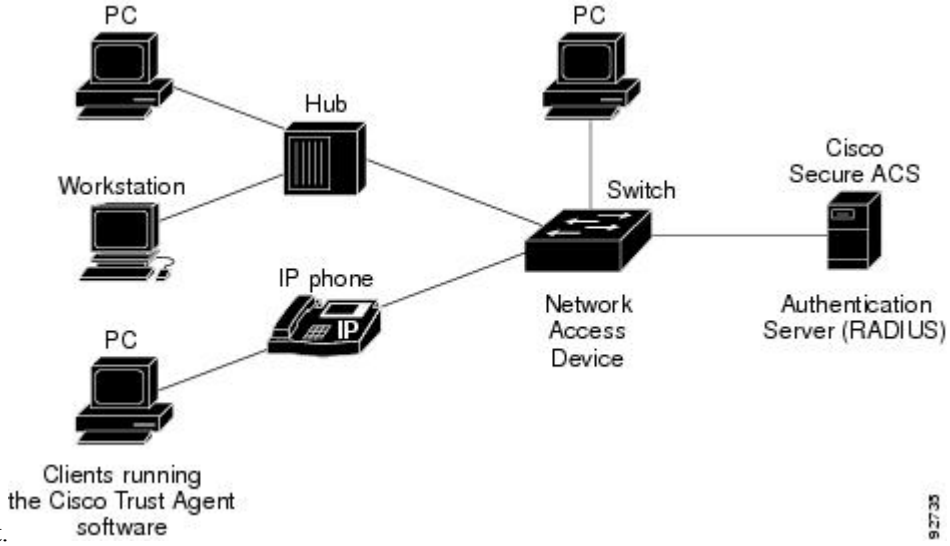
NAC LAN port IP (LPIP) validation uses the Layer 3 transport EAPoUDP to carry posture validation information. LPIP validation has the following characteristics:

- Operates only on Layer 2 ports and cannot operate on Layer 3 ports.
- Subjects all hosts sending IP traffic on the port to posture validation.

LPIP validation triggers admission control by snooping on DHCP messages or Address Resolution Protocol (ARP) messages rather than intercepting IP packets on the data path. LPIP validation performs policy enforcement using access control lists (ACLs).

Figure 3: Network Using LPIP Validation

This figure shows the LPIP validation process for a single host connected to a NAD port or multiple hosts on the same NAD port.



When you enable LPIP validation, EAPoUDP only supports IPv4 traffic. The NAD checks the antivirus status of the endpoint devices or clients and enforces access control policies.

Posture Validation

When you enable LPIP validation on a port connected to one or more endpoint devices, the Cisco NX-OS device uses DHCP snooping and ARP snooping to identify connected hosts. The Cisco NX-OS device initiates posture validation after receiving an ARP packet or creating a DHCP snooping binding entry. ARP snooping is the default method to detect connected hosts. If you want the NAD to detect hosts when a DHCP snooping binding entry is created, you must enable DHCP snooping.

Admission Triggers

ARP snooping allows LPIP validation to detect hosts with either dynamically acquired or statically configured IP addresses. When the NAD receives an ARP packet from an unknown host, it triggers posture validation. If you have enabled DHCP snooping on the interface, the creation of a DHCP binding entry on the NAD triggers posture validation. DHCP snooping provides a slightly faster response time because DHCP packets are exchanged prior to sending ARP requests. Both ARP snooping and DHCP snooping can trigger posture validation on the same host. In this case, the trigger initiated by the creation of a DHCP snooping binding takes precedence over ARP snooping.

Note When you use DHCP snooping and ARP snooping to detect the presence of a host, a malicious host might set up a static ARP table to bypass posture validation. To protect against this type of exposure, you can enable IP Source Guard on the port. IP Source Guard prevents unauthorized hosts from accessing the network.

Posture Validation Methods

After posture validation is triggered for a host, you can use one of two possible methods to determine the policy to be applied for the host:

- Exception lists
- EAPoUDP

Exception Lists

An exception list contains local profile and policy configurations. Use the identity profile to statically authorize or validate devices based on the IP address and MAC address. You can associate an identity profile with a local policy that specifies the access control attributes.

Using an exception list, you can bypass posture validation for specific endpoint devices and apply a statically configured policy. After posture validation is triggered, the NAD checks for the host information in the exception list. If a match is found in the exception list, the NAD applies the configured policy for the endpoint device.

EAPoUDP

If an endpoint device does not match the exception list, the NAD sends an EAPoUDP packet to initiate posture validation. While posture validation occurs, the NAD enforces the default access policy. After the NAD sends an EAPoUDP message to the host and the host responds to the antivirus condition request, the NAD forwards the EAPoUDP response to the Cisco Secure ACS. If the NAD does not receive a response from the host after the specified number of attempts, the NAD classifies the host as nonresponsive. After the ACS validates the credentials, the authentication server returns an Access-Accept or Access-Reject message to the NAD. The NAD updates the EAPoUDP session table and enforces the access limitations, which segments and quarantines the poorly postured endpoint device or denies network access.

Note An Access-Reject message indicates that the EAPoUDP exchange has failed. This message does not indicate that the endpoint device is poorly postured.

For an Access-Accept message, the NAD applies the enforcement policy that contains the policy-based ACL (PACL) name and starts the EAP revalidation and status query timers.

For an Access-Reject message, the NAD removes any enforcement policy for the host and puts the endpoint device into the Held state for a configured period of time (Hold timer). After the Hold timer expires, the NAD revalidates the endpoint device.

Note If you delete a DHCP snooping binding entry for an endpoint device, the NAD removes the client entry in the session table and the client is no longer authenticated.

Policy Enforcement Using ACLs

LPIP validation uses PACLs for policy enforcement.

The NAD applies the PACL when the posture validation fails (the AAA server sends an Access-Reject message). The default policy is to use the active MAC ACL applied to the port (also called a port ACL [PACL]). The active MAC ACL could either be a statically configured PACL or an AAA server-specified PACL based on 802.1X authentication.

The PACL defines a group that expands to a list of endpoint device IP addresses. The PACLs usually contain the endpoint device IP addresses. Once the NAD classifies an endpoint device using a particular group, the

NAD adds the IP address that corresponds to the endpoint device to the appropriate group. The result is that the policy is applied to the endpoint device.

When you configure LPIP validation for an NAD port, you must also configure a default PACL on that NAD port. In addition, you should apply the default ACL to the IP traffic for hosts that have not completed posture validation.

If you configure the default ACL on the NAD and the Cisco Secure ACS sends a host access policy to the NAD, the NAD applies the policy to that traffic from the host that is connected to a NAD port. If the policy applies to the traffic, the NAD forwards the traffic. If the policy does not apply, the NAD applies the default ACL. However, if the NAD gets an endpoint device access policy from the Cisco Secure ACS but the default ACL is not configured, the LPIP validation configuration does not take effect.

Note Both DHCP snooping and ARP snooping are enabled per VLAN. However, security ACLs downloaded as a result of NAC Layer 2 posture validation are applied per port. As a result, all DHCP and ARP packets are intercepted when these features are enabled on any VLAN.

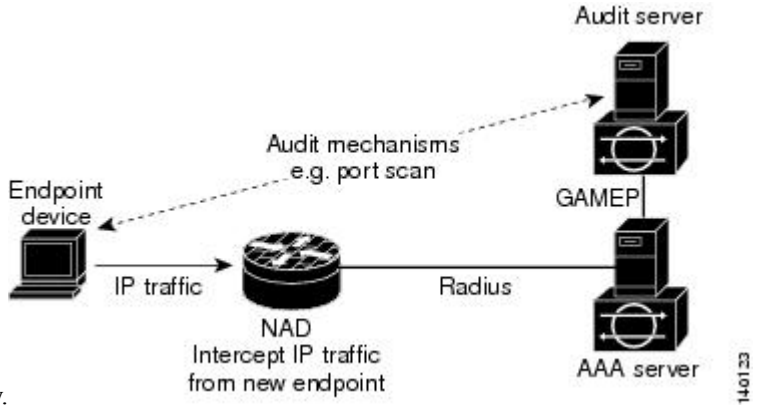
Audit Servers and Nonresponsive Hosts

Endpoint devices that do not run a posture agent (Cisco Trust Agent) cannot provide credentials when challenged by NADs. These devices are described as *agentless* or *nonresponsive*.

The NAC architecture supports audit servers to validate agentless endpoint devices. An audit server is a third-party server that can probe, scan, and determine security compliance of a host without needing a posture again on the endpoint device. The result of the audit server examination can influence the access servers to make network access policy decisions specific to the endpoint device instead of enforcing a common restrictive policy for all nonresponsive endpoint devices. You can build more robust host audit and examination functionality by integrating any third-party audit operations into the NAC architecture.

Figure 4: NAC Device Roles

This figure shows how audit servers fit into the typical topology.



NAC assumes that the audit server can be reached so that the endpoint device can communicate with it. When an endpoint device makes network access through the NAD configured for posture validation, the network access device eventually requests the AAA server (Cisco Secure ACS) for an access policy to be enforced for the host. The AAA server can be configured to trigger a scan of the host with an external audit server. The audit server scan occurs asynchronously and takes several seconds to complete. During the scan, the AAA server conveys a minimal restrictive security policy to NAD for enforcement along with a short poll timer

(session-timeout). The NAD polls the AAA sever at the specified timer interval until the result is available from the audit server. After the AAA server receives the audit result, it computes an access policy based on the audit result and sends it to the NAD for enforcement on its next request.

NAC Timers

This section describes the NAC timers.

Hold Timer

The hold timer prevents a new EAPoUDP session from immediately starting after the previous attempt to validate that the session fails. NAC uses this time only when the Cisco Secure ACS sends an Accept-Reject message to the NAD. The default value of the hold timer is 180 seconds (3 minutes).

An EAPoUDP session might not be validated when the posture validation of the host fails, a session timer expires, or the NAD or Cisco Secure ACS receives invalid messages. If the NAD or authentication server continuously receives invalid messages, a malicious user might be trying to cause a denial-of-service attack.

AAA Timer

The AAA timer controls the amount of time that the NAD waits for a response from the AAA server before resending a request during posture validation. The default value of the retransmission timer is 60 seconds.

Note Setting the timer value too low might cause unnecessary transmissions; setting the timer value too high might cause poor response times.

Retransmit Timer

The retransmit timer controls the amount of time that the NAD waits for a response from the client before resending a request during posture validation. The default value of the retransmission timer is 3 seconds.

Note Setting the timer value too low might cause unnecessary transmissions; setting the timer value too high might cause poor response times.

Revalidation Timer

The revalidation timer controls the amount of time that the NAD applies a NAC policy to an endpoint device that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation completes. The timer resets when the host is revalidated. The default value of the revalidation timer is 36000 seconds (10 hours).

The Cisco NX-OS software bases the revalidation timer operation on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS-REQUEST attribute (Attribute[29]) in the Access-Accept message from the AAA server (Cisco Secure ACS). If the NAD receives the Session-Timeout value, this value overrides the revalidation timer value on the NAD.

If the revalidation timer expires, the NAD action depends on one of these values of the Termination-Action attribute:

- If the value of the Termination-Action RADIUS attribute is the default, the session ends.

- If the NAD receives a value for the Termination-Action attribute other than the default, the EAPoUDP session and the current access policy remain in effect during posture revalidation.
- If the value of the Termination-Action attribute is RADIUS, the NAD revalidates the client.
- If the packet from the server does not include the Termination-Action attribute, the EAPoUDP session ends.

Status-Query Timer

The status-query timer controls the amount of time that the NAD waits before verifying that the previously validated client is present and that its posture has not changed. Only clients that were authenticated with EAPoUDP messages use this timer, which starts after the client is initially validated. The default value of the status-query timer is 300 seconds (5 minutes).

The timer resets when the host is reauthenticated. When the timer expires, the NAD checks the host posture validation by sending a Status-Query message to the host. If the host sends a message to the NAD that the posture has changed, the NAD revalidates the posture of the host.

NAC Posture Validation and Redundant Supervisor Modules

When a switchover occurs, the Cisco NX-OS device maintains information about the endpoint devices and the current PACL application but loses the current state of each EAPoUDP session. The Cisco NX-OS device removes the current PACL application and restarts posture validation.

LPIP Validation and Other Security Features

This section describes how LPIP validation interacts with other security features on the Cisco NX-OS device.

802.1X

If you configure both 802.1X and LPIP on a port, the traffic that does not pass the 802.1X-authenticated source MAC check does not trigger posture validation. When you configure 802.1X on a port, the port cannot transmit or receive traffic (other than EAP over LAN [EAPOL] frames) until the attached host is authenticated via 802.1X. This mechanism ensures that the IP traffic from the host does not trigger posture validation before it is authenticated.

Port Security

The NAD checks the source MAC against the port security MACs and drops the endpoint device if the check fails. The NAD allows posture validation only on port security-validated MAC addresses. If a port security violation occurs and results in a port shutdown, the Cisco NX-OS software removes the LPIP state of the port.

DHCP Snooping

Posture validation does not occur until after a DHCP creates a binding entry. When you enable DHCP snooping and LPIP, the Cisco NX-OS software triggers posture validation for a host when DHCP creates a binding entry for the host using DHCP to acquire IP address.

Dynamic ARP Inspection

If you enable LPIP validation on the interface, posture validation is triggered only if the packet passes the dynamic ARP inspection (DAI) check. If you do not enable DAI, then all ARP packets (with valid MAC/IP pairs) will trigger posture validation.

Note ARP snooping is the default mechanism of detecting hosts. However, ARP snooping is not the same as DAI. If you enable LPIP validation, the Cisco NX-OS software passes the ARP packets to LPIP validation. If you enable DAI, the Cisco NX-OS software passes the ARP packets to DAI.

Note If you have enabled DHCP snooping, the Cisco NX-OS software bypasses DAI.

IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the DHCP snooping binding table.
- Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent attacks that rely on spoofing the IP address of a valid host. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

Posture Host-Specific ACEs

The Cisco NX-OS software drops the packet if the packet matches the deny condition and skips the active PACL if a packet matches a permit condition. If no implicit deny exists at the end of the ACEs and no match occurs, the Cisco NX-OS software checks the packet against the active PACL.

Note If you enable DHCP snooping or DAI, the NAD does not process posture host-specific ACEs.

Active PACLs

The active PACL is either a statically configured PACL or an AAA server-specified PACL that is based on 802.1X authentication. The packet is dropped if it matches any deny condition and moves to the next step if it matches a permit condition.

Note If you have enabled DHCP snooping or DAI, the NAD does not process the active PACL.

VACLs

The Cisco NX-OS software drops any packet that matches a deny condition.

Note If you have enabled DHCP snooping or DAI, the NAD bypasses the VACLs.

Virtualization Support for NAC

NAC configuration and operation are local to the virtual device context (VDC).

For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Prerequisites for NAC

NAC has the following prerequisites:

- Ensure that a Layer 3 route exists between the NAD and each endpoint device.

NAC Guidelines and Limitations

NAC has the following guidelines and limitations:

- EAPoUDP bypass and AAA down policy are not supported.
- NAC uses only RADIUS for authentication.

LPIP Limitations

LPIP validation has the following limitations:

- LPIP validation is allowed only on access ports.
- You cannot enable LPIP validation on trunk ports or port channels.
- LPIP validation is not allowed on ports that are SPAN destinations.
- LPIP validation is not allowed on ports that are part of a private VLAN.
- LPIP validation does not support IPv6.
- LPIP validation is allowed only for endpoint devices directly connected to the NAD.
- You cannot use LPIP validation unless you have a Layer 3 route between the NAD and the endpoint device.

Default Settings for NAC

This table lists the default settings for NAC parameters.

Table 1: Default NAC Parameter Settings

Parameters	Default
EAPoUDP	Disabled.
EAP UDP port number	21862 (0x5566).
Clientless hosts allowed	Disabled.
Automatic periodic revalidation	Enabled.
Revalidation timeout interval	36000 seconds (10 hours).
Retransmit timeout interval	3 seconds.
Status query timeout interval	300 seconds (5 minutes).
Hold timeout interval	180 seconds (3 minutes).
AAA timeout interval	60 seconds (1 minute).
Maximum retries	3.
EAPoUDP rate limit maximum	20 simultaneous sessions.
EAPoUDP logging	Disabled.
IP device tracking	Enabled.

Configuring NAC

This section describes how to configure NAC.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Process for Configuring NAC

Follow these steps to configure NAC:

SUMMARY STEPS

1. Enable EAPoUDP.
2. Configure the connection to the AAA server.
3. Apply PACLs to the interfaces connected to endpoint devices.
4. Enable NAC on the interfaces connected to the endpoint devices.

DETAILED STEPS

Step 1 Enable EAPoUDP.

Step 2 Configure the connection to the AAA server.

Step 3 Apply PACLs to the interfaces connected to endpoint devices.

Step 4 Enable NAC on the interfaces connected to the endpoint devices.

Related Topics

Enabling EAPoUDP, on page 14
Enabling the Default AAA Authenication Method for EAPoUDP, on page 15
Applying PACLs to Interfaces, on page 16
Enabling NAC on an Interface, on page 17

Enabling EAPoUDP

The Cisco NX-OS device relays Extensible Authentication Protocol (EAP) messages between the endpoints and the authentication server. You must enable EAP over UDP (EAPoUDP) before configuring NAC on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. **feature eou**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature eou** **Example:** `switch(config)# feature eou`	Enables EAPoUDP. The default is disabled.

	Command or Action	Purpose

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling the Default AAA Authenication Method for EAPoUDP

You must enable the default AAA authentication method EAPoUDP.

Note LPIP can use only RADIUS for authentication.

Before you begin

Enable EAPoUDP.

Configure RADIUS or TACACS+ server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication eou default group** *group-list*
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**aaa authentication eou default group** *group-list* **Example:** `switch(config)# aaa authentication eou default group RadServer`	Configures a list of one or more RADIUS server groups as the default AAA authentication method for EAPoUDP. The *group-list* argument consists of a space-delimited list of groups. The group names are as follows: • **radius**—Uses the global pool of RADIUS servers for authentication.

	Command or Action	Purpose
		• *named-group*—Uses a named subset of RADIUS servers for authentication. The default setting is no method.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	Displays the default AAA authentication methods.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Configuring AAA
Configuring RADIUS

Applying PACLs to Interfaces

You must apply a PACL to the access interfaces on the NAD that perform LPIP posture validation if no PACL is available from the AAA server.

Before you begin

Create a MAC ACL.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **mac access-group** *access-list*
4. **exit**
5. (Optional) **show running-config interface**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**mac access-group** *access-list* **Example:** `switch(config-if)# mac access-group acl-01`	Applies a PACL to the interface for traffic that flows in the direction specified. **Note** An interface can have only one PACL. To replace the PACL on the interface, enter this command again using the new PACL name.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits global configuration mode.

Step 5	(Optional) **show running-config interface** **Example:** `switch(config)# show running-config interface`	Displays the interface PACL configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling NAC on an Interface

You must enable NAC on an interface for posture validation to occur.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **switchport**
4. **switchport mode access**
5. **nac enable**
6. **exit**
7. (Optional) **show running-config interface**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**switchport** **Example:** `switch(config-if)# switchport`	Sets the interface as a Layer 2 switching interface. By default, all ports are Layer 3 ports.
Step 4	**switchport mode access** **Example:** `switch(config-if)# switchport mode access`	Configures the port mode as access.
Step 5	**nac enable** **Example:** `switch(config-if)# nac enable`	Enables NAC on the interface.

Step 6	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits global configuration mode.

Step 7	(Optional) **show running-config interface** **Example:** `switch(config)# show running-config interface`	Displays the interface PACL configuration.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14

Configuring Identity Policies and Identity Profile Entries

You can use the identity profile to configure exceptions to LPIP posture validation. The identity profile contains entries for the endpoint devices for which are not subject to LPIP validation. You can optionally configure an identity policy for each identity profile entry that specifies a PACL that the NX-OS device applies to the endpoint device. The default identity policy is the PACL for the interface.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **identity policy** *policy-name*
3. **object-group** *access-list*
4. (Optional) **description** " *text* "
5. **exit**
6. (Optional) **show identity policy**
7. **identity profile eapoudp**
8. **device** {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*ipv4-subnet-mask*] | **mac-address** *mac-address* [*mac-subnet-mask*]} **policy** *name*
9. **exit**
10. (Optional) **show identity profile eapoudp**
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**identity policy** *policy-name*
	Example:
	`switch(config)# identity policy AccType1`
	`switch(config-id-policy)#`
		Specifies the identity policy name and enters identity policy configuration mode. You can create a maximum of 1024 identity policies. The maximum length of the name is 100 characters.

Step 3	**object-group** *access-list* **Example:** `switch(config-id-policy)# object-group maxaclx`	Specifies the IP ACL or MAC ACL for the policy.
Step 4	(Optional) **description** " *text* " **Example:** `switch(config-id-policy)# description "This policy prevents endpoint device without a PA"`	Provides a description for the identity policy. The maximum length is 100 characters.

Step 5	**exit**
	Example:
	`switch(config-id-policy)# exit`
	`switch(config)#`
		Exits identity policy configuration mode.

Step 6	(Optional) **show identity policy** **Example:**	Displays the identity policy configuration.

	Command or Action	Purpose
	`switch(config)# show identity policy`	

Step 7	**identity profile eapoudp**
	Example:
	`switch(config)# identity profile eapoudp`
	`switch(config-id-prof)#`
		Enters identity profile configuration mode for EAPoUDP.

Step 8	**device** {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*ipv4-subnet-mask*] | **mac-address** *mac-address* [*mac-subnet-mask*]} **policy** *name* **Example:** `switch(config-id-prof)# device authenticate ip-address 10.10.2.2 policy AccType1`	Specifies an exception entry. The maximum number of entries is 5000.

Step 9	**exit**
	Example:
	`switch(config-id-prof)# exit`
	`switch(config)#`
		Exits identity profile configuration mode.

Step 10	(Optional) **show identity profile eapoudp** **Example:** `switch(config)# show identity profile eapoudp`	Displays the identity profile configuration.
Step 11	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14

Allowing Clientless Endpoint Devices

You can allow posture validation endpoint devices in your network that do not have a posture agent installed (clientless). The posture validation is performed by an audit server that has access to the endpoint devices.

Before you begin

Enable EAPoUDP.

Verify that the AAA server and clientless endpoint devices can access the audit server.

SUMMARY STEPS

1. **configure terminal**
2. **eou allow clientless**
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou allow clientless** **Example:** `switch(config)# eou allow clientless`	Allows posture validation for clientless endpoint devices. The default is disabled.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14

Enabling Logging for EAPoUDP

You can enable logging for EAPoUDP event messages. EAPoUDP events include errors and status changes. The destination for these event messages is the configured syslog.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou logging**
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou logging** **Example:** `switch(config)# eou logging`	Enables EAPoUDP logging. The default is disabled.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show eou** **Example:** `switch)# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14

Changing the Global EAPoUDP Maximum Retry Value

You can change the global maximum number of EAPoUDP retries. The default value is three.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou max-retry** *count*
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou max-retry** *count* **Example:** `switch(config)# eou max-retry 2`	Changes the EAPoUDP maximum retry count. The default is 3. The range is from 1 to 3.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Changing the EAPoUDP Maximum Retry Value for an Interface, on page 23

Changing the EAPoUDP Maximum Retry Value for an Interface

You can change the maximum number of EAPoUDP retries for an interface. The default value is three.

Before you begin

Enable EAPoUDP.

Enable NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **eou max-retry** *count*
4. **exit**
5. (Optional) **show eou**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**eou max-retry** *count* **Example:** `switch(config-if)# eou max-retry 2`	Changes the EAPoUDP maximum retry count. The default is 3. The range is from 1 to 3.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	(Optional) **show eou** **Example:** `switch(config)# show eou`	Displays the EAPoUDP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Changing the Global EAPoUDP Maximum Retry Value, on page 22
Enabling NAC on an Interface, on page 17

Changing the UDP Port for EAPoUDP

You can change the UDP port used by EAPoUDP. The default port is 21862.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou port** *udp-port*
3. **exit**

4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou port** *udp-port* **Example:** `switch(config)# eou port 27180`	Changes the UDP port used by EAPoUDP. The default is 21862. The range is from 1 to 65535.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14

Configuring Rate Limiting of Simultaneous EAPoUDP Posture Validation Sessions

You can configure rate limiting to control the number of simultaneous EAPoUDP posture validations sessions. You can change the rate-limiting value that controls the maximum number of simultaneous EAPoUDP posture validation sessions. The default number is 20. Setting the number to zero (0) disables rate limiting.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou ratelimit** *number-of-sessions*
3. **exit**

4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou ratelimit** *number-of-sessions* **Example:** `switch(config)# eou ratelimit 15`	Configures the number of simultaneous EAPoUDP posture validation sessions. The default is 20. The range is from 0 to 200. **Note** A setting of zero (0) disables rate limiting.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14

Configuring Global Automatic Posture Revalidation

The Cisco NX-OS software automatically revalidates the posture of the endpoint devices for the Cisco NX-OS device at a configured interval. The default interval is 36,000 seconds (10 hours). You can disable revalidation or change the length of the revalidation interval.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **eou revalidate**
3. (Optional) **eou timeout revalidation** *seconds*

4. **exit**
5. (Optional) **show eou**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	(Optional) **eou revalidate** **Example:** `switch(config)# eou revalidate`	Enables the automatic posture validation. The default is enabled.
Step 3	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds. Use the **no eou revalidate** command to disable automatic posture validation.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 5	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Configuring Automatic Posture Revalidation for an Interface, on page 27

Configuring Automatic Posture Revalidation for an Interface

The Cisco NX-OS software automatically revalidates the posture of the endpoint devices for the Cisco NX-OS device at a configured interval. The default interval is 36,000 seconds (10 hours). You can disable revalidation or change the length of the revalidation interval.

Before you begin

Enable EAPoUDP.

Enable NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. (Optional) **eou revalidate**
4. (Optional) **eou timeout revalidation** *seconds*
5. **exit**
6. (Optional) **show eou**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	(Optional) **eou revalidate** **Example:** `switch(config-if)# eou revalidate`	Enables the automatic posture validation. The default is enabled. Use the **no eou revalidate** command to disable automatic posture validation.
Step 4	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config-if)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds.

Step 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits global configuration mode.

Step 6	(Optional) **show eou** **Example:** `switch(config)# show eou`	Displays the EAPoUDP configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Configuring Global Automatic Posture Revalidation, on page 26
Enabling NAC on an Interface, on page 17

Changing the Global EAPoUDP Timers

The Cisco NX-OS software supports the following global timers for EAPoUDP:

AAA
Controls the amount of time that the NAD waits for a response from the AAA server before resending a request during posture validation.

Hold period
Prevents a new EAPoUDP session from immediately starting after the previous attempt to validate that the session fails. NAC uses this time only when the Cisco Secure ACS sends an Accept-Reject message to the NAD.

Retransmit
Controls the amount of time that the NAD waits for a response from the client before resending a request during posture validation.

Revalidation
Controls the amount of time that the NAD applies a NAC policy to an endpoint device that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation completes.

Status query
Controls the amount of time that the NAD waits before verifying that the previously validated client is present and that its posture has not changed. Only clients that were authenticated with EAPoUDP messages use this timer, which starts after the client is initially validated.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **eou timeout aaa** *seconds*
3. (Optional) **eou timeout hold-period** *seconds*
4. (Optional) **eou timeout retransmit** *seconds*
5. (Optional) **eou timeout revalidation** *seconds*
6. (Optional) **eou timeout status-query** *seconds*
7. **exit**
8. (Optional) **show eou**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
Step 2	(Optional) **eou timeout aaa** *seconds* **Example:** `switch(config)# eou timeout aaa 30`	Changes the AAA timeout interval. The default is 60 seconds (1 minute). The range is from 0 to 60 seconds.
Step 3	(Optional) **eou timeout hold-period** *seconds* **Example:** `switch(config)# eou timeout hold-period 300`	Changes the hold period timeout interval. The default is 180 seconds (3 minutes). The range is from 60 to 86400 seconds.
Step 4	(Optional) **eou timeout retransmit** *seconds* **Example:** `switch(config)# eou timeout retransmit 10`	Changes the retransmit timeout interval. The default is 3 seconds. The range is from 1 to 60 seconds.
Step 5	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds.
Step 6	(Optional) **eou timeout status-query** *seconds* **Example:** `switch(config)# eou timeout status-query 360`	Changes the status query timeout interval. The default is 300 seconds (5 minutes). The range is from 10 to 1800 seconds.

Step 7	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 8	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Changing the EAPoUDP Timers for an Interface, on page 30
NAC Timers, on page 9

Changing the EAPoUDP Timers for an Interface

The Cisco NX-OS software supports the following timers for EAPoUDP for each interface enabled for NAC:

AAA

Controls the amount of time that the NAD waits for a response from the AAA server before resending a request during posture validation.

Hold period

Prevents a new EAPoUDP session from immediately starting after the previous attempt to validate that the session fails. NAC uses this time only when the Cisco Secure ACS sends an Accept-Reject message to the NAD.

Retransmit

Controls the amount of time that the NAD waits for a response from the client before resending a request during posture validation.

Revalidation

Controls the amount of time that the NAD applies a NAC policy to an endpoint device that used EAPoUDP messages during posture validation. The timer starts after the initial posture validation completes.

Status query

Controls the amount of time that the NAD waits before verifying that the previously validated client is present and that its posture has not changed. Only clients that were authenticated with EAPoUDP messages use this timer, which starts after the client is initially validated.

Before you begin

Enable EAPoUDP.

Enable NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. (Optional) **eou timeout aaa** *seconds*
4. (Optional) **eou timeout hold-period** *seconds*
5. (Optional) **eou timeout retransmit** *seconds*
6. (Optional) **eou timeout revalidation** *seconds*
7. (Optional) **eou timeout status-query** *seconds*
8. **exit**
9. (Optional) **show eou**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	(Optional) **eou timeout aaa** *seconds* **Example:** `switch(config-if)# eou timeout aaa 50`	Changes the AAA timeout interval. The default is 60 seconds (1 minute). The range is from 0 to 60 seconds.
Step 4	(Optional) **eou timeout hold-period** *seconds* **Example:** `switch(config-if)# eou timeout hold-period 300`	Changes the hold period timeout interval. The default is 180 seconds (3 minutes). The range is from 60 to 86400 seconds.
Step 5	(Optional) **eou timeout retransmit** *seconds* **Example:** `switch(config-if)# eou timeout retransmit 10`	Changes the retransmit timeout interval. The default is 3 seconds. The range is from 1 to 60 seconds.
Step 6	(Optional) **eou timeout revalidation** *seconds* **Example:** `switch(config-if)# eou timeout revalidation 30000`	Changes the revalidation timer interval. The default is 36000. The range is from 5 to 86400 seconds.
Step 7	(Optional) **eou timeout status-query** *seconds* **Example:** `switch(config-if)# eou timeout status-query 360`	Changes the status query timeout interval. The default is 300 seconds (5 minutes). The range is from 10 to 1800 seconds.

Step 8	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 9	(Optional) **show eou** **Example:** `switch(config)# show eou`	Displays the EAPoUDP configuration.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Changing the Global EAPoUDP Timers, on page 29
NAC Timers, on page 9
Enabling NAC on an Interface, on page 17

Resetting the EAPoUDP Global Configuration to the Default Values

You can reset the EAPoUDP global configuration to the default values.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. **configure terminal**
2. **eou default**
3. **exit**
4. (Optional) **show eou**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**eou default** **Example:** `switch(config)# eou default`	Resets the EAPoUDP configuration to the default values.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 4	(Optional) **show eou** **Example:** `switch# show eou`	Displays the EAPoUDP configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Resetting the EAPoUDP Interface Configuration to the Default Values, on page 34

Resetting the EAPoUDP Interface Configuration to the Default Values

You can reset the EAPoUDP configuration for an interface to the default values.

Before you begin

Enable EAPoUDP.

Enabled NAC on the interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **eou default**
4. **exit**
5. (Optional) **show eou interface ethernet** *slot*/*port*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot*/*port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the Ethernet interface and enters interface configuration mode.

Step 3	**eou default** **Example:** `switch(config-if)# eou default`	Resets the EAPoUDP configuration for the interface to the default values.

Step 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits interface configuration mode.

Step 5	(Optional) **show eou interface ethernet** *slot*/*port* **Example:** `switch(config)# show eou interface ethernet 2/1`	Displays the EAPoUDP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14
Resetting the EAPoUDP Global Configuration to the Default Values, on page 33
Enabling NAC on an Interface, on page 17

Configuring IP Device Tracking

You can configure IP device tracking. The process for the IP device tracking for AAA servers operates is as follows:

- The Cisco NX-OS device detects a new session.
- Before posture validation is triggered and if the AAA server is unreachable, the Cisco NX-OS device applies the IP device tracking policy and maintains the session state as AAA DOWN.
- When the AAA server is once again available, a revalidation occurs for the host.

Note When the AAA server is down, the Cisco NX-OS device applies the IP device tracking policy only if no existing policy is associated with the endpoint device. During revalidation when the AAA server goes down, the Cisco NX-OS device retains the policies that are used for the endpoint device.

SUMMARY STEPS

1. **configure terminal**
2. **ip device tracking enable**
3. (Optional) **ip device tracking probe** {**count** *count* | **interval** *seconds*}
4. (Optional) **radius-server host** {*hostname* | *ip-address*} **test** [**username** *username* [**password** *password*]] [**idle-time** *minutes*]
5. **exit**
6. (Optional) **show ip device tracking all**
7. (Optional) **show radius-server** {*hostname* | *ip-address*}
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip device tracking enable** **Example:** `switch(config)# ip device tracking enable`	Enables the IP device tracking. The default state is enabled.

	Command or Action	Purpose
Step 3	(Optional) **ip device tracking probe** {**count** *count* | **interval** *seconds*} **Example:** `switch(config)# ip device tracking probe count 4`	Configures these parameters for the IP device tracking table: **count** Sets the number of times that the Cisco NX-OS device sends the ARP probe. The range is from 1 to 5. The default is 3. **interval** Sets the number of seconds that the Cisco NX-OS device waits for a response before resending the ARP probe. The range is from 1 to 302300 seconds. The default is 30 seconds
Step 4	(Optional) **radius-server host** {*hostname* | *ip-address*} **test** [**username** *username* [**password** *password*]] [**idle-time** *minutes*] **Example:** `switch(config)# radius-server host 10.10.1.1 test username User2 password G1r2D37&k idle-time 5`	Configures RADIUS server test packet parameters. The default username is test and the default password is test. The **idle-time** parameter determines how often the server is tested to determine its operational status. If there is no traffic to the RADIUS server, the NAD sends dummy packets to the RADIUS server based on the idle timer value. The default value for the idle timer is 0 minutes (disabled). If you have multiple RADIUS servers, reenter this command.

Step 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits global configuration mode.

Step 6	(Optional) **show ip device tracking all** **Example:** `switch# show ip device tracking all`	Displays IP device tracking information.
Step 7	(Optional) **show radius-server** {*hostname* | *ip-address*} **Example:** `switch# show radius-server 10.10.1.1`	Displays RADIUS server information.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Related Topics

Enabling EAPoUDP, on page 14

Clearing IP Device Tracking Information

You can clear IP device tracking information for AAA servers.

SUMMARY STEPS

1. (Optional) **clear ip device tracking all**
2. (Optional) **clear ip device tracking interface ethernet** *slot/port*
3. (Optional) **clear ip device tracking ip-address** *ipv4-address*
4. (Optional) **clear ip device tracking mac-address** *mac-address*
5. (Optional) **show ip device tracking all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **clear ip device tracking all** **Example:** `switch# clear ip device tracking all`	Clears all EAPoUDP sessions.
Step 2	(Optional) **clear ip device tracking interface ethernet** *slot/port* **Example:** `switch# clear ip device tracking interface ethernet 2/1`	Clears EAPoUDP sessions on a specified interface.
Step 3	(Optional) **clear ip device tracking ip-address** *ipv4-address* **Example:** `switch# clear ip device tracking ip-address 10.10.1.1`	Clears an EAPoUDP session for a specified IPv4 address in the format A.B.C.D.
Step 4	(Optional) **clear ip device tracking mac-address** *mac-address* **Example:** `switch# clear ip device tracking mac-address 000c.30da.86f4`	Clears an EAPoUDP session for a specified MAC address in the format XXXX.XXXX.XXXX.
Step 5	(Optional) **show ip device tracking all** **Example:** `switch# show ip device tracking all`	Displays IP device tracking information.

Manually Initializing EAPoUDP Sessions

You can manually initialize EAPoUDP sessions.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. (Optional) **eou initialize all**

2. (Optional) **eou initialize authentication** {**clientless** | **eap** | **static**}
3. (Optional) **eou initialize interface ethernet** *slot/port*
4. (Optional) **eou initialize ip-address** *ipv4-address*
5. (Optional) **eou initialize mac-address** *mac-address*
6. (Optional) **eou initialize posturetoken** *name*
7. (Optional) **show eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **eou initialize all** **Example:** `switch# eou initialize all`	Initializes all EAPoUDP sessions.
Step 2	(Optional) **eou initialize authentication** {**clientless** | **eap** | **static**} **Example:** `switch# eou initialize authentication static`	Initializes EAPoUDP sessions with a specified authentication type.
Step 3	(Optional) **eou initialize interface ethernet** *slot/port* **Example:** `switch# eou initialize interface ethernet 2/1`	Initializes EAPoUDP sessions on a specified interface.
Step 4	(Optional) **eou initialize ip-address** *ipv4-address* **Example:** `switch# eou initialize ip-address 10.10.1.1`	Initializes an EAPoUDP session for a specified IPv4 address in the format A.B.C.D.
Step 5	(Optional) **eou initialize mac-address** *mac-address* **Example:** `switch# eou initialize mac-address 000c.30da.86f4`	Initializes an EAPoUDP session for a specified MAC address in the format XXXX.XXXX.XXXX.
Step 6	(Optional) **eou initialize posturetoken** *name* **Example:** `switch# eou initialize posturetoken Healthy`	Initializes an EAPoUDP session for a specific posture token name. **Note** Use the **show eou all** command to display the token names.
Step 7	(Optional) **show eou all** **Example:** `switch# show eou all`	Displays the EAPoUDP session configuration.

Related Topics

Enabling EAPoUDP, on page 14

Manually Revalidating EAPoUDP Sessions

You can manually revalidate EAPoUDP sessions.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. (Optional) **eou revalidate all**
2. (Optional) **eou revalidate authentication** {**clientless** | **eap** | **static**}
3. (Optional) **eou revalidate interface ethernet** *slot/port*
4. (Optional) **eou revalidate ip-address** *ipv4-address*
5. (Optional) **eou revalidate mac-address** *mac-address*
6. (Optional) **eou revalidate posturetoken** *name*
7. (Optional) **show eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **eou revalidate all** **Example:** `switch# eou revalidate all`	Revalidates all EAPoUDP sessions.
Step 2	(Optional) **eou revalidate authentication** {**clientless** | **eap** | **static**} **Example:** `switch# eou revalidate authentication static`	Revalidates EAPoUDP sessions with a specified authentication type.
Step 3	(Optional) **eou revalidate interface ethernet** *slot/port* **Example:** `switch# eou revalidate interface ethernet 2/1`	Revalidates EAPoUDP sessions on a specified interface.
Step 4	(Optional) **eou revalidate ip-address** *ipv4-address* **Example:** `switch# eou revalidate ip-address 10.10.1.1`	Revalidates an EAPoUDP session for a specified IPv4 address.
Step 5	(Optional) **eou revalidate mac-address** *mac-address* **Example:** `switch# eou revalidate mac-address 000c.30da.86f4`	Revalidates an EAPoUDP session for a specified MAC address.
Step 6	(Optional) **eou revalidate posturetoken** *name* **Example:** `switch# eou revalidate posturetoken Healthy`	Revalidates an EAPoUDP session for a specific posture token name. **Note** Use the **show eou all** command to display the token names.

	Command or Action	Purpose
Step 7	(Optional) **show eou all** **Example:** `switch# show eou all`	Displays the EAPoUDP session configuration.

Related Topics

Enabling EAPoUDP, on page 14

Clearing EAPoUDP Sessions

You can clear EAPoUDP sessions from the Cisco NX-OS device.

Before you begin

Enable EAPoUDP.

SUMMARY STEPS

1. (Optional) **clear eou all**
2. (Optional) **clear eou authentication** {**clientless** | **eap** | **static**}
3. (Optional) **clear eou interface ethernet** *slot/port*
4. (Optional) **clear eou ip-address** *ipv4-address*
5. (Optional) **clear eou mac-address** *mac-address*
6. (Optional) **clear eou posturetoken** *name*
7. (Optional) **show eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) **clear eou all** **Example:** `switch# clear eou all`	Clears all EAPoUDP sessions.
Step 2	(Optional) **clear eou authentication** {**clientless** | **eap** | **static**} **Example:** `switch# clear eou authentication static`	Clears EAPoUDP sessions with a specified authentication type.
Step 3	(Optional) **clear eou interface ethernet** *slot/port* **Example:** `switch# clear eou interface ethernet 2/1`	Clears EAPoUDP sessions on a specified interface.
Step 4	(Optional) **clear eou ip-address** *ipv4-address* **Example:** `switch# clear eou ip-address 10.10.1.1`	Clears an EAPoUDP session for a specified IPv4 address.

	Command or Action	Purpose
Step 5	(Optional) **clear eou mac-address** *mac-address* **Example:** `switch# clear eou mac-address 000c.30da.86f4`	Clears an EAPoUDP session for a specified MAC address.
Step 6	(Optional) **clear eou posturetoken** *name* **Example:** `switch# clear eou posturetoken Healthy`	Clears an EAPoUDP session for a specific posture token name. **Note** Use the **show eou all** command to display the token names.
Step 7	(Optional) **show eou all** **Example:** `switch# show eou all`	Displays the EAPoUDP session configuration.

Related Topics

Enabling EAPoUDP, on page 14

Disabling the EAPoUDP Feature

You can disable the EAPoUDP feature on the Cisco NX-OS device.

Caution Disabling EAPoUDP removes all EAPoUDP configuration from the Cisco NX-OS device.

Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

SUMMARY STEPS

1. **configure terminal**
2. **no feature eou**
3. **exit**
4. (Optional) **show feature**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no feature eou**	Disables EAPoUDP.

	Command or Action	Purpose
	Example: `switch(config)# no feature eou`	**Caution** Disabling the EAPoUDP feature removes all EAPoUDP configuration.

Step 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration mode.

Step 4	(Optional) **show feature** **Example:** `switch# show feature`	Displays the enabled or disabled status for the Cisco NX-OS features.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the NAC Configuration

To display NAC configuration information, perform one of the following tasks:

Command	Purpose
show eou [**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** *name*]	Displays the EAPoUDP configuration.
show ip device tracking [**all** | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address*]	Displays IP device tracking information.
show running-config eou [**all**]	Displays the EAPoUDP configuration in the running configuration.
show startup-config eou	Displays the EAPoUDP configuration in the startup configuration.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Configuration Example for NAC

The following example shows how to configure NAC:

```
feature eou
aaa authentication eou default group radius
mac access-list macacl-01
  10 permit any any 0x100
```

```
interface Ethernet8/1
  mac access-group macacl-01
```

Additional References for NAC

This section lists the additional references for NAC.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*