

Configure Pop-Up Notification in Cisco Secure Endpoint

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure Pop-Up notifications when Cisco Secure Endpoint detects a malicious file.

Contributed by Javier Martinez, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- Cisco Secure Endpoint Console dashboard
- An account with administrator privileges

Components Used

The information in this document is based on Cisco Secure Endpoint version 6.3.7 and above.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

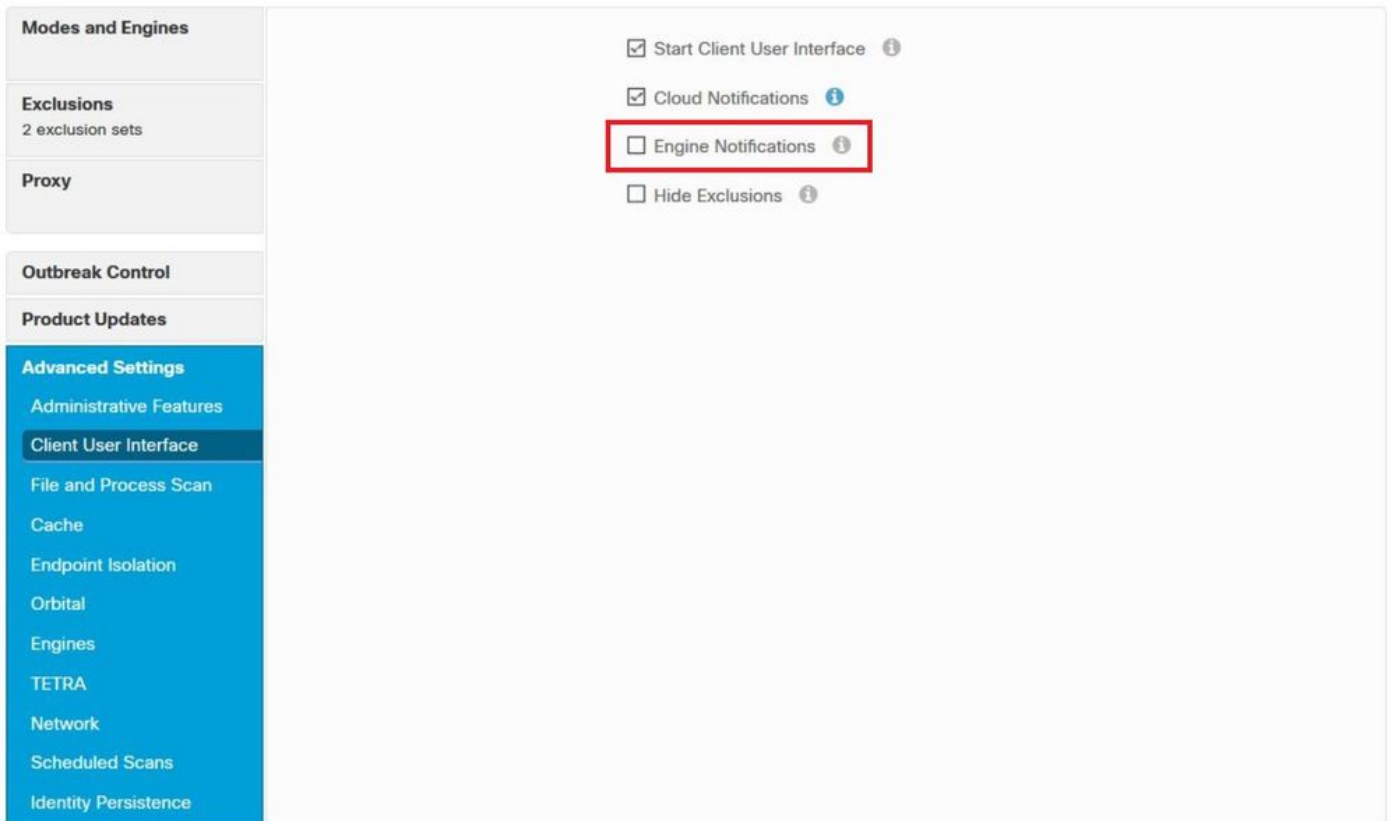
Configure

Cisco Secure Endpoint can send a Pop-Up alert in the Endpoint about the main Secure Endpoint engines when it detects, blocks, or quarantines a file/process.

Step 1. Log in to AMP Console; <https://console.amp.cisco.com/> as shown in the image.

Step 2. Navigate to **Management > Policies** (select the policy) **>Advance settings > Client User Interface**.

Engine Notifications is disabled by default as shown in the image.



The screenshot shows the 'Client User Interface' settings page. On the left, a navigation menu lists various settings categories, with 'Client User Interface' selected. The main content area displays four checkboxes: 'Start Client User Interface' (checked), 'Cloud Notifications' (checked), 'Engine Notifications' (unchecked and highlighted with a red box), and 'Hide Exclusions' (unchecked). Each checkbox has an information icon to its right.

Step 3. Mark **Engine Notifications** checkbox as shown in the image.

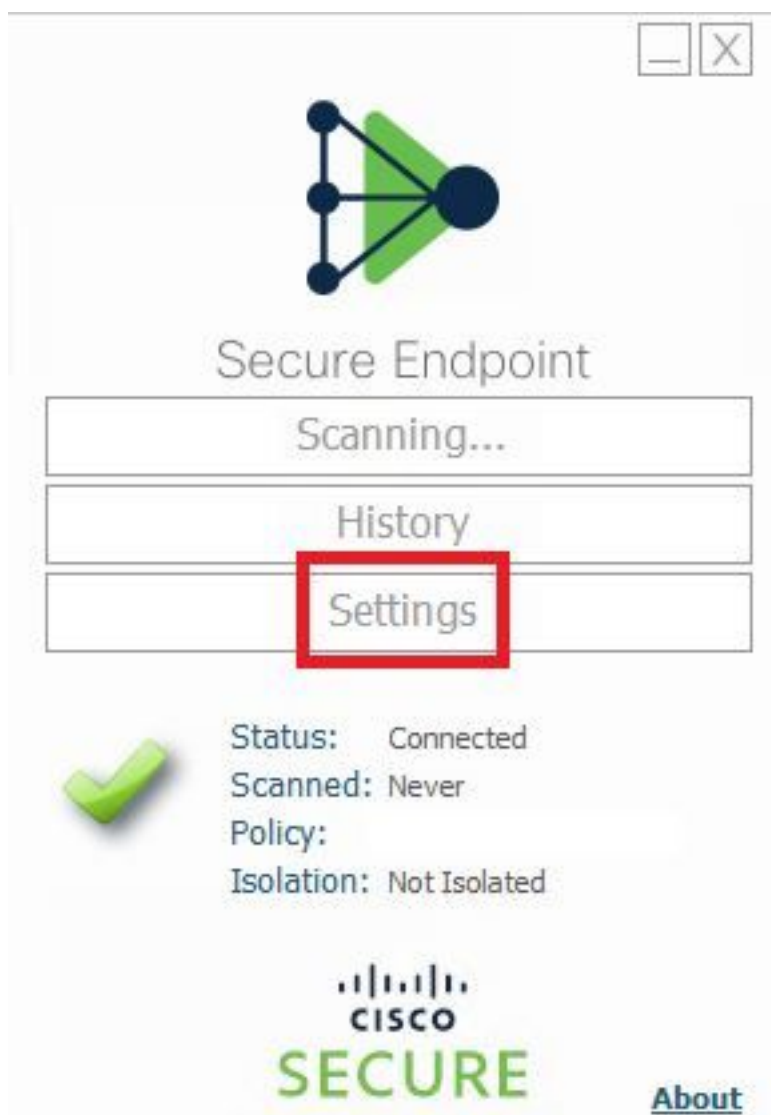
Start Client User Interface 

Cloud Notifications 

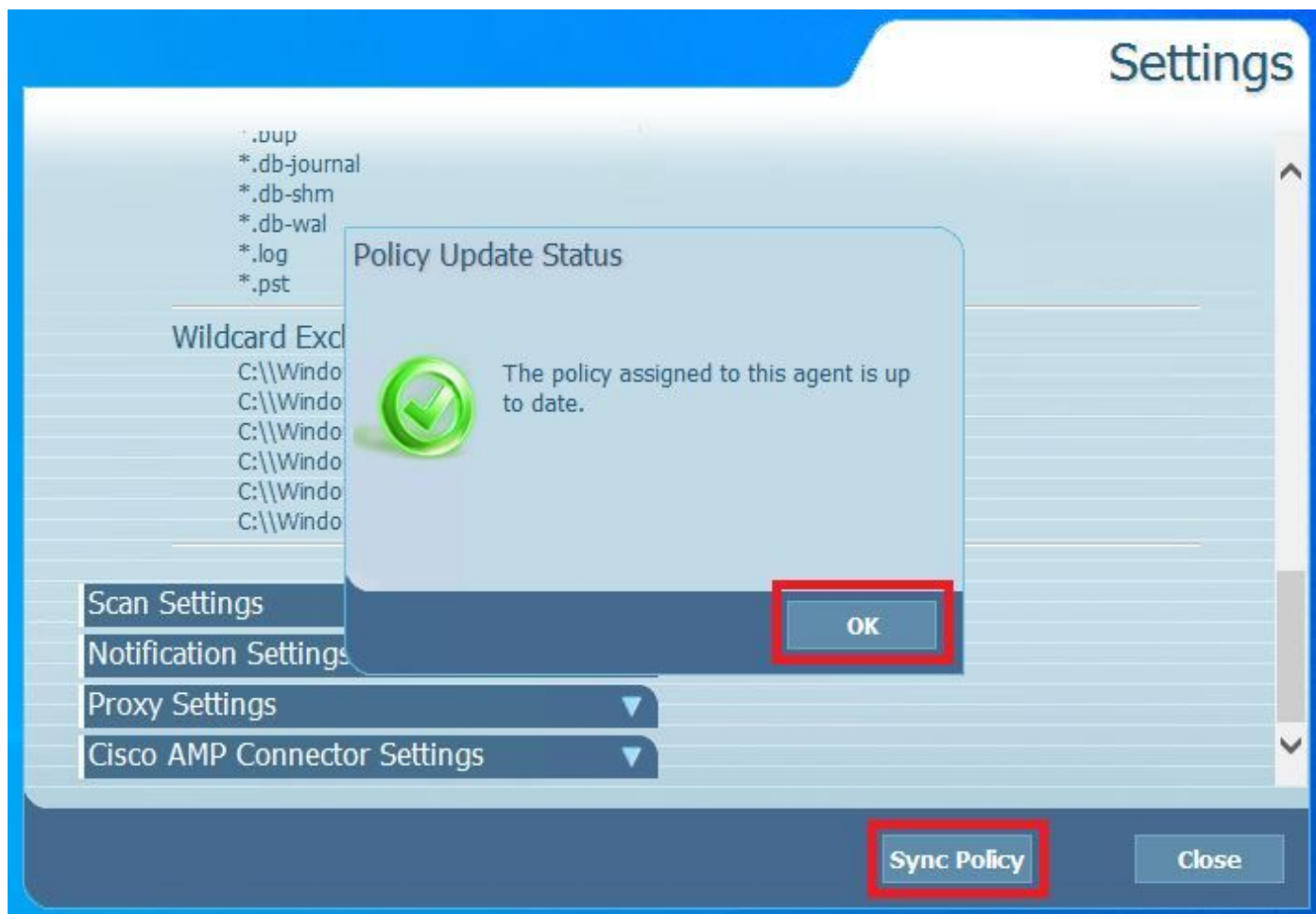
Engine Notifications 

Hide Exclusions 

Step 4. In order to apply the new changes, navigate to Desktop > OpenCisco Secure Endpoint and select **Settings**, as shown in the image.



Step 5. Click on **Sync Policy** and select **OK**, as shown in the image.



Verify

Use this section in order to confirm that your configuration works properly.

When the Secure Endpoint engine quarantines a file/process, you can see a pop-up notification on the desktop, as shown in the image.



Note: This configuration applies to all devices that belong to the Policy.

Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

In case Secure Endpoint does not trigger a Pop-Up notification, you can see an Alert Event on Secure Endpoint Console.

Navigate to **Cisco Secure Endpoint Console > Dashboard > Events**, as shown in the image.

[redacted] detected \$RMTWB9L.7z as Trojan.Agent.DPDW		Medium	Quarantine: Successful	2020-09-01 11:18:29 CDT
File Detection	Detection	Trojan.Agent.DPDW		
Connector Details	Fingerprint (SHA-256)	[redacted]		
Comments	File Name	\$RMTWB9L.7z		
	File Path	[redacted]		
	File Size	1.17 KB		
	Parent	No parent SHA/Filename available.		
[Analyze] [Restore File] [All Computers]		[View Upload Status]	[Add to Allowed Applications]	[File Trajectory]

If there is not a pop-up Notification in the Endpoint or Alert Event in Secure Endpoint Console, please contact Cisco Support.

Cisco Support: Visit the online portal at <http://cisco.com/tac/caseopen> or Phone: Regional free phone numbers: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html