Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node. This service monitors and controls network access of endpoints. ANC is invoked by the ISE administrator on the admin GUI, and also can be invoked through pxGrid from third-party systems. ANC supports wired and wireless deployments and requires a Plus License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint. As a result, the established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

There are no limits to the number of users that can be quarantined at one time. Also, there are no time constraints on the quarantine period length.

You can perform the following operations to monitor and control network access through ANC:

- Quarantine: Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.

- Unquarantine: Allows you to reverse the quarantine status that permits full access to the network for an endpoint. This happens by returning the endpoint to its original VLAN.

- Shutdown: Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shut down on the NAS to which an endpoint is connected, manually reset the port on the NAS again. This allows an endpoint to connect to the network, which is not available for wireless deployments.

Quarantine and unquarantine operations can be triggered from the session directory reports for active endpoints.

Note If a quarantined session is unquarantined, the initiation method for a newly unquarantined session depends on the authentication method that is specified by the switch configuration.

- Enable Adaptive Network Control in Cisco ISE, on page 2
- Configure Network Access Settings, on page 2
- ANC NAS Port Shutdown Flow, on page 3

- Endpoints Purge Settings, on page 4
- Quarantined Endpoints Do Not Renew Authentication Following Policy Change, on page 5
- ANC Operations Fail when IP Address or MAC Address is not Found, on page 5
- Externally Authenticated Administrators Cannot Perform ANC Operations, on page 6

Enable Adaptive Network Control in Cisco ISE

ANC is disabled by default. ANC gets enabled only when pxGrid is enabled, and it remains enabled until you manually disable the service in the Admin portal.

Configure Network Access Settings

ANC allows you to reset the network access status of an endpoint to quarantine, unquarantine, or shut down a port. These define the degree of authorization for the endpoints in the network.

You can quarantine or unquarantine endpoints, or shut down the network access server (NAS) ports to which endpoints are connected, by using their endpoint IP addresses or MAC addresses. You can perform quarantine and unquarantine operations on the same endpoint multiple times, provided they are not performed simultaneously. If you discover a hostile endpoint on your network, you can shut down the endpoint's access, using ANC to close the NAS port.

To assign an ANC policy to an endpoint:

Before you begin

- Enable ANC.
- Create authorization profiles and exception type authorization policies for ANC.

Step 1 Choose **Operations** > **Adaptive Network Control** > **Policy List**.

Step 2 Click **Add**.

Step 3 Enter a name for the ANC policy and specify the ANC action. The following options are available:

- Quarantine
- Shut_Down
- Port_Bounce

You can select one or multiple actions, but you cannot combine Shut_Down and Port_Bounce with the other ANC actions .

Quarantine and Re_Authenticate are the only two actions that can be combined.

When an ANC policy with Quarantine, Port_Bounce, or Re_Authenticate is assigned or unassigned to an active endpoint, a CoA is triggered for that endpoint.

When an ANC policy with Shut_Down action is assigned to an active endpoint, a CoA is triggered to shutdown the switch interface. However, CoA is not triggered when an ANC policy with Shut_Down action is unassigned.

Step 4 Choose **Policy** > **Policy Sets**, and expand the policy set.

Step 5 Associate the ANC policy with the corresponding authorization policy by using the ANCPolicy attribute.

Step 6 Choose **Operations > Adaptive Network Control > Endpoint Assignment**.

Step 7 Click **Add**.

Step 8 Enter the IP address or MAC address of the endpoint and select the policy from the **Policy Assignment** drop-down list.

Step 9 Click **Submit**.

Create Authorization Profiles for Network Access through ANC

You need to create an authorization profile that should be use with ANC. you can view the authorization profile in the list of Standard Authorization Profiles. An endpoint can be authenticated and authorized in the network, but restricted to access network.

Step 1 Choose **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add**.

Step 3 Enter a unique name and description for the authorization profile, and update the **Access Type** as **ACCESS_ACCEPT**.

Step 4 Check the **DACL Name** check box, and choose **DENY_ALL_TRAFFIC** from the drop-down list.

Step 5 Click **Submit**.

Exception authorization polices are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement. For ANC authorization, you need to create a quarantine exception policy that is processed before all standard authorization policies. You need to create an exception rule with the following condition:

Session:ANCPolicy EQUALS Quarantine.

ANC NAS Port Shutdown Flow

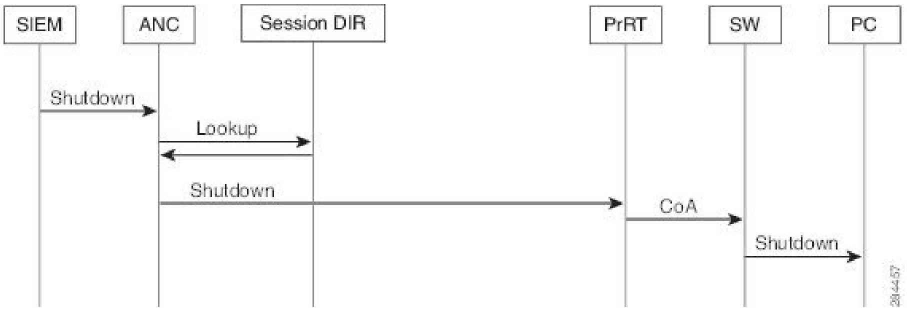
You can shut down the NAS port to which an endpoint is connected by using the endpoint IP address or MAC address.

Shutdown allows you to close a NAS port based on a specified IP address for a MAC address. You have to manually reinstate the port to bring the endpoint back into the network, which is effective only for endpoints that are connected through wired media.

Shutdown may not be supported on all devices. Most switches should support the shutdown command, however. You can use the getResult() command to verify that the shutdown is executed successfully.

This figure illustrates the ANC shutdown flow. For the client device, the shutdown operation is performed on the NAS that the client device uses to access the network.

Figure 1: ANC Shutdown Flow



Endpoints Purge Settings

You can define the endpoint purge policy by configuring the rules, based on identity groups and other conditions. Choose **Administration** > **Identity Management** > **Settings** > **Endpoint Purge**. You can choose not to purge specified endpoints and to purge endpoints based on selected profiling conditions.

You can schedule an endpoint purge job. This endpoint purge schedule is enabled by default. Cisco ISE, by default, deletes endpoints and registered devices that are older than 30 days. The purge job runs at 1:00 a.m. (midnight) every day based on the time zone configured in the primary PAN.

Endpoint purge deletes over five thousand endpoints every 3 minutes.

The following are some of the conditions with examples you can use for purging the endpoints:

- InactivityDays— Number of days since last profiling activity or update on endpoint
  - This condition purges stale devices that have accumulated over time, commonly transient guest or personal devices, or retired devices. These endpoints tend to represent noise in your deployment as they are no longer active on network or not likely to be seen in near future. If they do happen to connect again, then they will be rediscovered, profiled, registered, etc as needed.
  - When there are updates from endpoint, InactivityDays will be reset to 0 only if profiling is enabled.
- ElapsedDays—Numbers days since object is created.
  - This condition can be used for endpoints that have been granted unauthenticated or conditional access for a set time period, such as a guest or contractor endpoint, or employees leveraging webauth for network access. After the allowed connect grace period, they must be fully reauthenticated and registered.
- PurgeDate—Date to purge the endpoint.
  - This option can be used for special events or groups where access is granted for a specific time, regardless of creation or start time. This allows all endpoints to be purged at same time. For example, a trade show, a conference, or a weekly training class with new members each week, where access is granted for specific week or month rather than absolute day, week, or month.

Quarantined Endpoints Do Not Renew Authentication Following Policy Change

Problem

Authentication has failed following a change in policy or additional identity and no reauthentication is taking place. Authentication fails or the endpoint in question remains unable to connect to the network. This issue often occurs on client machines that fails posture assessment per the posture policy that is assigned to the user role.

Possible Causes

The authentication timer setting is not correctly set on the client machine, or the authentication interval is not correctly set on the switch.

Solution

There are several possible resolutions for this issue:

1. Check the **Session Status Summary** report in Cisco ISE for the specified NAD or switch, and ensure that the interface has the appropriate authentication interval configured.
2. Enter “show running configuration” on the NAD/switch and ensure that the interface is configured with an appropriate “authentication timer restart” setting. (For example, “authentication timer restart 15,” and “authentication timer reauthenticate 15.”)
3. Enter “interface shutdown” and “no shutdown” to bounce the port on the NAD/switch and force reauthentication following a potential configuration change in Cisco ISE.

Note Because CoA requires a MAC address or session ID, we recommend that you do not bounce the port that is shown in the Network Device SNMP report.

ANC Operations Fail when IP Address or MAC Address is not Found

An ANC operation that you perform on an endpoint fails when an active session for that endpoint does not contain information about the IP address. This also applies to the MAC address and session ID for that endpoint.

Note When you want to change the authorization state of an endpoint through ANC, you must provide the IP address or the MAC address for the endpoint. If the IP address or the MAC address is not found in the active session for the endpoint, then you will see the following error message:

```
No active session found for this MAC address, IP Address or Session ID
```

.

Externally Authenticated Administrators Cannot Perform ANC Operations

If an externally authenticated administrator tries to issue CoA-Quarantine from a live session, Cisco ISE returns the following error message:

```
CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User
 not found internally. Possible use of unsupported externally authenticated user
```

If an externally authenticated administrator performs an ANC operation from **Operations** in the Cisco ISE using the IP address or MAC address of the endpoint, Cisco ISE returns the following error message:

```
Server failure: User not found internally. Possible use of unsupported externally
 authenticated user
```