Setup Endpoint Protection ServiceAdaptive Network Control

Enable Endpoint Protection Service Adaptive Network Control in Cisco ISE

Endpoint Protection Service (EPS) Adaptive Network Control (ANC) is disabled by default. You must enable EPS ANC manually, and it remains enabled until you manually disable the service in the Admin portal.

You must have Super Admin and Policy Admin role privileges to enable EPS ANC in Cisco ISE.

Step 1 Choose **Administration** > **System** > **Settings** > **Endpoint Protection Service** > **Adaptive Network Control**.

Step 2 Click the Service Status drop-down list, and choose **Enabled**.

Step 3 Click **Save**.

Configure Network Access Settings

Endpoint Protection Service (EPS) Adaptive Network Control (ANC) allows you to reset the network access status of an endpoint to quarantine, unquarantine, or shutdown a port, which defines authorization to the network depending on the network access status.

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 EPS ANC to close the NAS port.

Before You Begin

- You must enable EPSANC.
- You must create authorization profiles and Exception type authorization policies for EPSANC.

Step 1 Choose **Operations** > **Endpoint Protection Service** > **Adaptive Network Control**.

Step 2 Under **Endpoint Operation**, enter the IP Address or MAC Address of an endpoint.

Step 3 Click the Operations drop-down list to choose one of the following actions:

- **Quarantine—**Isolates the endpoint, restricting access on the network
- **Unquarantine—**Reverses the quarantine process, allowing full access to the network
- **Shutdown—**Closes the NAS port to which the endpoint is connected

Step 4 Click **Submit**.

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 are failing 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 Try entering “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.

Endpoint Protection ServiceAdaptive Network Control

Endpoint Protection Service (EPS) Adaptive Network Control (ANC) is a service that runs on the Administration node that can be used for monitoring and controlling network access of endpoints. EPS is also known as Adaptive Network Control (ANC). EPS ANC can be invoked by the ISE administrator on the admin GUI and also through pxGrid from third party systems. EPS ANC supports wired and wireless deployments and requires a Plus License.

You can use EPS ANC to change the authorization state without having to modify the overall authorization policy of the system. EPS ANC allows you to set the authorization state when you quarantine an endpoint as a result of established authorization policies where authorization policies are defined to check for EPSStatus 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, and there are no time constraints on the length of the quarantine period.

You can perform the following operations to monitor and control network access through EPS 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 EPSStatus. 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 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 shutdown on the NAS to which an endpoint is connected, you must manually reset the port on the NAS again to allow 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.

Create Authorization Profiles for Network Access through EPSANC

You must create an authorization profile for use with EPS ANC and the authorization profile appears 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 leave 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**.

Create Exception Policies for Network Access through EPSANC

For EPS ANC authorization, you must create a quarantine exception policy that is processed before all standard authorization policies. Exception authorization polices are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement. Standard authorization policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.

Before You Begin

You should have successfully created standard authorization profiles for use with EPS ANC.

Step 1 Choose **Policy** > **Authorization**, and expand **Exceptions**.

Step 2 Choose **Enabled** or **Disabled** or **Monitor Only option**.

Step 3 Click **Create a New Rule**.

Step 4 Enter the exception rule name.

Step 5 Click the plus [+] sign to choose an identity group.

Step 6 Click the plus [+] sign to choose **Create New Condition (Advanced Option)**.

Step 7 Click the down arrow icon in the first field to display the dictionaries list and choose **Session** > **EPSStatus**.

Step 8 Choose **Equals** from the drop-down list in the second field.

Step 9 Choose **Quarantine** from the drop-down list in the third field.

Step 10 Click **Save**.

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

An EPS 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 EPS 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 EPSANC 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 EPS ANC operation from Operations > Endpoint Protection Service Adaptive Network Control in the Cisco ISE Admin portal using the IP address or MAC address of the endpoint, Cisco ISE returns the following error message:

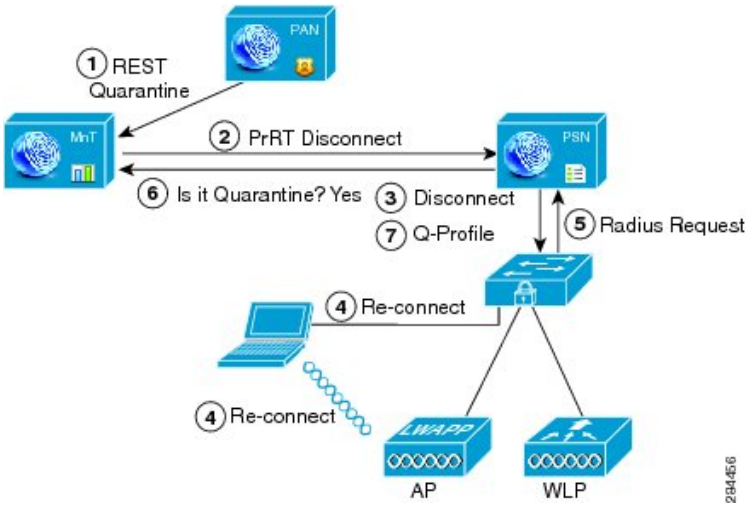
Server failure: User not found internally. Possible use of unsupported externally authenticated user

EPSANC Quarantine and Unquarantine Flow

You can quarantine selected endpoints with EPS ANC, to limit their access to the network. You can quarantine endpoints and establish exception authorization policies that assign different authorization profiles, depending on the status. An authorization profile acts as a container for permissions that you define in the authorization policies that allow access to specified network services. When the authorization is complete, the permissions are granted for a network access request. If the endpoint is then validated, you can unquarantine the endpoint to allow it full access to the network.

This figure illustrates the quarantine flow, which assumes that authorization rules have been configured and the EPS ANC session has been established.

Figure 1: EPS ANC Quarantine Flow



1. A client device logs onto the network through a wireless device (WLC), and a quarantine REST API call is issued from the Administration node (PAP) to the Monitoring node (MnT).
2. The Monitoring node then calls PrRT through the Policy Services ISE node (PDP) to invoke a CoA.
3. The client device is disconnected.
4. The client device then reauthenticates and reconnects.
5. A RADIUS request for the client device is sent back to the Monitoring node.
6. The client device is quarantined while the check is made.
7. The Q-Profile authorization policy is applied, and the client device is validated.
8. The client device is unquarantined, and allowed full access to the network.

EPSANC 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, and 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 shut down command, however. You can use the getResult() command to verify that the shutdown executed successfully.

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

Figure 2: EPS ANC Shutdown Flow

Endpoints Purge Settings

You can define the Endpoint Purge Policy by configuration rules based on identity groups and other conditions using **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 AM every day based on the time zone configured in the Primary Administration Node (PAN).

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 most deployments as they are no longer active on network or 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 days/weeks/months.