

在思科安全终端中配置弹出通知

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍当思科安全终端检测到恶意文件时如何配置弹出通知。

作者：Javier Martinez，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全终端控制台控制面板
- 具有管理员权限的帐户

使用的组件

本文档中的信息基于思科安全终端版本6.3.7及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

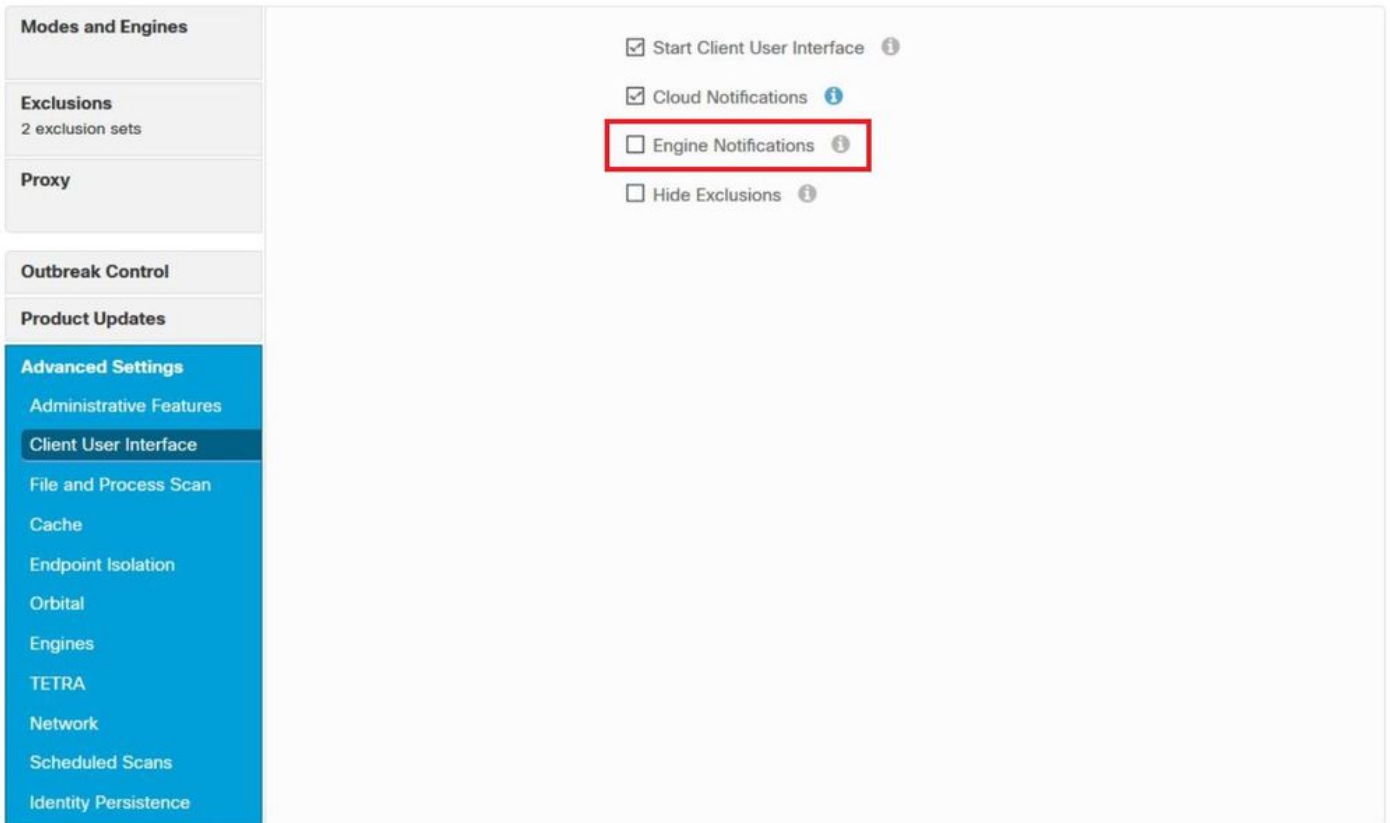
配置

当思科安全终端检测、阻止或隔离文件/进程时，可在终端中发送有关主安全终端的弹出警报。

步骤1. 登录AMP控制台；<https://console.amp.cisco.com/>，如图所示。

步骤2. 导航至 **Management > Policies (选择策略) > Advance settings > Client User Interface**。

默认情况下，引擎通知处于禁用状态，如图所示。



The screenshot shows the 'Client User Interface' settings page. On the left is a navigation menu with the following items: Modes and Engines, Exclusions (2 exclusion sets), Proxy, Outbreak Control, Product Updates, **Advanced Settings** (expanded), Administrative Features, **Client User Interface** (selected), File and Process Scan, Cache, Endpoint Isolation, Orbital, Engines, TETRA, Network, Scheduled Scans, and Identity Persistence. The main content area contains four settings:

- Start Client User Interface ⓘ
- Cloud Notifications ⓘ
- Engine Notifications ⓘ (highlighted with a red box)
- Hide Exclusions ⓘ

步骤3. 如图所示，标记引擎通知复选框。

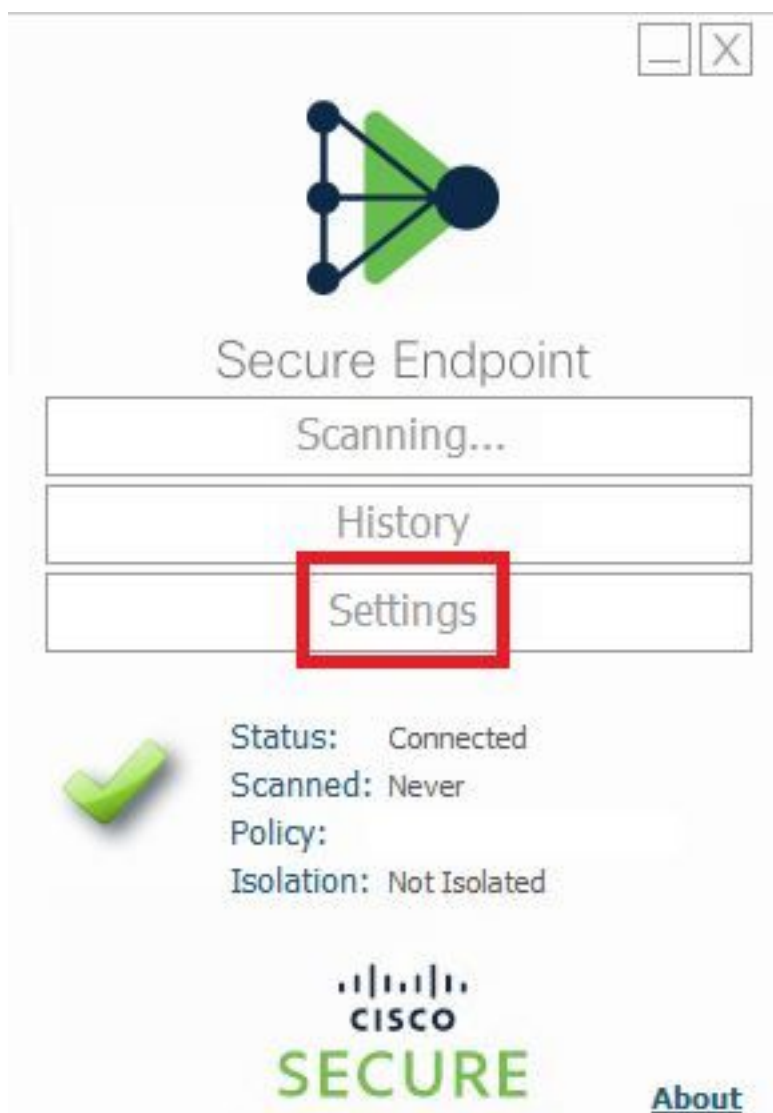
Start Client User Interface 

Cloud Notifications 

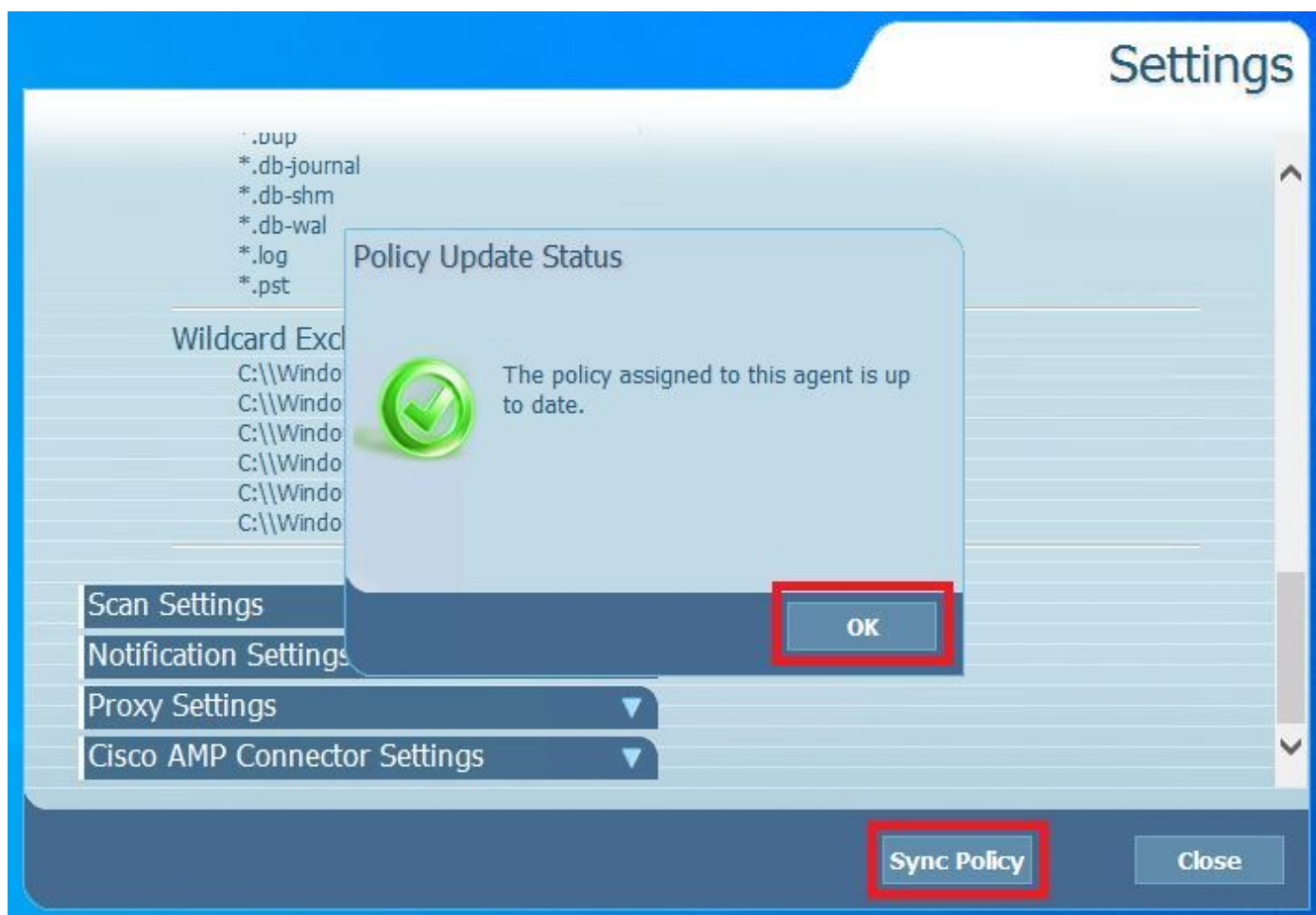
Engine Notifications 

Hide Exclusions 

步骤4.要应用新更改，请导航至Desktop (桌面) > OpenCisco Secure Endpoint (OpenCisco安全终端) 并选择Settings(设置)，如图所示。



步骤5.单击“同步策略”并选择“确定”，如图所示。



验证

使用本部分可确认配置能否正常运行。

当安全终端引擎隔离文件/进程时，您可以在桌面上看到弹出通知，如图所示。



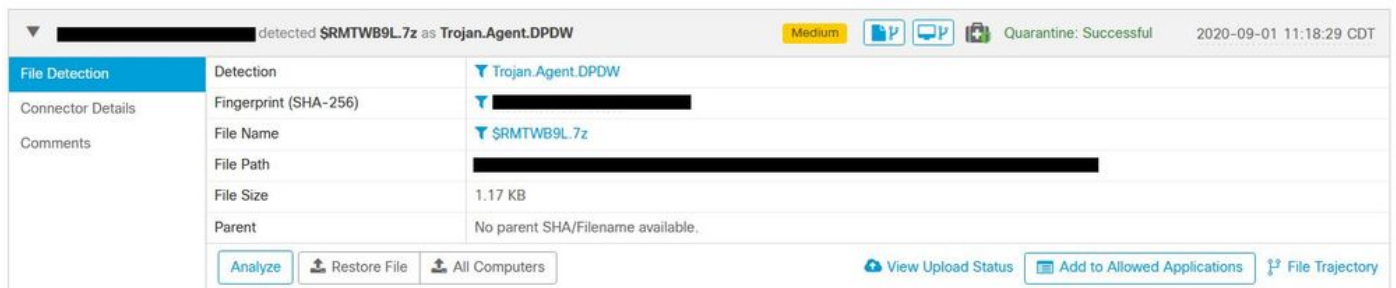
注意：此配置适用于属于策略的所有设备。

故障排除

本节提供可用于排除配置故障的信息。

如果安全终端未触发弹出通知，您可以在安全终端控制台上看到警报事件。

导航至Cisco Secure Endpoint Console > Dashboard > Events，如图所示。



如果终端或安全终端控制台中的警报事件中未弹出通知，请联系思科支持。

思科支持：请访问<http://cisco.com/tac/caseopen>或电话：地区免费电话号码

：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html