McAfee Application and Change Control 6.4.x - Linux Installation Guide
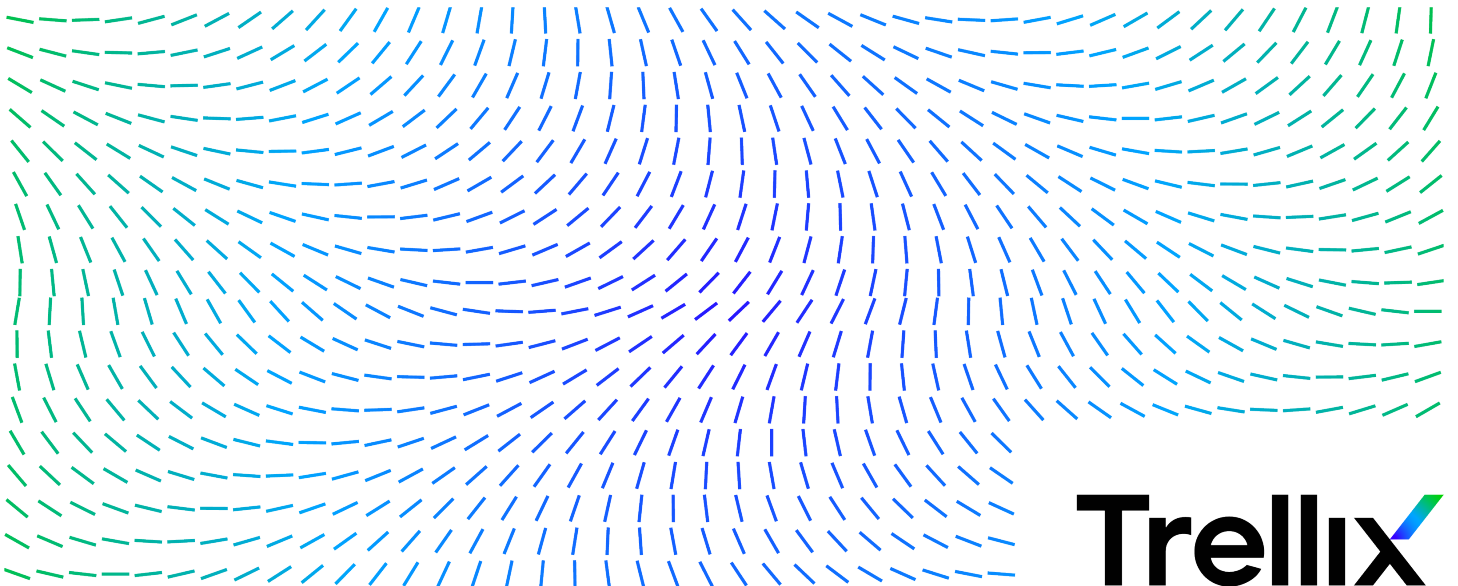
Trellix

Contents

Installation overview

You can install McAfee® Application Control and McAfee® Change Control in a managed McAfee® ePolicy Orchestrator® (McAfee® ePO™) environment or an unmanaged environment.

McAfee ePO is a management tool that installs software and deploys policies on the managed endpoints. It also allows you to monitor client activities, create reports, and store and distribute content and software updates.

Which type of installation do you need?

Determine which type of installation you need to perform: a first-time installation in a new environment or an upgrade to a later version of Application Control and Change Control.

When you install or upgrade the software using McAfee ePO, you can:

- Install it manually.
- Install it using the agent deployment task.

When you install the software in an unmanaged system, the installation is non-interactive with no progress bar or displayed messages

First-time installation workflow

You can install Application Control and Change Control in a managed McAfee ePO environment or an unmanaged environment.

First-time installation (managed)

1. Install the Solidcore extension on McAfee ePO server
2. Add the license key
3. Add Solidcore client package to master repository
4. Install the Solidcore client on the endpoints
5. Verify the installation
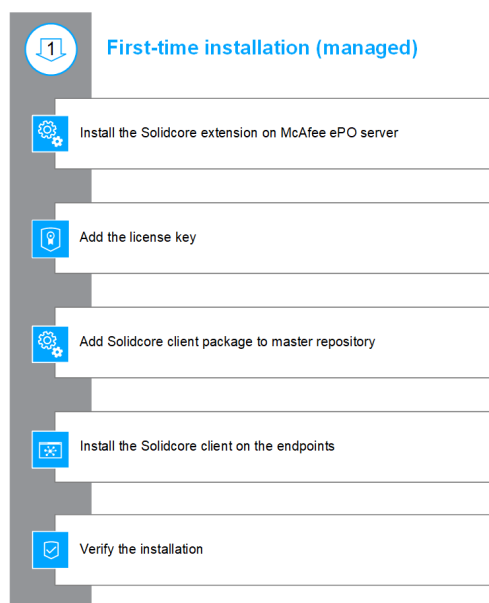
First-time installation (unmanaged)

Download the package

Install the package

Verify the installation

Upgrade installation workflow

You can upgrade Application Control and Change Control in a managed McAfee ePO environment or an unmanaged environment.

Upgrade (managed)

Upgrade the Solidcore extension on the McAfee ePO server

Add the Solidcore client package to the Master Repository

Upgrade the Solidcore client on the endpoints

Verify the upgrade

Upgrade (unmanaged)

Upgrade the software

Verify the upgrade

System requirements

Make sure that your system environment meets all requirements and that you have administrator rights.

ⓘ **Important**

To review system requirements for this release, see KB87944.

For information about how to build Application Control and Change Control on an unsupported kernel, see KB89516.

Before installing or upgrading, verify your environment setup.

Managed

- McAfee ePO server and database are installed and configured.
- McAfee® Agent is installed on each endpoint where you want to install the software.
- Your Linux distribution is supported (see KB87944).
- Your database size is adequate (see KB72753).

Unmanaged

- Your system's kernel is supported (see KB87944).
- Your Linux distribution is supported (see KB87944).

Install software for the first time

Install the software for McAfee ePO management

Install the extension manually on McAfee ePO

The Solidcore extension integrates with the McAfee ePO console and provides Change Control and Application Control features.

Task

1. Download the Solidcore extension package from the McAfee Downloads site.
2. On the McAfee ePO console, select **Menu → Software → Extensions** to open the **Extensions** page.
3. Click **Install Extension**.
4. Browse to and select the Solidcore_epo_extn_<version>.<build>.zip file, then click **OK**.

   📝 **Note**

   > Solidcore extension version 8.x can be used with Solidcore client version 6.x or later.

5. Verify the information about the **Install Extension** page, then click **OK**.
6. Verify that the Solidcore product name appears in the **Extensions** list.

   📝 **Note**

   > If the product name is not listed or you encounter errors during installation, review the Orion.log file in the <McAfee ePO install dir>\Server\Logs directory to analyze the cause.

Install the extension with Software Catalog on McAfee ePO

The Solidcore extension integrates with the McAfee ePO console and provides Change Control and Application Control features.

Task

1. On the McAfee ePO console, select **Menu → Software → Software Catalog**.
2. From the **Products** category list, select **Endpoint Security**.
3. Select **McAfee Application Control 8.x.x** or **McAfee Change Control 8.x.x**
4. Click **Check In** for the **ePO Management Extension 8.x.x**.
5. On the **Check In** page, select **I accept the terms in the license agreement** and click **Check In**.

Add the software license key

Licenses determine the product features that are enabled in your system. Any or all features can be enabled and used at the same time.

Installing the Solidcore extension provides a default evaluation license for **Integrity Control** lasting 90 days. You can extend this evaluation license for another 90 days or add a full license.

Task

1. On the McAfee ePO console, select **Menu → Configuration → Server Settings** to open the **Setting Categories** page.
2. Select **Solidcore**, then click **Edit** to open the **Edit Solidcore** page.
3. Enter the license keys, then click **Save**.

   📝 **Note**

   For information about your license key, see KB90666.

Check in the Solidcore client package to Main Repository

The Solidcore client provides change monitoring, change prevention, and whitelisting features. For all supported platforms, the Solidcore client works on both physical and virtual machines (VM).

Task

1. On the McAfee ePO console, select **Menu → Software → Main Repository**.
2. From the **Packages in Main Repository** page, click **Check In Package**.
3. Set the package type to **Product or Update (.zip)**.
4. Browse to and select the package (.zip) file and click **Next** to open the **Package Options** page.
5. Check and confirm the information.

   • **Package info** — Verify the package details.
   • **Branch** — Select the branch you want. Set to **Current** for new products.
   • **Options** — (Optional) Select **Move the existing package to the Previous branch**.
   • **Package signing** — Indicates if the package is signed by McAfee or if it is a third-party package.
   • **Conflicting Packages that will be removed** — Displays a list of any packages to be deleted.

6. Click **Save** to add the package.

Results

The new package appears in **Packages in Main Repository** list.

Install the Solidcore client with Software Catalog on McAfee ePO

The Solidcore client provides change monitoring, change prevention, and whitelisting features. For all supported platforms, the Solidcore client works well on both physical and virtual machines (VM).

Task

1. On the McAfee ePO console, select **Menu** → **Software** → **Software Catalog**.
2. From the **Products** category list, select **Endpoint Security**.
3. Select **McAfee Application Control 8.x.x** or **McAfee Change Control 8.x.x**.
4. Click **Check In** for the **Solidcore Client for Windows 8.x.x** package.
5. On the **Check In** page, select **I accept the terms in the license agreement** and click **Check In**.

Deploy the Solidcore client to the endpoints

The Solidcore client provides change monitoring, change prevention, and whitelisting features. For all supported platforms, the Solidcore client works on both physical and virtual machines (VM).

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Apply the client task to a group or an endpoint:
    - **Group** — select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
    - **Endpoint** — select the endpoint on the **Systems** page and click **Actions** → **Agent** → **Edit Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select the **McAfee Agent** product and **Product Deployment** task type, then click **Create New Task**.
    a. Specify the task name and add any descriptive information.
    b. Select the target platform.
       For example, when installing the Solidcore client package on the Linux operating system, select **Linux** as the target platform.
5. Specify the component and action.
    - Select the appropriate package from the **Products and components** list.
    - Select the **Install** action.
    - Select the language of the package.
    - Specify the branch where to add the package.
6. Click **Save**, then specify scheduling details.
7. Review and verify the task details, then click **Save**.
8. (Optional) Click **Wake Up Agents** to send your client task to the endpoint immediately.

Verify the Solidcore client installation

You can verify that the software is installed successfully on an endpoint.

Task

1. On the McAfee ePO console, select **Menu → Systems → System Tree**.
2. Select a group or endpoint from the list to view its details in the **Systems** tab.
3. Review logs from the McAfee ePO console.
   a. Select a system on the **Systems** page.
   b. Select **Actions → Agent → Show Agent Log** to view the agent log for the endpoint.
   c. Check the log to verify that the software was successfully installed on the endpoint.
4. Review the properties for the system.
   a. Click **Wake Up Agents** to fetch properties immediately.
      Typically, information is exchanged between the agent and server after an agent-server communication interval (ASCI). The default ASCI value is 60 minutes. You can send an agent wake-up call to make sure immediate communication and data exchange between the server and the agent, without waiting for the ASCI to expire.
   b. Click a system on the **Systems** page to view its details.
   c. Click the **Products** tab and review the **Solidcore** version. Click the row to review additional information, including the product version and installation path.
      If the **Solidcore** information is not listed, check the log files on the endpoint to verify that the software was successfully installed. If the Solidcore client installation fails, the log files provide information about the cause for failure.
      Logs files are located in /var/log/mcafee/solidcore and installation logs in /var/log/mcafee/solidcore/solidcoreS3_install*.log.

Enable the Solidcore client

The Solidcore client must be in Enabled mode to be activated.

Task

1. On the McAfee ePO console, select **Menu → Systems → System Tree**.
2. Apply the client task to a group or an endpoint:
   - **Group** — Select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
   - **Endpoint** — Select the endpoint on the **Systems** page and click **Actions → Agent → Edit Tasks on a Single System**.
3. Click **Actions → New Client Task Assignment** to open the **Client Task Assignment Builder** page.
   a. Select the **Solidcore 8.x.x** product and **SC: Enable** task type, then click **Create New Task**.
   b. On the **Client Task Catalog** page, specify the task name and add any descriptive information.
   c. Select the platform, the subplatform, and indicate whether to enable Change Control, Application Control, or both.

4. Deselect Reboot endpoint checkbox to enable Change Control and Application Control.
5. Click **Save**, then specify scheduling details.
6. Review and verify the task details, then click **Save**.
7. (Optional) Click **Wake Up Agents** to send your client task to the endpoint immediately.
8. Verify that the software is enabled.
    a. Click **Wake Up Agents** to fetch properties immediately.
    b. Click a system on the **Systems** page.
       The details for the selected system are displayed.
    c. Select the **Products** tab and review the **Solidcore** version. Click the row to review the license status.

Install the software in an unmanaged environment

Download the Solidcore client package

The Solidcore client is the software component that provides change monitoring, change prevention, and whitelisting features.

Task

1. Download the package from the McAfee Downloads site.
   The available Solidcore client package for Linux is: SOLIDCOR<version>-<build>_LNX.zip

   📝 **Note**

   In the file name, `<version>` and `<build>` represent the version and build number associated with the product.

2. Save the package file to an accessible location.
3. Open the package file.
   The Solidcore client package file includes the installers for all operating systems.
4. Extract the installer.

Install the software on an unmanaged system

When you install in silent mode on an unmanaged system, no messages are displayed. Instead, a log file captures installation information, including whether the installation was successful. You can review the log file and determine the installation results.

To install the software in silent mode, use the provided command-line options to suppress all interaction and provide parameters for all options.

Task

1. Log on to an unmanaged system as *root super user* (administrator rights).
2. Verify that the required installer is available.

3. Run the installer script:

`./mapkg_install.sh`

4. Add the purchased license:

`sadmin license add xxxx-xxxx-xxxx-xxxx-xxxx`

✏ **Note**

For information about your license key, see KB90666.

5. If the purchased license is for Application Control:
   a. Solidify the system:

   `sadmin so`

   b. Enable the software:

   `sadmin enable`

   c. Restart the Solidcore service:

   `service scsrvc restart`

6. If the purchased license is for Change Control:
   a. Enable the software:

   `sadmin enable`

   b. Restart the Solidcore service:

   `service scsrvc restart`

7. Verify that the Solidcore client is successfully installed and is in Enabled mode:

`sadmin status`

Upgrade to a new software version

Upgrade the software with McAfee ePO

Upgrade Solidcore extension manually

To access the new features in a release, you must upgrade the Solidcore extension.

1. Stop the McAfee ePO Event Parser service.
   a. Select **Control Panel → Administrative Tools → Services**.
   b. Right-click the **McAfee ePolicy Orchestrator <version> Event Parser** service and click **Stop**.
2. Back up these items:

   • McAfee ePO database

   McAfee ePO database includes policies, policy assignments, and rule groups.

   • <McAfee ePO install dir>\Server\extensions\installed\Solidcore directory
   • <McAfee ePO install dir>\Server\conf\Catalina\localhost\SOLIDCORE_META.xml file

3. On the McAfee ePO console, select **Menu → Software → Extensions** to open the **Extensions** page.
4. Click **Install Extension**, browse to, and select the Solidcore_epo_extn_<ver>.<build>.zip file, then click **OK**.
5. Verify the information about the **Install Extension** page, then click **OK**.

What to do next

When you upgrade the solidcore extension, don't make any changes to the existing rules and configuration until the **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. See KB84651 for details.

Upgrade Solidcore extension with Software Catalog

Upgrade the Solidcore extension to access the new features in a release. You can also upgrade the Solidcore extension using Software Catalog.

Task

1. Stop the McAfee ePO Event Parser service.
   a. Select **Control Panel → Administrative Tools → Services**.
   b. Right-click the **McAfee ePolicy Orchestrator <version> Event Parser** service and click **Stop**.

2. Back up these items:

    - McAfee ePO database.

    McAfee ePO database includes policies, policies assignments, and rule groups.

    - \<McAfee ePO install dir>\Server\extensions\installed\Solidcore directory.
    - \<McAfee ePO install dir>\Server\conf\Catalina\localhost\SOLIDCORE_META.xml file.

3. On the McAfee ePO console, select **Menu → Software → Software Catalog**.
4. From the **Products** category list, select **Endpoint Security**.
5. Select **McAfee Application Control 8.x.x** or **McAfee Change Control 8.x.x**.
6. Click **Update** for the **ePO Management Extension 8.x.x**.
7. On the **Update** page, click **Update**.

Verify the Solidcore extension upgrade

Check if the Solidcore extension was upgraded successfully.

Task

1. Check if the Solidcore product name appears in the **Extensions** list.
   If the product name is not listed or you encounter errors during upgrade, review the Orion.log file in the \<McAfee ePO install dir>\Server\Logs directory to analyze the cause of the failure.

   ✎ Note

   > After you upgrade the Solidcore extension, the domain NetBIOS Name is not available for existing users imported directly from an Active Directory to rule groups and policies. To make sure the domain NetBIOS Name is available for such users, delete and reimport users from the Active Directory. After the upgrade, any users that you import from the Active Directory and add to new or existing rule groups and policies automatically include the domain NetBIOS Name.

2. Start the McAfee ePO Event Parser service.
   a. Select **Control Panel → Administrative Tools → Services**.
   b. Right-click the **McAfee ePolicy Orchestrator \<version> Event Parser** service and click **Start**.
3. Verify that migration of data was successful.
   a. On the McAfee ePO console, select **Menu → Automation → Server Task Log**.
   b. Check if the **Solidcore: Migration** server task is complete.
      This server task completes upgrade-related activities. If the task is in progress, wait until the task completes. Make sure you do not edit any existing settings while this task is in progress.
   c. If the migration fails, review the Server Task Log, resolve any issues, and run the **Solidcore: Migration** server task manually to complete the migration.
4. (Optional) Run the **Rule Group Sanity Check** server task from the McAfee ePO console to fix the inconsistencies in the rule groups.

This task updates and corrects the Solidcore Rule Group for errors in installers and certificates. This task also issues warnings for trusted groups-related issues.

    a. On the McAfee ePO console, select **Menu → Automation → Server Tasks**.

    b. Click **New Task**to open the **Server Task Builder** wizard.

    c. Type the task name and click **Next**.

    d. Select **Solidcore: Rule Group Sanity Check** from the **Actions** drop-down list, then click **Next**.

    e. Specify the schedule for the task, then click **Next** to open the **Summary** page.

    f. Review the task summary and click **Save**.

    g. Review the logs generated by the server task (on the **Server Task Log** page) to view the warnings, if any.

Add the Solidcore client package to the repository manually

Before you can upgrade, you must add the Solidcore client package to the McAfee ePO Main Repository.

Before you begin

Review KB87944 for information about the supported kernels for the Linux operating system.

Task

1. On the McAfee ePO console, select **Menu → Software → Main Repository** to open the **Packages in Main Repository** page.
2. Click **Check In Package**.
3. Set the package type to **Product or Update (.zip)**.
4. Browse to and select the package (.zip) file, then click **Next** to open the **Package Options** page.
5. Check and confirm the information.

   - **Package info** — Verify the package details.
   - **Branch** — Select the branch you want. Set to **Current** for new products.
   - **Options** — (Optional) Select **Move the existing package to the Previous branch**.
   - **Package signing** — Indicates if the package is signed by McAfee or if it is a third-party package.
   - **Conflicting Packages that will be removed** — Displays a list of any packages to be deleted.

6. Click **Save** to check in the package.

Results

The new package appears in the **Packages in Main Repository** list.

Add the Solidcore client package to the repository with Software Catalog

Before you can upgrade, you must add the Solidcore client package to the McAfee ePO repository. You can add it automatically using Software Catalog.

Before you begin

See KB87944 for information about the supported kernels for the Linux operating system.

Task

1. On the McAfee ePO console, select **Menu → Software → Software Catalog**.
2. From the **Products** category list, select **Endpoint Security**, then select one of the below products:

   - **McAfee Application Control 6.x.x**
   - **McAfee Change Control 6.x.x**

3. Select the package you want to install.
   For McAfee ePO 5.9 or earlier, select the build you want to install under **Components**. Verify the build number under **Available Version** and **Additional Check In Details**.
4. Click **Update** for the **Solidcore Client for Windows 8.x.x** package.
5. On the **Update** page, click **Update**.

Upgrade the Solidcore client on the endpoints

You must upgrade the Solidcore client on the endpoints to access new features available in the recent version.

Before you begin

Place the endpoints in Disable mode or Update mode.

Task

1. On the McAfee ePO console, select **Menu → Systems → System Tree**.
2. Apply the client task to a group or an endpoint:

   - **Group** — Select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
   - **Endpoint** — Select the endpoint on the **Systems** page and click **Actions → Agent → Edit Tasks on a Single System**.

3. Click **Actions → New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select the **McAfee Agent** product, **Product Deployment** task type, then click **Create New Task** to open the **Client Task Catalog** page.
5. Specify the task name, add any descriptive information, select the target platform, then specify the component and action:

   - Select the appropriate package from the **Products and components** list.
   - Select **Install** for the action.
   - Select the language of the package.

- Select the branch you want. Set to **Current** for new products.
6. Click **Save**, then specify scheduling details.
7. Review and verify the task details, then click **Save**.
8. Restart the endpoints.

Verify the Solidcore client upgrade

Once you upgrade the Solidcore client, you can check if it was upgraded successfully on an endpoint.

Task

1. On the McAfee ePO console, select **Menu → Systems → System Tree**.
2. Select a group or endpoint from the list to view its details in the **Systems** tab.
3. Review logs from the McAfee ePO console.
   a. Select an endpoint on the **Systems** page.
   b. Select **Actions → Agent → Show Agent Log** to view the agent log for the endpoint.
   c. Check the log to verify that the software was successfully upgraded on the endpoint.
4. Review the properties for the endpoint.
   a. Click **Wake Up Agents** to fetch properties immediately.
   b. Click an endpoint on the **Systems** page to view its details.
   c. Select the **Products** tab and review the **Solidcore** version. Click the row to review additional information, including the product version and installation path.
   If the **Solidcore** information is not listed or is incorrect, check the log files on the endpoint to verify that the software was successfully upgraded. If the Solidcore client upgrade fails, the log files provide information about the cause for failure.

Upgrade the software in an unmanaged environment

Upgrade the software on an unmanaged system

You can upgrade the software in silent mode on an unmanaged Linux operating system.

Task

1. Log on to an unmanaged system as *root super user* (administrator rights).
2. Verify that the required installer is available.
3. Switch to Update mode:

   `sadmin begin-update`
4. Run this command:

   `./mapkg_install.sh`

5. Restart the system to complete the upgrade.
6. Exit Update mode:

```
sadmin end-update
```

Results

Now the software is back to Enabled mode.

Verify the upgrade on an unmanaged system

You can verify if that software is upgraded successfully on an unmanaged system.

Task

1. Review the log file:

   • If the upgrade is successful, the solidcoreS3_install_<rel>-<build>.log file is created in the /var/log/mcafee/solidcore directory.

   • If the upgrade fails, the solidcoreS3_install.log file is present in the /tmp directory. For error details, review the most-recent bitrock_installer.log or bitrock_installer_<PID>.log file in the /tmp directory.

2. Run this command to verify that the Solidcore product is reported in the package database of the system.

   • For Linux (RedHat, CentOS, Oracle, and SUSE):

   ```
   # rpm -q solidcoreS3 solidcoreS3-kmod
   ```

   These messages are displayed.

   ```
   solidcoreS3-<rel>-<build>
   solidcoreS3-kmod-<rel>-<build>
   ```

   • For Linux (Ubuntu):

   ```
   dpkg -l solidcores3 solidcores3-kmod
   ```

   These messages are displayed.

   ```
   solidcores3         <rel>-<build>    The Trellix Solidifier provides a comprehensive control
   solution for enterprise server systems.
   ```

   ```
   solidcores3-kmod    <rel>-<build>    This package provides the kernel component of Trellix
   Solidifier for Linux.
   ```

Remove the software

Remove the Solidcore client from managed endpoints

You must remove the Solidcore client from the endpoints to uninstall the software.

Task

1. Place the endpoints in Disabled mode.
2. Restart the endpoints.
3. On the McAfee ePO console, select **Menu → Systems → System Tree**.
4. Apply the client task to a group or endpoint:
   - **Group** — Select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
   - **Endpoint** — Select the endpoint on the **Systems** page and click **Actions → Agent → Edit Tasks on a Single System**.
5. Click **Actions → New Client Task Assignment** to open the **Client Task Assignment Builder** page.
6. Select the **McAfee Agent** product, **Product Deployment** task type, and click **Create New Task** to open the **Client Task Catalog** page.
7. Specify the task name, add any descriptive information, select the platform, and specify the components and action:
   - Select the appropriate package from the **Products and components** list, then click **Remove**.
   - Select the language of the package and Set branch to **Current** for new packages.
8. Click **Save**.
9. Specify scheduling details and click **Save**.
10. Verify the Solidcore client removal.
    a. Click **Wake Up Agents** to fetch properties immediately.
       Typically, information is exchanged between the agent and the server after an agent-server communication interval (ASCI). The default ASCI value is 60 minutes. Send an agent wake-up call to verify immediate communication and data exchange between the server and the agent, without waiting for the ASCI to expire.
    b. Click an endpoint on the **Systems** page to view details for the selected endpoint.
    c. Click the **Products** tab and make sure that Solidcore is not listed.

Remove the Solidcore extension from McAfee ePO

You must remove the Solidcore extension from the McAfee ePO server to successfully uninstall the software.

ⓘ **Warning**

If you uninstall the Solidcore extension, the extension is removed from the McAfee ePO server and database with all associated policies and tables.

Task

1. On the McAfee ePO console, select **Menu → Software → Extensions** to open the **Extensions** page.
2. Select **Solidcore** from the **Extensions** list.
3. Click **Remove**.
4. Verify that the Solidcore product name no longer appears in the **Extensions** list.

Results

If the product name is not removed or you encounter errors when you uninstall, review the Orion.log file in the <McAfee ePO install dir>\Server\Logs directory to analyze the cause of the failure.

Remove the Solidcore client package from McAfee ePO

You must remove the Solidcore client package from the McAfee ePO server to successfully uninstall the software.

Task

1. On the McAfee ePO console, select **Menu → Software → Main Repository** to open the **Packages in Main Repository** page.
2. Select **Solidcore Client for Windows**.
3. Click **Actions → Delete Package** to delete **Solidcore Client for Windows** package.
4. Click **OK**.

Uninstall the software from an unmanaged system

You can uninstall the software on a Linux platform.

Task

1. Log on to a terminal as *root super user* (administrator rights).
2. Switch to Disabled mode.
   ```
   sadmin disable
   ```
3. Restart the endpoint to completely disable the Solidcore client.
4. As *root super user*, go to `/usr/local/mcafee/solidcore` and run the `./uninstall` script.
5. Verify that the software is removed from the system.

   • On RHEL, CentOS, SUSE and Oracle systems, run:

   ```
   rpm -qa | grep solidcoreS3
   ```

   • On Ubuntu systems, run:

```
dpkg -l | grep solidcores3
```

Results

If the software was uninstalled successfully, these commands don't show any results.

COPYRIGHT