McAfee

TM

Together is power.

McAfee Application Control and McAfee Change Control 8.3.x - Windows Release Notes

Contents

What's new in the 8.3.0 release

The current release of the product includes these enhancements and changes.

Release details

For release date and build number details of McAfee® Application Control and McAfee® Change Control 8.3.0, see KB87944.

Updated platform, environment, or operating system support

This release is available on Microsoft Windows 7, Windows Server 2008 R2, and subsequent platforms including Windows Server 2019 and Windows 10. This release is unavailable on the Microsoft Windows Vista platform or earlier. For more information, see KB87944.

McAfee ePO versions support

This release supports McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.3.0-5.3.3, 5.9.0, 5.9.1, and 5.10.

McAfee Agent versions support

This release supports McAfee® Agent 5.0.3 or later. Installation or upgrade of McAfee Application Control and McAfee Change Control client on earlier versions of McAfee Agent fails.

Important: You need to install McAfee Agent product update MsgBusCertsUpdater.zip if using McAfee Agent version earlier than 5.6.3.

Upgrade support

This release supports upgrading from:

• Application Control and Change Control extension 6.2.x, 7.0.x, 8.0.x, 8.1.x, and 8.2.x.
• Application Control and Change Control client 6.2.x, 7.0.x, 8.0.x, 8.1.x, and 8.2.x.

Note: To upgrade from 8.1.x on Windows 32-bit, see KB90785.

When you upgrade Solidcore extension, don't make any changes to existing rules and configuration until Solidcore: Migration server task is complete. Also, the migration task can take longer than usual. Depending on the volume of inventory data in your environment, the task can take a few hours or a day to complete. For more information, see KB84651.

If you are upgrading Solidcore extension earlier than 6.2.0, follow this order:

1. Upgrade Solidcore extension to 6.2.0.
2. Upgrade McAfee ePO to 5.3.0-5.3.3.
3. Upgrade Solidcore extension from 6.2.0 to 8.3.x.

Note: We recommend that you upgrade from 6.2.0 to 7.x.x and then to 8.3.x.

New features

Inventory mode — Inventory mode creates the inventory that contains information about the executable files and script files present on the endpoint. The information stored in the inventory includes complete file name, file size, SHA-1, SHA-256, file reputation, file type, embedded application name, certificate details, and version. This mode tracks and records each change. Also, it dynamically updates the inventory to make sure that the changed or added binaries and files are in the inventory.

Common Platform Enumeration (CPE) — Common Platform Enumeration (CPE) matches applications in the Application Control inventory with applications registered on the CPE official dictionary or Custom CPE dictionary, using different matching methods.

Trusted local group — Trusted local group provides an option to add local groups in the trust model. Application Control supports trusted users. You can add users as updaters to allow them to perform installations or update operations on a protected system. While adding the user information, you can also provide the domain details.

Additional information

For information about installing or upgrading McAfee Application Control and McAfee Change Control, see *McAfee Application Control and McAfee Change Control Installation Guide*

Note: Make sure to restart the system after a product upgrade. This action is specific to product upgrade on the client system.

Updater rules for standalone systems

In the standalone environment, if you are upgrading the product to Solidcore 8.3.0, make sure the latest certificates are available in the repository. For information about new code-signing certificate, see KB91662.

Before installing or upgrading to Application Control and Change Control 8.3.0, add the following updater rules to install Windows Update patches successfully:

Note: These changes are applicable to Application Control and Change Control standalone systems only and needs to be added manually. In managed systems, Application Control and Change Control extensions are updated automatically.

- **Windowsupdatebox**
    - ◦ Filename: windowsupdatebox.exe
    - ◦ Label: Win_Up_Start19
    - ◦ Parent: setuphost.exe

- **Setupplatform**
    - ◦ Filename: setupplatform.exe
    - ◦ Label: Win_Up_Start20
    - ◦ Parent: windeploy.exe

- **SearchUI**
    - ◦ Filename: searchUI.exe
    - ◦ Label: Cortana
    - ◦ Parent: svchost.exe

- **Onedrivestandaloneupdater**
    - ◦ Filename: onedrivestandaloneupdater.exe
    - ◦ Label: OneDrive
    - ◦ Parent: svchost.exe

- **Msdt**
    - ◦ Filename: msdt.exe
    - ◦ Label: Win_Up_Troubleshooter
    - ◦ Inherence: disable

Remove the following updater rule:

- skiplist -I \windows\winsxs\temp

Also, add the exclusion rule ignoring the following path:

- \windows\servicing\packages
- \windows\cbstemp

For more information, see KB91257 and KB86551.

Resolved issues in the 8.3.0 release

This release resolves known issues.

For a list of current known issues, see KB87839 for McAfee Application Control and KB87838 for McAfee Change Control.

Solidcore client

Reference	Resolution
MACC-8406	Files operations on the winsxs\temp folder are now tracked and files are solidified when an updater process renames a binary file from that location.
MACC-8380	The CLI authentication to modify Application Control service private memory is no longer bypassed using the PowerShell script.
MACC-8479	Paged pool memory use is now optimized.
MACC-8396	Bug check E3 no longer happens after upgrading to Solidcore 8.3.0 or later.
MACC-8419 and MACC-8743	The system no longer crashes after upgrading to Solidcore 8.3.0 or later.
MACC-7386	Renaming of the folder containing solidified script files is now blocked.
MACC-8742	The CCT events are now generated when a shared directory's file is modified from the remote system.
MACC-8487	The SC: Enable system no longer crashes when accessing Control Panel.
MACC-6651	The Solidcore client no longer hangs when it upgrades on Microsoft Windows 7.
MACC-8711	Client systems are now displayed on the Real-Time Search page of McAfee® MVISION Endpoint Detection and Response workspace when Solidcore is in the enable mode.

Solidcore extension

Reference	Resolution
MACC-8745	The Japanese translation for SC: Enable Client Task is now corrected.
MACC-8744	The correct list of Unknown Applications is now displayed on the Inventory page.

COPYRIGHT

McAfee™

Together is power.