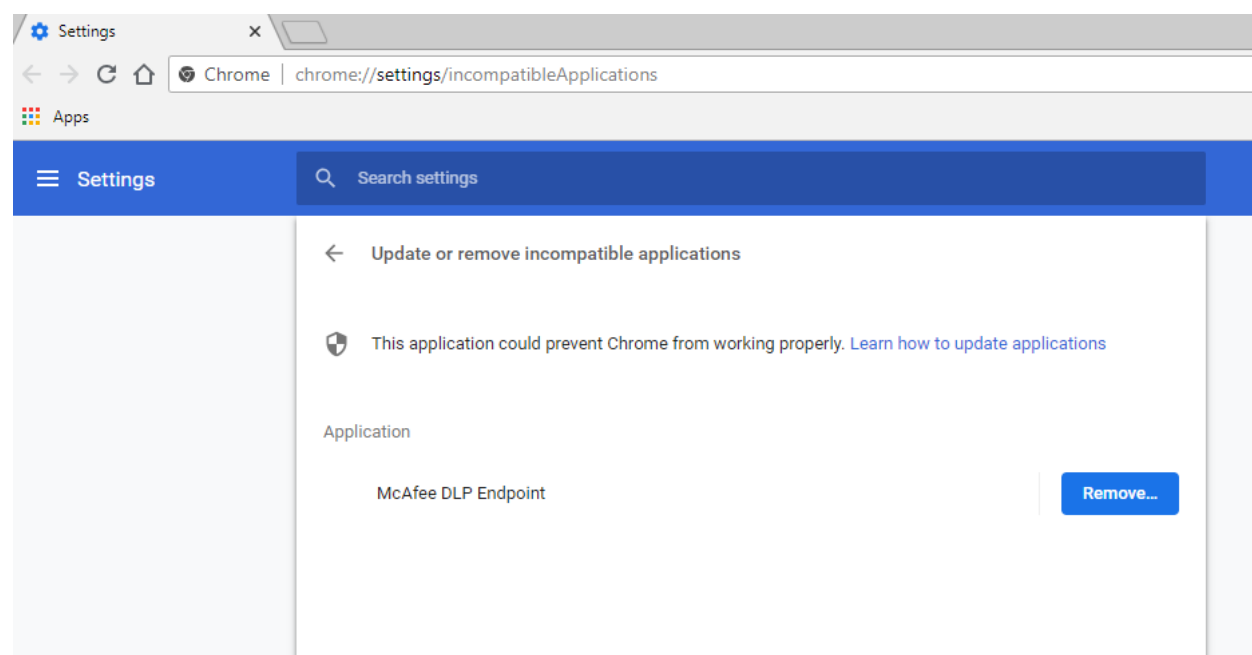


McAfee Data Loss Prevention and Google Chrome

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.

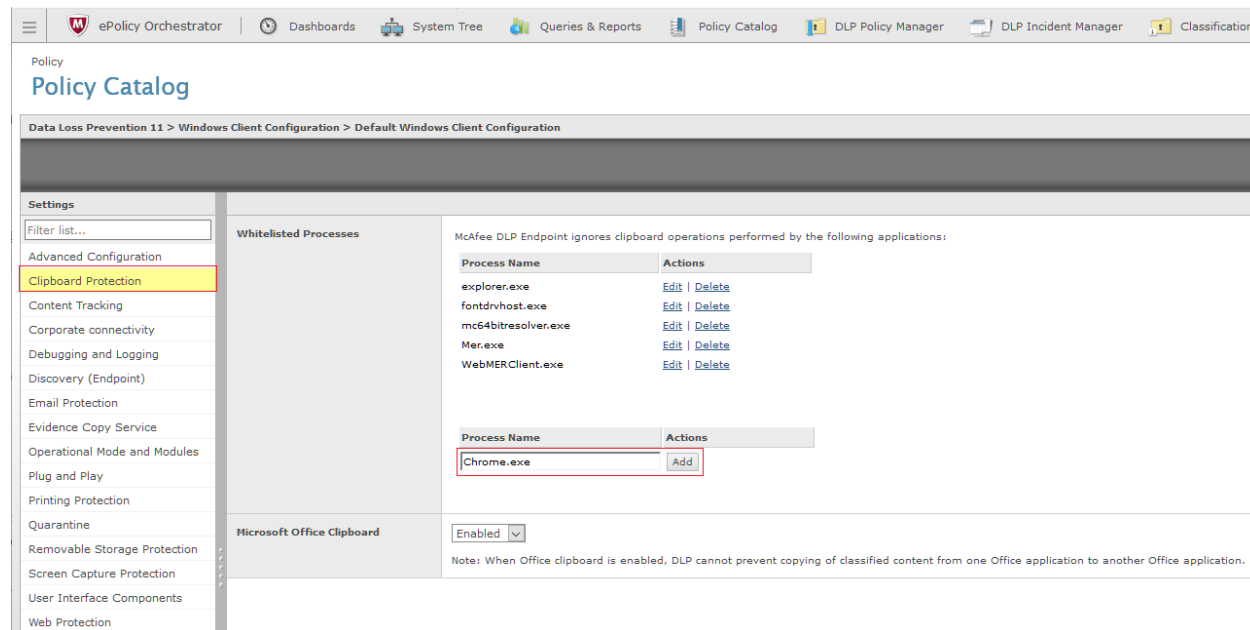
For more information about the upcoming changes in Google Chrome browsers, please refer the following link: <https://blog.chromium.org/2017/11/reducing-chrome-crashescaused-by-third.html>

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**



The screenshot shows the McAfee ePolicy Orchestrator interface. The left sidebar is expanded to 'Clipboard Protection'. The main content area is titled 'Data Loss Prevention 11 > Windows Client Configuration > Default Windows Client Configuration'. Under 'Whitelisted Processes', there is a table of processes that the McAfee DLP Endpoint ignores clipboard operations performed by. The table lists several processes with 'Edit' and 'Delete' links. Below this table, there is an input field for 'Process Name' containing 'Chrome.exe' and an 'Add' button. Below that, there is a section for 'Microsoft Office Clipboard' which is currently set to 'Enabled'.

Process Name	Actions
explorer.exe	Edit Delete
fontdrvhost.exe	Edit Delete
mc64bitresolver.exe	Edit Delete
Mer.exe	Edit Delete
WebMERCClient.exe	Edit Delete

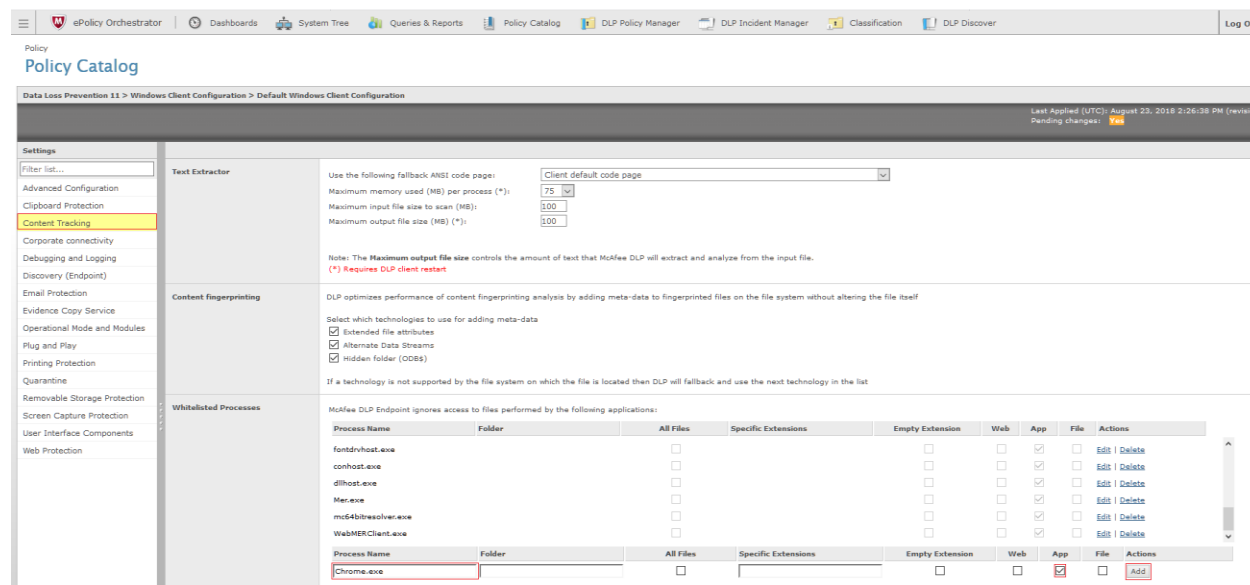
Process Name	Actions
Chrome.exe	Add

Microsoft Office Clipboard: Enabled

Note: When Office clipboard is enabled, DLP cannot prevent copying of classified content from one Office application to another Office application.

Application File Access

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

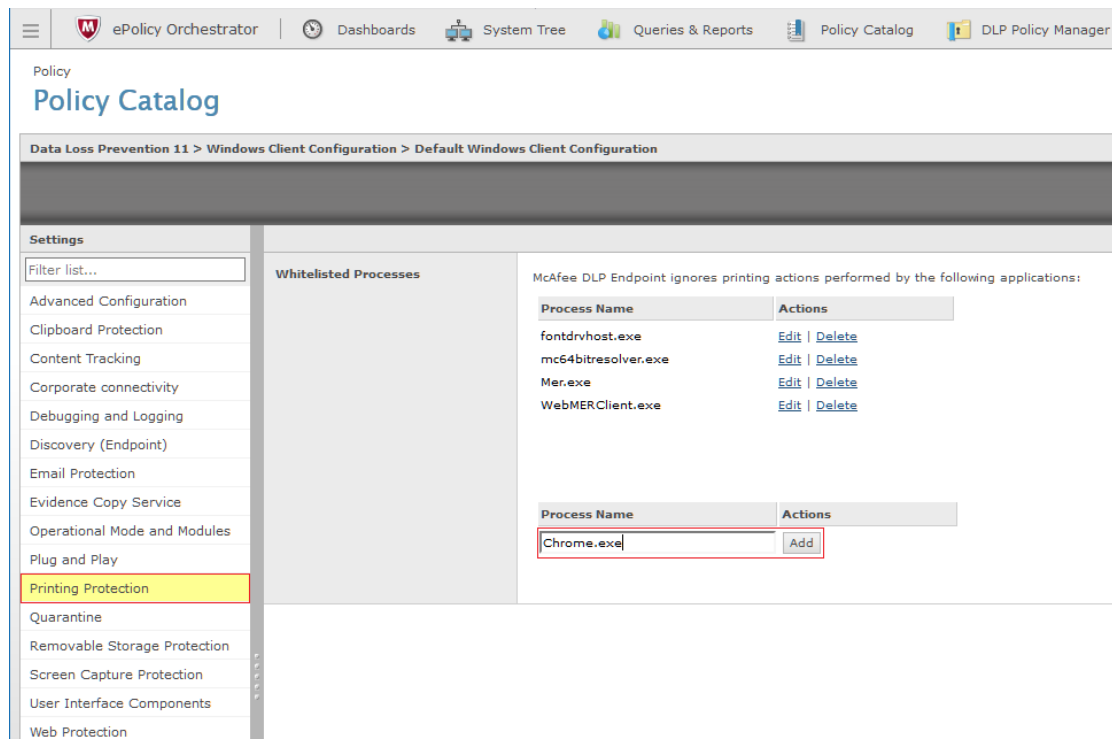


The screenshot shows the McAfee ePolicy Orchestrator interface. The left sidebar is expanded to 'Content Tracking'. The main content area is titled 'Data Loss Prevention 11 > Windows Client Configuration > Default Windows Client Configuration'. Under 'Whitelisted Processes', there is a table of processes that the McAfee DLP Endpoint ignores access to files performed by. The table has columns for Process Name, Folder, All Files, Specific Extensions, Empty Extension, Web, App, File, and Actions. The 'App' checkbox is checked for 'Chrome.exe'. Below this table, there is an input field for 'Process Name' containing 'Chrome.exe' and an 'Add' button.

Process Name	Folder	All Files	Specific Extensions	Empty Extension	Web	App	File	Actions
fontdrvhost.exe		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
conhost.exe		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
dllhost.exe		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
Mer.exe		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
ms64bitresolver.exe		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
WebMERCClient.exe		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
Chrome.exe		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Add

Printing Protection

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



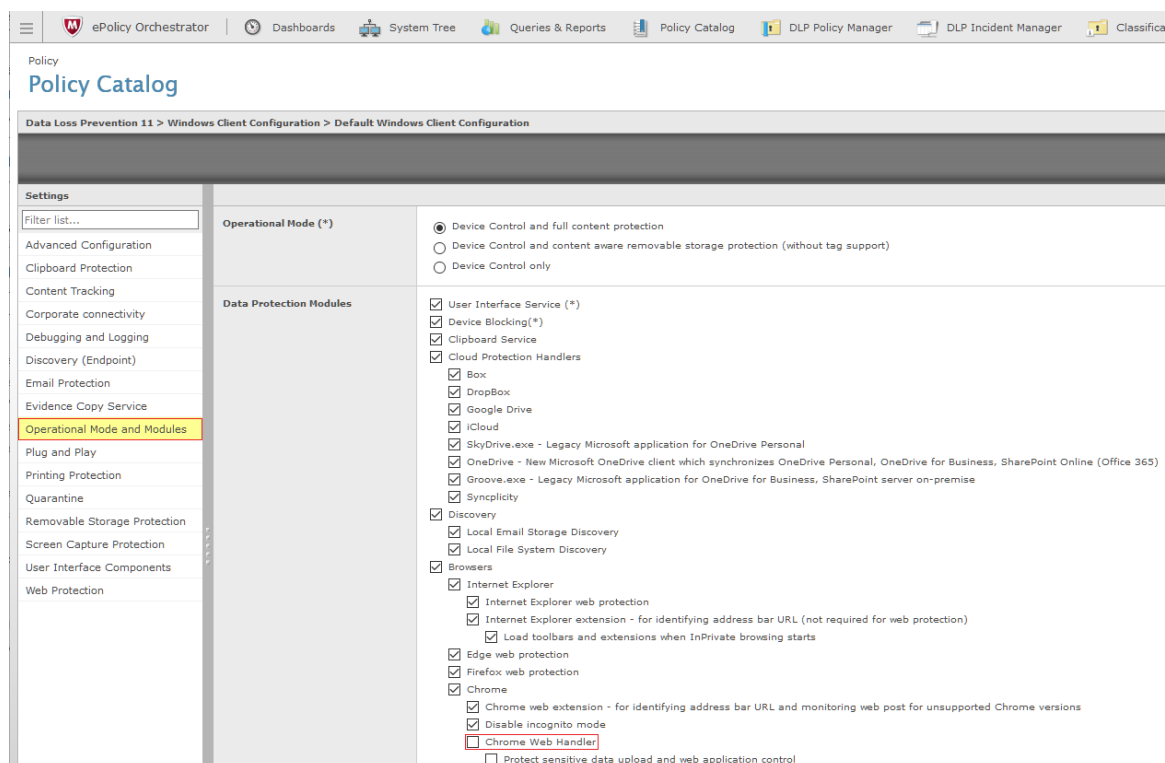
The screenshot shows the McAfee ePolicy Orchestrator interface. The top navigation bar includes 'ePolicy Orchestrator', 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', and 'DLP Policy Manager'. The main content area is titled 'Policy Catalog' and shows a breadcrumb path: 'Data Loss Prevention 11 > Windows Client Configuration > Default Windows Client Configuration'. On the left, a 'Settings' sidebar lists various protection modules, with 'Printing Protection' highlighted in yellow. The main area is divided into two sections: 'Whitelisted Processes' and 'McAfee DLP Endpoint ignores printing actions performed by the following applications:'. The 'Whitelisted Processes' section is currently empty. The second section contains a table with the following data:

Process Name	Actions
fontdrvhost.exe	Edit Delete
mc64bitresolver.exe	Edit Delete
Mer.exe	Edit Delete
WebMERClient.exe	Edit Delete

Below this table, there is an input field containing 'Chrome.exe' and an 'Add' button, both highlighted with a red border.

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



The screenshot shows the McAfee ePolicy Orchestrator interface. The top navigation bar includes 'ePolicy Orchestrator', 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', 'DLP Policy Manager', 'DLP Incident Manager', and 'Classification'. The main content area is titled 'Policy Catalog' and shows a breadcrumb path: 'Data Loss Prevention 11 > Windows Client Configuration > Default Windows Client Configuration'. On the left, a 'Settings' sidebar lists various protection modules, with 'Operational Mode and Modules' highlighted in yellow. The main area is divided into two sections: 'Operational Mode (*)' and 'Data Protection Modules'. The 'Operational Mode (*)' section has three radio button options: 'Device Control and full content protection' (selected), 'Device Control and content aware removable storage protection (without tag support)', and 'Device Control only'. The 'Data Protection Modules' section has a list of checkboxes, with 'Chrome Web Handler' unchecked and highlighted with a red border. Other checked items include 'User Interface Service (*)', 'Device Blocking(*)', 'Clipboard Service', 'Cloud Protection Handlers', 'Box', 'DropBox', 'Google Drive', 'iCloud', 'SkyDrive.exe - Legacy Microsoft application for OneDrive Personal', 'OneDrive - New Microsoft OneDrive client which synchronizes OneDrive Personal, OneDrive for Business, SharePoint Online (Office 365)', 'Groove.exe - Legacy Microsoft application for OneDrive for Business, SharePoint server on-premise', 'Synclivity', 'Discovery', 'Local Email Storage Discovery', 'Local File System Discovery', 'Browsers', 'Internet Explorer', 'Internet Explorer web protection', 'Internet Explorer extension - for identifying address bar URL (not required for web protection)', 'Load toolbars and extensions when InPrivate browsing starts', 'Edge web protection', 'Firefox web protection', 'Chrome', 'Chrome web extension - for identifying address bar URL and monitoring web post for unsupported Chrome versions', and 'Disable incognito mode'. The 'Protect sensitive data upload and web application control' checkbox is also present but unchecked.