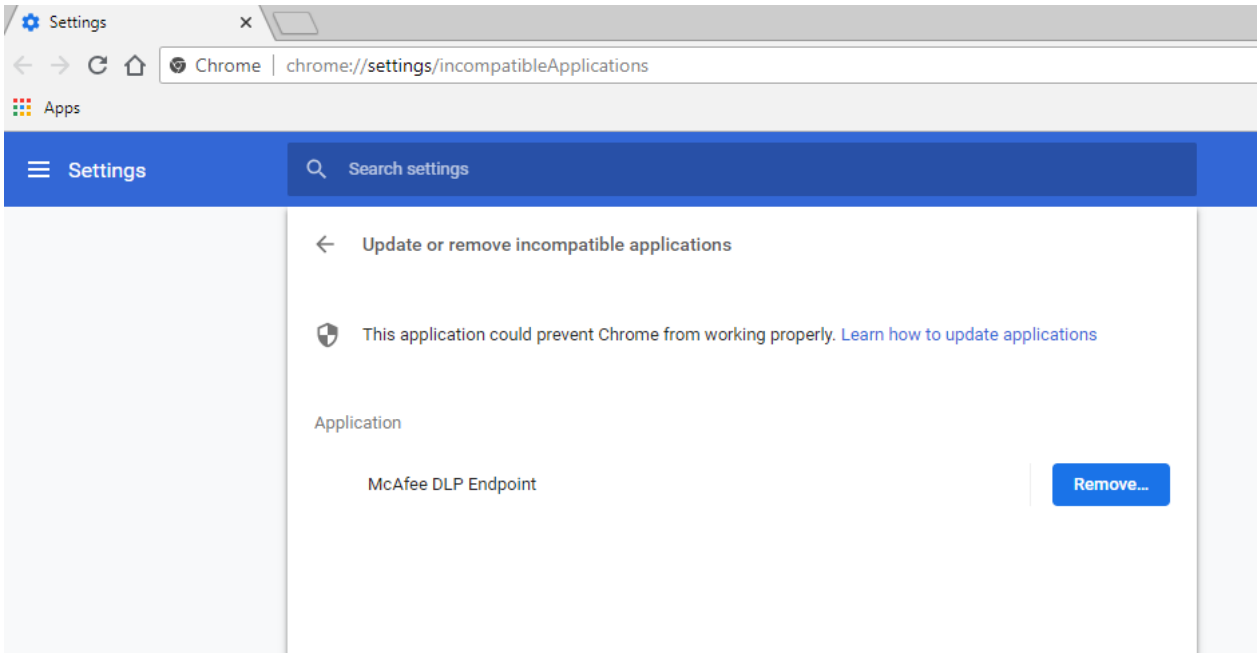
McAfee Data Loss Prevention and Google Chrome

Issue summary

The McAfee DLP endpoint inspects files and text uploads to web applications via web browsers as well as clipboard copy and paste actions and printing of web pages and files via web browsers.

Starting with Chrome version 68 and above, Google intermittently shows a one-time notification when a 3rd party code (dll) is injected into Chrome. McAfee DLP injects several dlls into Chrome browser to protect, printing, clipboard and application file access by Chrome, the code injection may trigger the Chrome notification as in the following image:



This document provides information about how to disable all McAfee DLP code injection into Chrome.

Note: Even after disabling the code injection into Chrome the McAfee DLP Endpoint will still be able to monitor and report on file or text web uploads through the Chrome browser using the McAfee DLP Chrome extension.
Disabling code injection will disable the ability of DLP to detect Printing and Clipboard activities in Chrome.

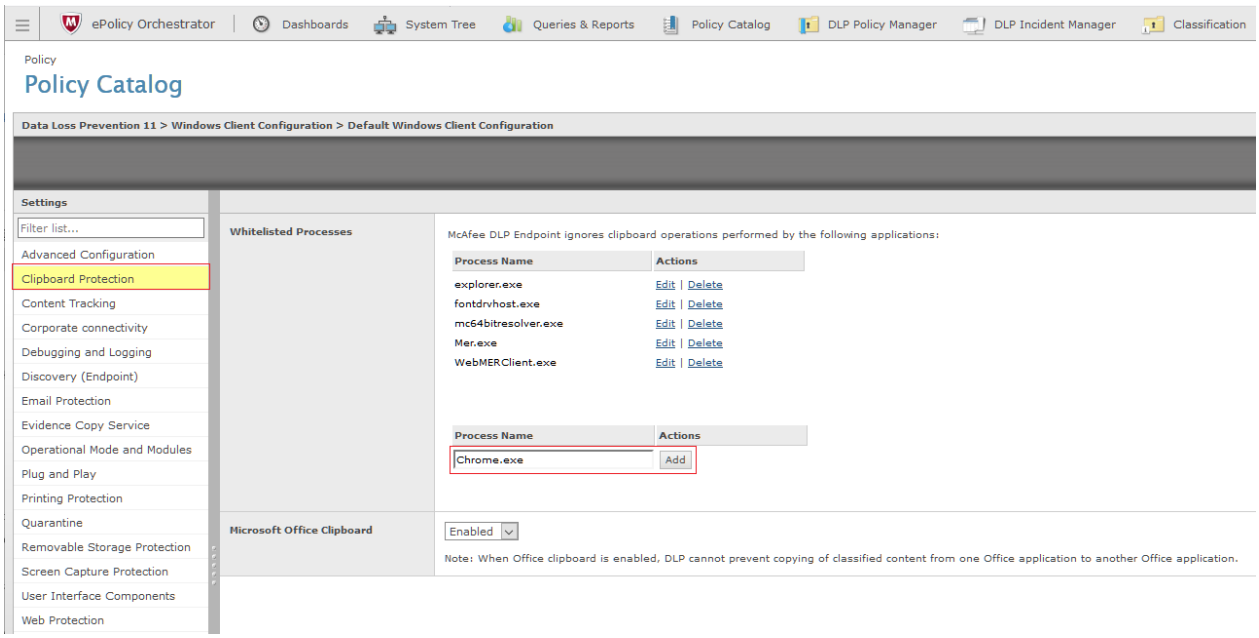
For more information about the upcoming changes in Google Chrome browsers, please refer the following link: https://blog.chromium.org/2017/11/reducing-chrome-crashescaused-by-third.html

Steps to disable all McAfee DLP code injection:

On ePO **Policy Catalog** Open DLP's **Windows Client Configuration**

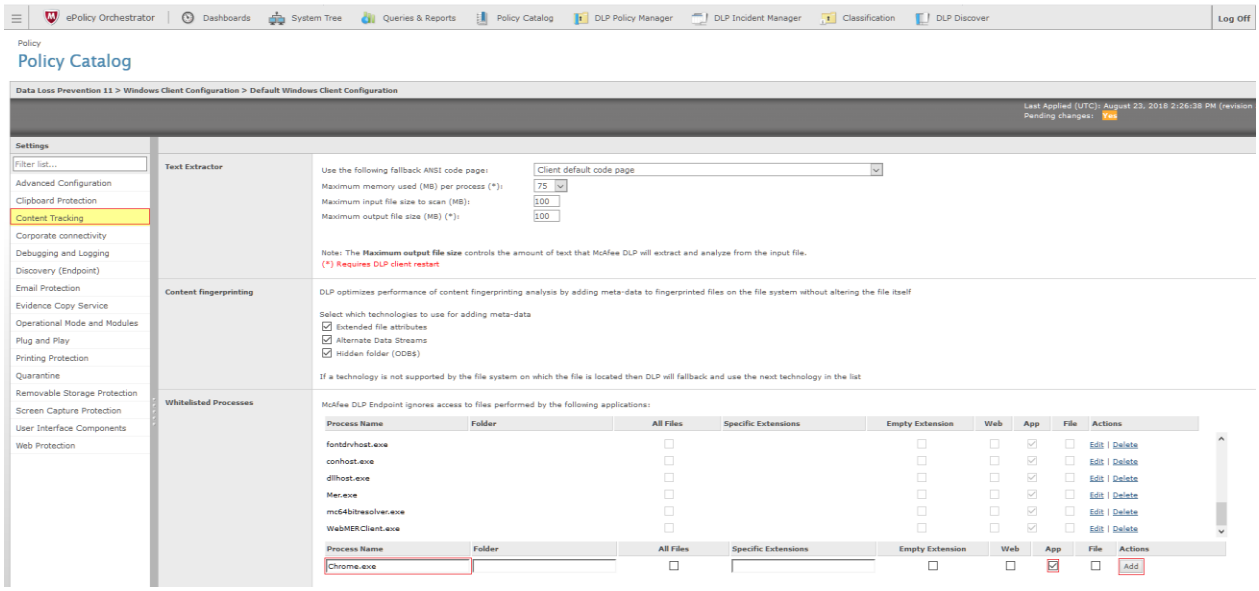
Clipboard

1. Select **Clipboard Protection** on the left
2. Type *Chrome.exe* on the **Whitelisted Processes** and click **Add**



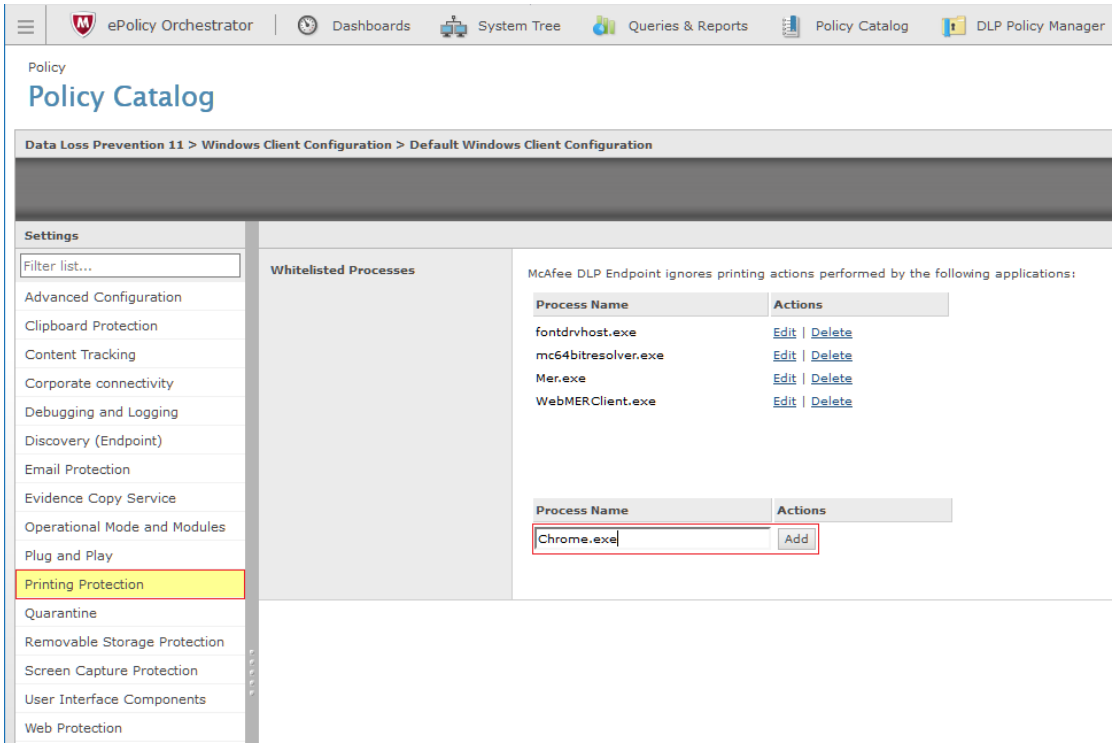
Application File Access

1. Select **Content Tracking** on the left
2. On **Whitelisted Processes** Type *Chrome.exe*, check the **App** checkbox and click **Add**



Printing Protection

1. Select **Printing Protection** on the left
2. Type *Chrome.exe* on the **Whitelisted Processes** and click **Add**



Chrome Web Handler

1. Select **Operational Mode and Modules** on the left
2. On the **Data Protection Modules** remove the check from the **Chrome Web Handler** checkbox