Release Notes
McAfee® Change Control®
Version 5.1.2

About this release

Thank you for using McAfee® Change Control® software version 5.1.2. This document contains important information about this release. We strongly recommend that you read the entire document.

Purpose

This document details features and fixes included in Change Control 5.1.2 release.

This release contains a variety of improvements. We have spent a significant amount of time finding, fixing, and testing the fixes in this release. Please review the Resolved Issues and Known Issues sections for additional information on the individual issues.

Installation instructions

System requirements

Change Control 5.1.2 is supported only on ePO versions 4.5 and 4.6. Refer to the *McAfee Solidcore 5.1.0 Installation Guide* for system requirements.

Upgrade the Solidcore Extension

This release supports upgrade from Solidcore Extension versions 5.0.0, 5.0.1, 5.0.2, 5.1.0, and 5.1.1.

The process used to upgrade the Solidcore Extension from the supported versions is the same as the first-time installation process. The new product software overwrites the existing copy with the new software. Refer to the *McAfee Solidcore 5.1.0 Installation Guide* for details. If you are upgrading from the 5.0.2 or earlier release, verify that the **Solidcore: Migration** server task is listed in the Server Task Log after the upgrade is complete. Ensure that this task is completed successfully. If the task fails, refer to the *McAfee Solidcore 5.1.0 Installation Guide* for details on how to run the task.

NOTE: Any previously configured Solidcore Policies and Tasks are saved, and will continue to function with the newer software version.

Upgrade the Solidcore Agent

This release supports upgrade from Solidcore Agent versions 5.0.0, 5.0.1, 5.0.2, 5.1.0, and 5.1.1. You can choose to upgrade in update or disabled mode. We recommend that you upgrade using the update mode. Use the disabled mode only if your system in currently in disabled mode.

Update mode	Complete the following steps to upgrade in **update** mode. 1. Add the 5.1.2-<version> package (SOLIDCOR512-<version_platform>.zip) to the ePO repository. 2. Create a SC: Begin Update Mode (Solidcore 5.1.2) client task to put the application into update mode. 3. Create the Product Deployment client task for ePO 4.5 or 4.6. Select the Install action. **Note:** On all Unix platforms, if you are using McAfee Agent 4.5 (earlier than patch 1), restart the cma service after installation, uninstallation, and upgradation. 4. Create the SC: End Update Mode (Solidcore 5.1.2) client task after the update completes. 5. Reboot the Solidcore Agent host, by creating an SC: Run Commands (Solidcore 5.1.2) client task and enter the command: ssreboot -t 300 -m "Rebooting machine as part of upgrade process for McAfee Solidifier".
Disabled mode	Complete the following steps to upgrade in **disabled** mode. 1. Add the 5.1.2-<version> package (SOLIDCOR512-<version_platform>.zip) to the ePO repository. 2. Create a SC: Disable (Solidcore 5.1.2) client task to put the application into disabled mode. Select Force Reboot with the Task to restart the client system. 3. Create the Product Deployment client task for ePO 4.5 or 4.6. Select the Install action. **Note:** On all Unix platforms, if you are using McAfee Agent 4.5 (earlier than patch 1), restart the cma service after installation, uninstallation, and upgradation. 4. Run the sadmin enable command through the SC: Run commands client task. 5. Reboot the Solidcore Agent host, by creating an SC: Run Commands (Solidcore 5.1.2) client task and enter the command: ssreboot -t 300 -m "Rebooting machine as part of upgrade process for McAfee Solidifier".

New features

Here is a list of new and updated features included with this release of the product.

Solidcore Extension

Support for BMC Remedy 7.5 and 7.6

You can now integrate the McAfee Change Control product with BMC® Remedy® Action Request System® versions 7.5 and 7.6. For detailed instructions, refer to the *McAfee Solidcore Change Reconciliation and Ticket-based Enforcement Guide*.

Change reconciliation

The Change Reconciliation feature helps you create a comprehensive list of the changes carried out on all monitored systems and correlate events with change tickets that a change management system (CMS) generates. Starting with the 5.1.2 release, you do not need Analytics Server to use change reconciliation feature. For detailed instructions, refer to the *McAfee Solidcore Change Reconciliation and Ticket-based Enforcement Guide*.

Ticket-based enforcement

Using ticket-based enforcement, you can ensure seamless system updates without any manual intervention. For detailed instructions, refer to the *McAfee Solidcore Change Reconciliation and Ticket-based Enforcement Guide*.

Solidcore Agent

Support for SLES 11 and SLED 11 platforms

Change Control and Integrity Control are now available on the following platforms:

- SUSE Linux Enterprise Server 11 (32- and 64-bit)
- SUSE Linux Enterprise Desktop 11 (32- and 64-bit)

Ensure that you use McAfee Agent version 4.0 or later.

Kernel support

Various new kernels are supported with the 5.1.2 release. Review the Platform Support Matrix for a list of all the supported kernels.

Resolved issues

Solidcore Extension

- Solidcore Purge task for Inventory does not show correct options to purge and the radio buttons do not work for more than one action. (637558)
- When using the Solidcore: Purge action in a server task for the Inventory feature, correct options are not displayed on the wizard. Also, if you add more than one action to a server task, the displayed radio buttons available do not work. (3-1311634885)
- Currently, we cannot define user authorization for the Menu | Configuration | Solidcore page. (637560)
- An error message is displayed when specifying any of the following properties as a label for all chart types (except Table) for a new Managed Systems (under System Management) query. (647339)
  - Local CLI Access
  - Reason for Non Compliance
  - Solidcore Status
  - Status After Reboot
  - License Type

Solidcore Agent

Unix (all versions)	• Pattern matching with rules containing '*' does not work for overlapping rules on the Solaris, Linux, HPUX, and AIX platforms. (602865) • On the Solaris, Linux, HPUX, and AIX platforms, the output of 'sadmin help-advanced' command does not show 'sadmin attr' command in its listing. (603699)
Linux	• (SLES11 SP1) Attribute modifications done via 'chattr' command on a write-protected file are not prevented. (610318) • On the Red Hat Enterprise Linux ES Release 3 platform, no default filters are available in the Minimal System Monitoring for Linux variants (McAfee Default) policy in ePO. (649223) • On the OpenSUSE 11.1 platform, the default policy rules are not applied when you run the Enable client task to apply the Integrity Monitoring license on the end points. (649871) • On the Red Hat Enterprise Linux 5 platform (64-bit), the system performance deteriorates (load shoots up to 1.0 on servers) after the Solidcore Agent is installed. (3-1379209524)
Solaris	• After the Solaris operating system is deployed and PID MAX parameter is set to a value of 32768 or higher, the Solidcore Agent service does not start. (3-1297960551)
AIX	• (AIX 6.1) Solidcore Agent is not supported on Power6 processor with storage key protection enabled. (608981) • On the AIX operating system, the permissions for the /var/log/solidcore directory were set incorrectly, an additional directory was created in the /var/log/solidcore/s3 directory, and the ownership of the rc.scsrvc file was set incorrectly. (3-1289501051)
Windows	• If 'SC:Enable' task to enable 'Integrity Monitor and Change Control' license is applied via ePO and ' Application Control' license is already applied on the end point, the task starts solidification on the end point. (609241) • After Change Control is installed and enabled on a system with an existing VirusScan Enterprise 8.8 installation, the system becomes unresponsive. (3-1435880581, 3-1416897611) • By default, the drvinst.exe file was added to the write-protect list. (666794) • The CLI on the endpoint does not allow you to run any other commands after you issue the config export <filename.txt> command from the ePO console (using a Run Command client task). (3-1185130507)
Windows 2008 R2	• The scgetcert utility fails to extract a certificate preventing successful installation of a signed application. (3-1411610001)
Windows 7	• After enabling package control on the Windows 7 platform, Microsoft Office executable files do not open. (3-1393882683)

Known issues

Known issues in this release of Change Control are described below.

Solidcore Extension

- Solidcore extension does not install on ePO if the database back-end is SQL Server 2000. It supports SQL Server 2005. It supports SQL Server 2005 with DB compatibility level of 90 and above. (608556 and 608557)
- Sometimes when you try to upload the Windows Solidcore Agent Deployment Package (~100 MB) to ePO in Microsoft Internet Explorer, the file upload may time out in case the network upload speed is slow. (608618)
  Workaround: If this error appears in Microsoft Internet Explorer 6, try using Microsoft Internet Explorer 7 or later. In case you encounter the error in Microsoft Internet Explorer 7 or later, copy the Solidcore Agent deployment package to a local directory on the ePO server, open a browser window on the ePO server to access the ePO UI, and upload the file from the local path. This way, upload will happen from the ePO server to ePO and will avoid network delays.
- Reports and dashboard entries are not removed after the Solidcore Extension is uninstalled. (607452)
  Workaround: In case you are uninstalling and reinstalling the Solidcore extension, please remove the report and dashboards manually after uninstalling and before reinstalling.
- PDF reports have minor data display and formatting issues if more than 50,000 records are reported. (607517)
- The Solidcore Policies Applied on Hosts report displays all the policies derived from the root, irrespective of the SKUs enabled on the platform. (608347)
- It is not possible to export data from the Reporting | Solidcore | Events page. (609304)
  Workaround: Use Queries (Reporting | Queries) to export event data.
- If you upgrade from 5.0.0, 5.0.1, 5.0.2, or 5.1.0 to 5.1.1 or higher, existing Solidcore events in the Solidcore Events table are not migrated to the ePO Events table.
- After removing the Solidcore Extension, all Solidcore-related events are retained in the ePO table. When you view the events in the Threat Event log, some fields might display garbage data. (636352)
- Solidcore policies cannot be duplicated by using the Policy Details page because the OK button is disabled. (607554)
- **Workaround**: Use the Policy Catalog page to duplicate policies.
- When using the Guided Configuration page on the ePO 4.6 console, the Save Policy button is not enabled when changes are made to Solidcore Policies. (643854)
- **Workaround**: Edit the policy by using the Policy Catalog without using Guided Configuration.
- When trying to enable an already enabled Solidcore Agent, the error displayed is not translated. (608374)
- The languages Chinese (Simplified), Chinese (Traditional), and Russian were not supported up to McAfee Solidcore extension patch release 5.0.2. Even on performing upgrade from 5.0.2 to 5.1.0, the report names and notes do not get localized. (611750)
- It is not possible to export more than 50,000 records from any table or report. (607908)
- (ePO 4.5) Incorrect message (Monitor Failure) is shown when a user without required permission attempts to access a dashboard. (607963)
- The Configuration page should not allow users to create a group with the name My Rules. (608017)
- Reports, tasks, and policies for all SKUs are listed even if the license for that SKU is not added. (608025)
- The File/Registry Name field in alerts does not accept more than 100 characters. (608151)
- Export of rule groups does not work in Internet Explorer when opened from the ePO Server. (609911)
  Workaround: Use Internet Explorer from a different computer to export rule groups.
- The Server Task pages on ePO might not work properly if you are using Mozilla Firefox version 3.0. (610303)
  Workaround: If you encounter issues, we recommend you use Mozilla Firefox version 3.6 (or higher) or Microsoft Internet Explorer 6.0 (or higher). For more information, see KB70035 in the McAfee Support online KnowledgeBase: https://mysupport.mcafee.com.
- In some cases, using the user name field of reported events on the ePO as a trusted user may not work if the client system is part of an AD domain. This is because the domain name reported in the events is not the full AD domain. (608753)
  Workaround: Use the environment variable USERDNSDOMAIN of AD client as the domain name. Alternatively, review the properties of the My Computer icon to identify the complete user name to specify as the trusted user.
- If ePO is installed on Japanese Windows, exporting the dashboard data to HTML format fails if the generated HTML file name contains digits. (608759)
- Saving a Change Control policy that is a copy of an existing policy with a large number of rules is very slow. (609220)
  Workaround: Because Change Control policies are multi-slot policies, we recommend that you create a new blank policy and add new rules to it instead of copying and modifying an existing policy.
- After a Change Control policy is saved, the yes, no, and none strings are not translated. (608373)
- When viewing an Integrity Monitor policy, the My Rules tab is not translated. (608390)
- The word exclude should be translated in the Integrity Monitor policy for the Windows 32-bit XP filter. (608370)
- If you run reconciliation on a setup with millions of unauthorized changes (for about 5000 hosts), the Systems with Unauthorized changes page does not open. When you select the Systems with Unauthorized changes link on the Reporting | Solidcore | Reconciliation page, the page times out and user is logged off the ePO console. (669563)
- If you install Solidcore Extension 5.1.2 on an existing ePO 4.5 system and then upgrade to ePO version 4.6 FIPS mode, the event parser stops working. (656518)
  Workaround: Execute the following command to upgrade the required DLL:
  https://[ePO IP address:port]/remote/scor.upgradeEventParser.do
- If you are using reconciliation with Solidcore Extension (version 5.1.1 or older) and upgrade to Solidcore Extension 5.1.2, you cannot access the older reconciliation data. (661203)

Solidcore Agent

Unix (all versions)

- If Solidcore Agent is installed on the non-default path, upgrade from ePO is not supported. Such an upgrade may leave Solidcore Agent in an inconsistent state. We recommend that you uninstall the existing version and then install the new version using ePO. (608671)
- If the partition containing the /opt/McAfee/cma directory has insufficient space events may not be generated and the "Failed to generate event xml" error message is added to the solidcore.log file. Free up space in partition containing the /opt/McAfee/cma directory. (608737)
- As per NFS protocol, if a file present on the NFS share is opened once on the NFS client, it cannot be reopened until the file attributes are changed. As a result, if a read-protected file located on an NFS share is opened on the client side in update mode, the user would be able to read it on client even in enable mode (after coming out of the update mode) until the file attributes are changed on the server. (601728)
- Modifying a hard link may cause the name of the link or program to appear in events. (601734)
- The application cannot retrieve information for processes that are invoked before the Solidcore Agent driver is loaded. This has the following implications: (601763)
  - If such a process makes file changes, these changes may not be reported.
  - If such a process executes a new process, the changes made by the new program are reported with full program name.
  - In case of NFS, for the changes done by the client, the change events appearing on the server have only the relative name for the NFS daemon (i.e. nfsd or nfsktcpd).
- For daemon processes, reported user name and original user name are same. (601914)
- A write-protected file can be modified through its hard link if the hard link has already been created. (602653)
- Scripts without '#!' tag cannot act as updaters. (602772)
- For loopback file systems, some features such as updater and monitoring do not work correctly when the loopback path is used instead of physical path in the sadmin commands. For instance, if /opt is mounted as loopback file system at /mnt, to add /mnt/abc as an updater you must add the path /opt/abc as an updater. (602977)
- Some features like updaters and mon-proc-exec do not work properly for unsupported file formats. Only executable binaries and #! scripts are supported file formats. (602990)
- The BOOTING_ENABLED and BOOTING_UPDATE_MODE events are not added to the system log. (603462)
  Workaround: At boot time, start the syslog service before the Solidcore Agent service.
- The following issues are observed when an updater calls another updater: (603490)
  - If the child process is added as an updater, the non-inheritable option (-d) of the parent process is overridden.
  - If the parent process is added as an updater, the non-inheritable option (-d) of the child is overridden.
- For processes that are not directly associated with a terminal, the original_user field is simply a replica of the user field. For example, when you run a script through Runlevel/init scripts, original_user is same as the user. (604780)

- The mmap system call at the nfs client will not work if the file is read-protected. (605062)
- A write-protected file can be modified or deleted if the file system is mounted to a different directory. (606674)
- Adding a script as an updater twice (once on its own and again with its parent) may lead to ambiguous behavior. (607014)
- By default, the deny-read feature is disabled. A read-protect rule is immediately applied to Solidcore Agent but is effective only after the deny-read feature is enabled on the Solidcore Agent. (607024)
- No events are generated for changes to a file containing the string "solidcore.log" in its name, for example, mysolidcore.log. (607245)
- Process information cannot be determined for those processes which are invoked before the Solidcore Agent driver is loaded. This has the following implications: (601763)
  - If such a process makes file changes then these changes may not be reported.
  - For processes that started before the driver was loaded, only the partial program names are reported.
  - In case of NFS, for the changes done by the client, the change events appearing on the server have only the relative name for the NFS daemon (i.e. nfsd or nfsktcpd).
  - No Process Start and Process Stop events are generated for already running processes.
  - On only the AIX platform, Change Tracking / Prevention on file systems mounted by such processes may or may not work as system calls executed by already running processes cannot be trapped due to difference in the way, system calls are implemented under AIX platform. As a workaround, you can restart such processes.
- Write/read protection does not work on files added via cachefs/lofs. (604604)
- If the install path is a mount point, forcibly unmounting [for example, using the umount –f command] may lead to non-deterministic behavior. (613214)
- The Solidcore Agent cannot be installed, upgraded, or uninstalled through init scripts that run at system boot time. (603386)
  Workaround: Add the following two statements in the init script before invoking the installer:
  HOME=""/""
  export HOME
- For a file with multiple hard links, the modification event contains the name of any one of the hard links as the filename. For instance, if the file named 'test' has 'test1' and 'test2' as hard links, the event generated on modifying the file test1 can contain any of the three names (test, test1 or test2) by which the file is known. (613205)
- Due to NFS protocol behavior, a large write request to the NFS client goes to the NFS server in the form of multiple RPC calls and hence multiple FILE_MODIFIED events are generated at the NFS server. (613213)
- If a parent process exits before its child processes, the Solidcore Agent is unable to track the parent process for the running child processes. (605868)
- McAfee Agent 4.6 is not supported with Solidcore Agent 5.1.2. (670210)

Solaris

- The Enable task may fail to enable the product if the 'init 6' command aborts. (607875)
  Workaround: Please reboot the machine manually.
- On Solaris 10, the user name reported for an operation performed in a whole root zone may be incorrect in certain cases. This happens when the global zone contains a user with the same uid as the whole zone user, but with a different user name. (601781)
- In case of an unsupported volume on the Solaris 8 platform, the filename and process name can appear as /? in various events. (605486)
- For files that exist on an unsupported volume or processes that launch from an unsupported volume only the basename (and not the complete path) appears in various events. (605639)
- If you are running Solaris 10 on the AMD64 architecture, the updaters command with -p option may not work correctly if the parent launches the child using system() system call. (606307)
  Workaround: Add the following rule: sadmin updaters add -p <parent> /sbin/sh
- The Solidcore Agent driver (scdrv) may remain loaded even after you have disabled the Solidcore Agent. This can be ignored since it does not affect any operations. (607201)
- The lofs partitions are not displayed in the output of sadmin status command. (603019)
- On modifying a file using echo command, the 'FILE_CREATED' event is also generated along with 'FILE_MODIFIED' event. (602767)
- For the HPUX and Solaris platforms, the Solidcore Agent 5.1.2 is not dual signed. (673267)

Linux

- When you login to a solidified system using telnet as a non-root user, the original_user name appears as root. (602174)
- When a single share is mounted on more than one mount point and a file operation is performed from any of these mount points, the events show the pathname which may refer to any of those shares. (602981)

AIX

- The Parent Process name may be incorrect in events if it cannot be resolved properly. (605295)
- For file truncation operations, only a FILE_MODIFICATION event is generated. This behavior on AIX platform is different from that on other UNIX platforms. (605854)
- For files that exist on an unsupported volume or processes that launch from an unsupported volume only the basename (and not the complete path) appears in various events. (605639)
- For a user in system WPAR with UID that does not exist on the global environment, username cannot be determined. Thus, events for this user are raised with username: UNKNOWN and original user name: UNKNOWN. (605819)
- The Solidcore Agent is not supported in Trusted Execution Environment. (605899)
- When you run the Enable client task from the ePO for the AIX platform, the task is erroneously listed as a failed task on the Client Task Log page. (649574)
  Workaround: The Enable client task runs successfully so you can ignore the task status on the Client Task Log page.
- Files in autofs file-system are reported with "/?" at the beginning. This has following implications: (664439)
  - Events will have "/?" at the beginning of the path.
  - rp/wp won't work on such files.
- If you are using McAfee Agent 4.5 earlier than patch 3 on the AIX 6.1 (64-bit) platform, upgrade via ePO to version McAfee Solidcore version 5.1.1 fails. Complete the following steps to manually upgrade to the 5.1.1 version on AIX 6.1: (649731)
  a) Stop the CMA service (/usr/sbin/cma stop).
  b) Uncompress the SOLIDCOR511-7505_AIX.zip file.
  c) Execute the slibclean command.
  d) Execute mapkg_install.sh (sh mapkg_install.sh) from the output directory of the zip file.
  e) Complete one of the following steps:
    - If upgraded in update mode, restart the system.
    - If upgraded in disabled mode, start the CMA service (/usr/sbin/cma start).

HPUX

- For files that exist on an unsupported volume or processes that launch from an unsupported volume only the basename (and not the complete path) appears in various events. (605639)
- When trying to read an empty read-protected file from the NFS client side, the *Permission denied* message is not generated. However, you are not allowed to read the file. (604822)
- The Solidcore Agent is not recommended to be installed in single-user mode. (608657)
- When you login to a solidified system using telnet as a non-root user, the original_user name appears as root. (602174)
- For processes that run on unsupported file systems, the Process Exit events might not get generated in real time. (606207)
- The User name in the FILE_MODIFICATION event is shown as root when the file is modified through FTP by a non-root user. (606551)
- On modifying a file using echo command, the 'FILE_CREATED' event is also generated along with 'FILE_MODIFIED' event. (602767)
- For the HPUX and Solaris platforms, the Solidcore Agent 5.1.2 is not dual signed. (673267)

Windows (all versions)

- Original Username reported in events is the same as Username. (608418)
- Multiple operating systems on the same machine are not supported. Product features will work only on the operating system it is installed on. (595051)
- Uninstallation fails if the uninstallation process is cancelled midway. (599812)
- Changes done by msiexec.exe in update mode are recorded with workflow ID of UPDATER: msiexec instead of the update mode workflow ID. (600037)
- While opening a write-protected network share in explorer, few deny-write errors are observed. (600805)
- The trusted, solidified, and write-protect features do not work correctly for folder-mounted volumes.
  Workaround: Contact McAfee Support for assistance in case the setup uses folder mounted volumes. (603747)
- Does not support post install script customization during upgrade. It can only be used during fresh installation of the Solidcore Agent. (604153)
- Mapped drive names cannot be used in commands issued by remote users/ePO. (608036)
- You cannot perform upgrades in UI mode for existing 5.0.0 deployments (that were done manually and not via ePO). Use the following methods to upgrade such standalone deployments. (609249)
  (a) UI -> Silent
  (b) Silent -> Silent.
- If the database tables are corrupted, upgrade of the McAfee Solidcore Agent fails and the following error message is displayed:
  ""Database: . Could not load table 'Control' in SQL query: SELECT `Control`,
  `Type`, `X`, `Y`, `Width`, `Height`, `Attributes`, `Property`, `Text`,
  `Control_Next`, `Help` FROM `Control` WHERE `Dialog_`=?"""
  Workaround: Use silent installation instead of UI mode installation.
- When Solidcore Agent installer is run by an agent installer with the /? argument, a series of unwanted dialog boxes appear due to a bug in the third-party packaging software. These dialog boxes can be ignored. (605369)
- Manual uninstallation of Solidcore Agent (deployed from ePO) fails on a client machine having McAfee Agent version 4.0 or lower. (609311)
  Workaround: Contact McAfee Support for assistance in case manual uninstallation has already been tried.
- Registry key protection does not work for all registry key hives, it works only for HKEY_LOCAL_MACHINE. (598002)
- A sub-key registry does not get added to a protected registry key when using the reg command. (599240)
- Creating a shortcut within a read-protected directory is not allowed. (601500)
- Any file operation performed on a read-protected file generates deny-read events corresponding to the file even when the file operation is allowed. (602122)
- Changes done to folder-mounted volumes that do not have any drive letter associated with them cannot be monitored. (603032)
  Workaround: Assign a drive letter to a volume before mounting it on any other folder.
- On 64-bit platforms, ACL modification events are not generated when update mechanism supersedes the deny-write policies for registries. (603628)
- When you attempt to read a read-protected file with certain file flags set through Windows Explorer, read-denied events may not be written to the event viewer. However, the events are logged in the Solidcore Agent log file. (605371)
- Only full long names are supported with commands that accept file or folder names. For example, the write-protect command. Names such as c:\myPackages\SETUP-~1.EXE are not supported. (606496)
- Virtual drive paths are not supported as path values in Solidcore Agent commands, such as write-protect, read-protect, and monitor. (606532)
- The deny-read feature is disabled by default. A read-protect rule is immediately applied to Solidcore Agent but is effective only after the deny-read feature is enabled on the Solidcore Agent. (607024)

Windows 2008 R2 [64 bit]

- During manual installation of McAfee Solidcore Agent on the Windows 2008 R2 (64-bit) platform, the 'Windows installer encountered a validation error' error appears for the msiexec.exe and kernelbase.dll files. (608636)
  Workaround: Click on 'Ignore once' or 'Ignore always' button on the error popup to continue installation.

Windows 2008 [64 bit]

- On the Windows 2008 (64-bit) platform, the rundll32.exe file crashes if an application is uninstalled by using the Add/Remove Programs and initially SetupInstallFromInfSection() function was used to install the application (609780).

Windows NT4

- When you deploy the Solidcore Agent from the ePO console on the Windows NT platform, the application erroneously creates a desktop icon for the Solidcore Agent. (645891)
- On the Windows NT platform, upgrading to the Solidcore Agent 5.1.2 build in Update mode via ePO fails. (656298)
  Workaround: To upgrade successfully, prior to applying the hotfix, apply a policy with rule: "sadmin attr add -bc mcscript_inuse.exe".

Windows XP SP2

- On the Windows XP SP2 platform, deny-write errors with two different filenames or folder names are logged when a file or folder is created under a write-protected folder. (601738)

Windows 2000 and Windows NT4

- On Windows 2000 and Windows NT4, new files are not allowed to be created under a read-protected directory. (600408)

Contacting support

- World Wide Web: http://mysupport.mcafee.com/
- Phone: (408) 988-3832
- Product Updates: https://secure.nai.com/apps/downloads/my_products/login.asp

Finding product documentation

McAfee^{TM} provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

1. Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.
2. Under Self Service, access the type of information you need:

   For user documentation:

   1. Click “Product Documentation.”
   2. Select a “Product,” then select a “Version.”
   3. Select a product document.

   For the KnowledgeBase:

   - Click “Search the KnowledgeBase” for answers to your product questions.
   - Click “Browse the KnowledgeBase” for articles listed by product and version.

Legal notices

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement