CHAPTER 11

Setting Up Endpoint Protection Services

This chapter describes how to set up and configure Endpoint Protection Services (EPS), and covers the following topics:

About Endpoint Protection Services

Endpoint Protection Services (EPS) is a service that runs on the Cisco Identity Services Engine Administration node to extend the monitoring and controlling of endpoints. You can use EPS to monitor and change the authorization state of an endpoint without having to modify the overall Authorization Policy of the system. EPS supports both wired and wireless deployments.

Note EPS is available only with an ISE Advanced license. If you do not have an ISE Advanced license installed, the EPS functionality is not available. For more information, see Chapter 12, "Managing Licenses."

EPS Functional Overview

This section provides an overview of the functional aspects of EPS in Cisco ISE. EPS operations are supported on both wired and wireless deployments.

EPS allows administrators to manage endpoints through the following actions:

- Quarantine—uses policies to disallow an endpoint access to the network, or limits its access. Policies can be created to assign different authorization profiles depending on the status.
- Unquarantine—reverses the quarantine status, and allowing the endpoint full access to the network.
- Shutdown—deactivates a port on the network attached system (NAS). Once a port is shutdown, you must manually reset the port.

Note Because you must manually reset the port, the shutdown operation is not available for wireless access and devices.

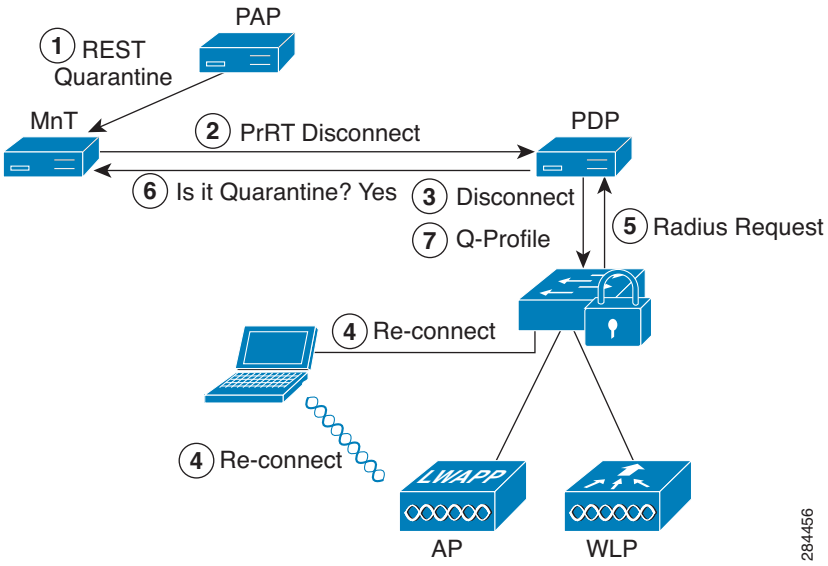
Quarantine and Unquarantine

You can set endpoint protection status to quarantine, and establish policies that assign different authorization profiles, depending on the status of the endpoint.

Quarantine essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. The The Quarantine VLAN must be previously defined by a network administrator and supported on the same NAS as the endpoint. Unquarantine reverses the quarantine action, returning the endpoint to its original VLAN.

The quarantine and unquarantine actions are performed as a result of established Authorization Rules that are defined to check for EPSStatus. In Figure 11-1, the quarantine flow assumes that rules have been configured and the EPS session has been established.

Figure 11-1 EPS Quarantine Flow

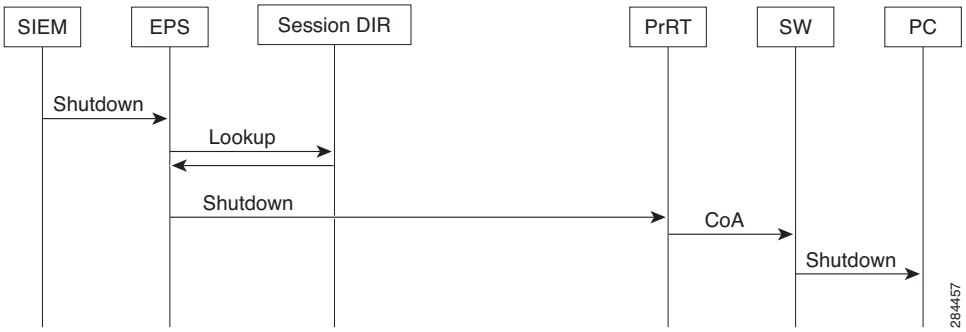


1. A PC endpoint logs onto the network through a wireless device (WLC), and a quarantine REST API call is issued from the Administration ISE node to the Monitoring ISE node.
2. The Monitoring ISE node then calls PrRT through the Policy Services ISE node to invoke a CoA.
3. The PC endpoint is disconnected.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

Shutdown

The shutdown function gives the administrator the ability to close a port based on a specified IP address for MAC address. This function may not be supported on all devices. Figure 11-2 illustrates the EPS shutdown flow.

Figure 11-2 EPS Shutdown Flow



For the PC in the illustration, the shutdown operation is performed on the switch that the PC uses to access the network.

Warning **When you shutdown a port in this manner, you must manually reset the port to make it active again.**

Enabling and Disabling EPS

Endpoint Protection Services (EPS) is disabled by default. You must have Super Admin and Policy Admin role privileges to enable the service, as described in the following procedure.

Note EPS is only available with an ISE Advanced license. If you do not have an ISE Advanced license installed, the EPS functionality is not available. For more information, see Chapter 12, "Managing Licenses."

To enable and disable EPS, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Administration > System > Settings**.

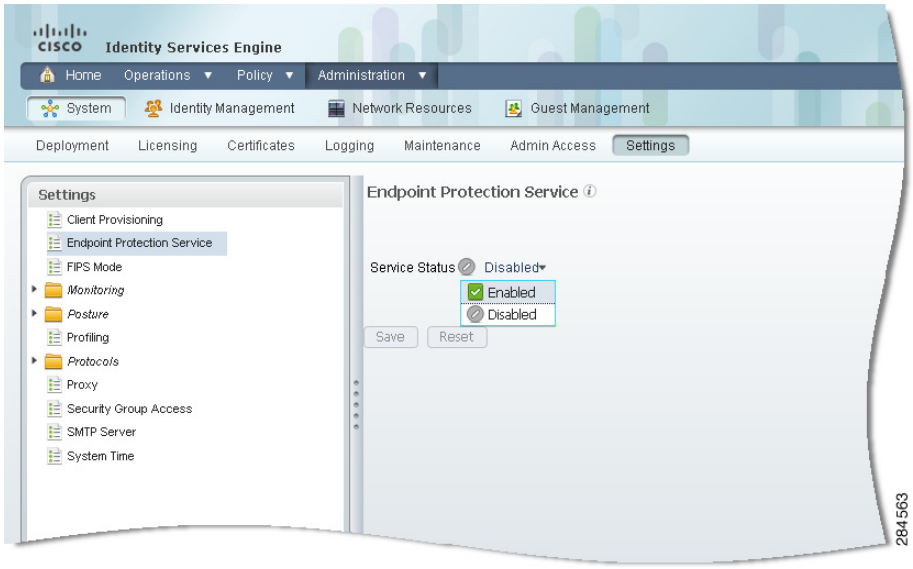
Step 2 In the Settings panel on the left, select **Endpoint Protection Service**.

Step 3 To enable EPS, from the Service Status drop-down menu select **Enabled** and click **Save**.

The service remains enabled until it is manually disabled.

Step 4 To disable EPS, from the Service Status drop-down menu select **Disabled** and click **Save**.

Figure 11-3 Enable and Disable EPS



For information on how to verify that EPS is enabled or disabled using the command line interface (CLI), see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*.

EPS Authorization

EPS allows you to reset the access status of an endpoint to quarantine, unquarantine, or shutdown. For this to occur, you must create an EPS authorization profile and policy rule.

This section covers the following topics:

Creating a Quarantine Authorization Profile

An authorization profile acts as a container for permissions that you define to allow access to specified network services. When authorization is complete, the permissions are granted for a network access request. For more information, see Cisco ISE Authorization Policies and Profiles, page 17-5.

This section provides an example of how to create a quarantine authorization profile for use with EPS.

To create a quarantine authorization profile, complete the following steps:

Step 1 In the Cisco ISE Admin user interface, go to **Policy > Policy Elements > Results**.

Step 2 In the Results panel on the left, select **Authorization > Authorization Profiles**.

The Standard Authorization Profiles panel appears on the right.

Step 3 In the Standard Authorization Profiles panel, click **Add**.

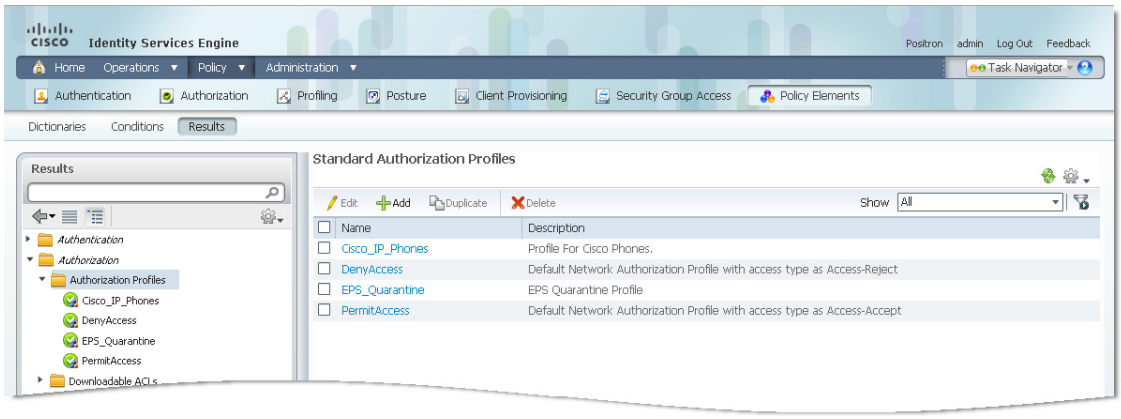
Step 4 Enter a unique **Name** and **Description**, and leave the Access Type as ACCESS_ACCEPT.

Step 5 Check the DACL Name check box and choose **DENY_ALL_ACCESS** from the drop-down list.

Step 6 Click **Save**.

The quarantine profile appears in the list of Standard Authorization Profiles, as shown in Figure 11-4.

Figure 11-4 EPS Quarantine Profile



Creating an EPS Policy and Rule

There are two types of authorization policies: standard and exception. Standard policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.

By contrast, exception policies act as exceptions to standard policies. Exception polices are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement.

For EPS authorization, it is recommended that you create a quarantine status exception rule that is processed before the standard policies are processed. For more information on both of these types of policies, see Understanding Authorization Policies, page 17-1.

Prerequisite

You should have successfully completed Creating a Quarantine Authorization Profile, page 11-4.

To create an EPS exception policy and rule, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Policy > Authorization**, and expand the **Exceptions** panel.

Step 2 Click **Create New Rule** and enter a **Rule Name** in the text field, such as EPS Exception Rule.

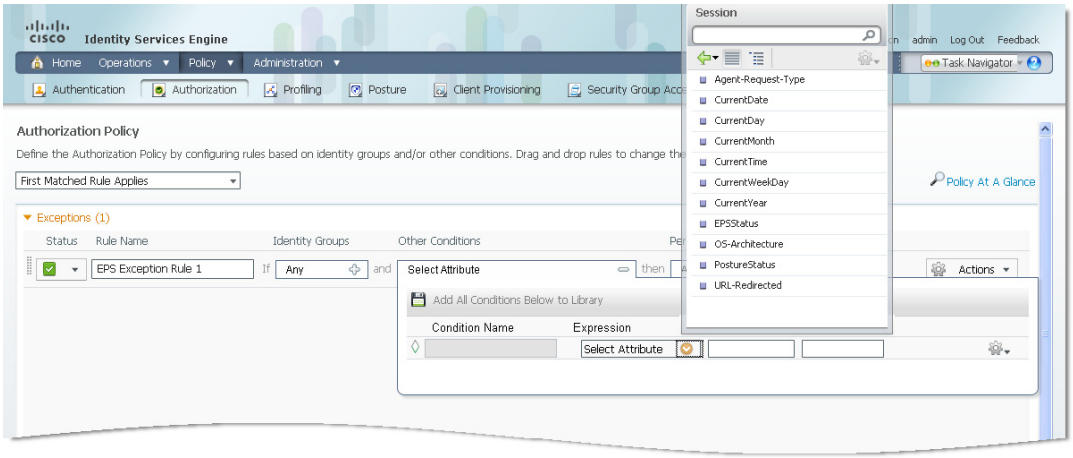
Step 3 Click the **Identity Group** plus sign (**+**) and choose an identity group, or leave the default, Any, as desired.

Step 4 Click the **Conditions** plus sign (**+**), and then click **Create New Condition (Advanced Option)**.

Step 5 Under Expression click **Select Attribute**, and then from the Dictionaries list choose **Session**.

Step 6 From the Session list, choose **EPSStatus**, then choose **Equals** from the first drop-down list on the right, and choose **Quarantine** from the second drop-down list.

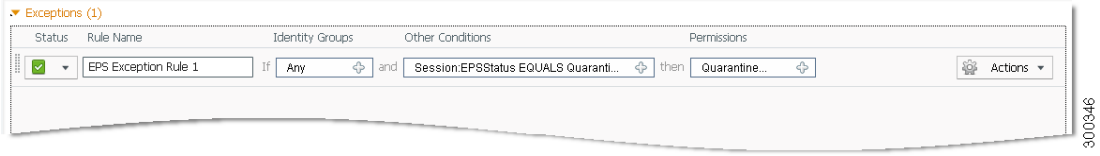
Figure 11-5 Set EPSStatus



Step 7 Scroll down and click **Save**.

The EPS exception rule appears in the Exception list, as shown in Figure 11-6.

Figure 11-6 EPS Exception Rule



Controlling Endpoints

You can quarantine selected endpoints with EPS, to limit their access to the network. If the endpoint is then validated, you can unquarantine the endpoint to allow it full access to the network. If you discover a hostile endpoint on your network, you can shutdown the endpoint's access, using EPS to close the port.

Note 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 executed successfully.

Quarantine and Unquarantine Endpoints

You can quarantine and unquarantine an endpoint using the endpoint IP address or MAC address.

Prerequisites

- EPS must be enabled, as described in Enabling and Disabling EPS, page 11-3.
- You should have established EPS Authorization, page 11-4.

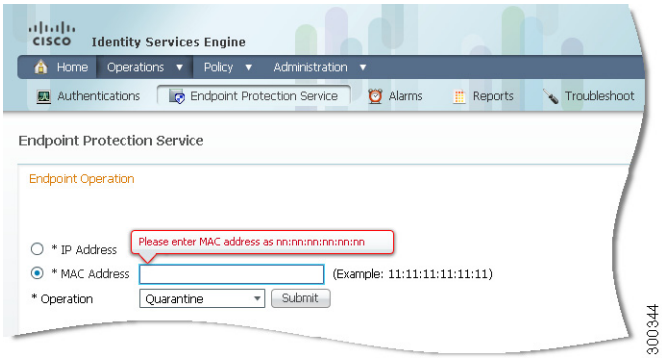
To quarantine and unquarantine an endpoint, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Endpoint Protection Service**.

Step 2 Click the **IP Address** or **MAC address** radio button, then enter the address for the endpoint in the text field, following the designated format.

Note If an active session does not contain information about the IP address of an endpoint, then an EPS operation with that IP address fails in Cisco ISE. This also applies to the MAC address and session ID for that endpoint. Cisco ISE throws the following error message: No active session found for this MAC address, IP Address, or Session ID when an EPS operation is performed with that IP address, MAC address, or session ID not found in the active session.

Figure 11-7 Endpoint Operation



Step 3 From the Operation drop-down menu, select one of the following:

- Quarantine — isolates the endpoint, restricting access on the network
- Unquarantine — reverses the quarantine process, allowing full access to the network

Note Cisco ISE allows you to perform quarantine and unquarantine operations on the same endpoint multiple times, provided they are not performed simultaneously.

Step 4 Click **Submit.**

Port Shutdown

You can shutdown the switch port that an endpoint is connected to using the endpoint IP address or MAC address.

Warning **The shutdown operation closes the switch port. Once this occurs, you have to manually reinstate the port to bring the endpoint back onto the network.**

The shutdown operation is effective only for endpoints that are connected through wired media.

To shutdown an endpoint, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Endpoint Protection Service**.

Step 2 Click the **IP Address** or **MAC address** radio button, then enter the address for the endpoint in the text field, following the designated format.

Step 3 From the Operation drop-down menu, select **Shutdown.**

Step 4 Click **Submit**.

Note You can also verify that a port is shutdown using the getResult() command on the CLI. For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*.

Monitoring EPS Data

You can view EPS data in the following formats:

- Endpoint Protection Services Report
- Session Directory Reports

This section walks you through the process of running each of these reports. For more information on Cisco ISE reports, see Chapter 25, “Reporting.”

Endpoint Protection Services Report

To view EPS report data, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Endpoint Protection Services**.

Step 3 In the Reports panel on the right, click the **Endpoint Operations History** check box.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last 30 minutes
- Last hour
- Last 12 hours

- Today
- Yesterday
- Last 7 days
- Last 30 days
- Query and run

The report runs upon choosing the time period, and the Endpoint Operations History data appears.

Session Directory Reports

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

RADIUS Session Directory reports can also be used to track EPS data. 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.

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.

To track EPS data using Session Directory reports, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Session Directory**.

Step 3 In the Reports panel on the right, click one of the following radio buttons:

- RADIUS Active Sessions—Provides information on RADIUS authenticated, authorized, and started sessions.
- RADIUS Session History—Provides a summary of RADIUS session history, such as total authenticated and terminated sessions, as well as total and average session duration and throughput for a selected time period.
- RADIUS Terminated Sessions—Provides all the RADIUS terminated session information for a selected time period.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last 30 minutes
- Last hour
- Last 12 hours
- Today
- Yesterday
- Last 7 days

- Last 30 days
- Query and run

The report runs upon choosing the time period, and the report data appears.