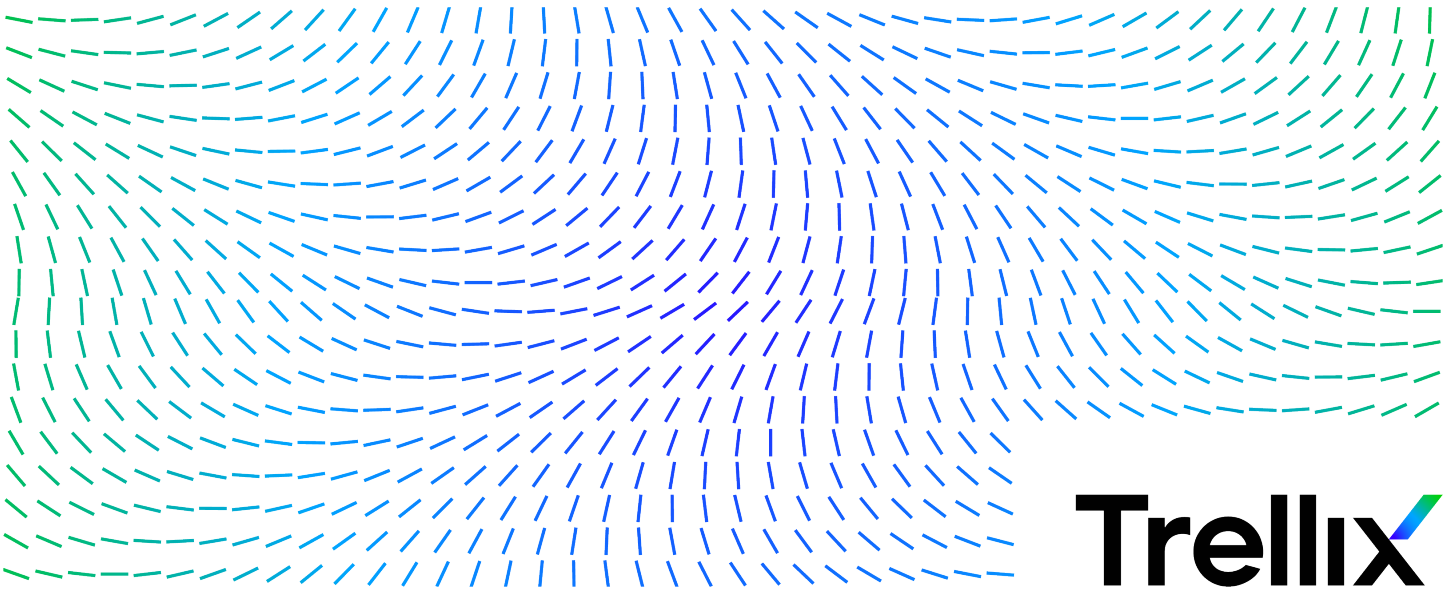
Trellix Policy Auditor 6.5.x Installation Guide



Contents

Introducing Trellix Policy Auditor

Trellix® Policy Auditor automates the process required to conduct system compliance audits. It measures compliance by comparing the actual configuration of a system to the wanted state of a system.

This guide provides system requirements for **Trellix Policy Auditor** software, and information about installing it as a managed product, as well as changing, repairing, removing, and reinstalling the software.

Pre-Installation

Before installing **Trellix Policy Auditor**, you need to make sure your system is ready and meets the minimum system and database storage requirements.

Preparation for installing the software

You must complete these tasks before installing the **Trellix Policy Auditor** software.

1. Get the **Trellix Policy Auditor** software and documentation from the **Trellix** download site.
2. Review the release notes to identify last minute changes or known issues.
3. Verify that you have local administrator rights for the computer where you plan to install **Trellix Policy Auditor**.
4. Verify that your server or workstation meets the system requirements before you start the installation process. Refer to *System requirements* for details.
5. If you are installing a licensed version over an evaluation version of **Trellix Policy Auditor**, you must upgrade the license. The license is not automatically upgraded from an evaluation version.

System requirements

Most of the system requirements for **Trellix Policy Auditor** are the same as **McAfee ePO** system requirements.

The difference for **Trellix Policy Auditor** is the storage requirement for the database. The amount of storage required depends on the amount of data you plan on retaining, how frequently you collect that data, and how long you need to keep that data.

Note

Unless otherwise specified, these are minimum requirements and are not optimal for performance. They apply only to **Trellix Policy Auditor**.

Supported McAfee ePO software versions

One of these versions of **McAfee ePO** software must be installed and working before you can install **Trellix Policy Auditor**.

- **McAfee ePO** software version 5.9
- **McAfee ePO** software version 5.9.1
- **McAfee ePO** software version 5.10

Domain controller requirements

The server must have a trust relationship with the Primary Domain Controller (PDC) on the network. For instructions, see the Microsoft product documentation.

Supported operating systems

Trellix Policy Auditor is installed as an extension of **McAfee ePO** software and runs on operating systems supported by that product.

For the most current information about supported operating systems, see KB51569.

Browsers supported

McAfee ePO runs on the most commonly used browsers and can be accessed from anywhere on the network.

For the most current information about **McAfee ePO** browser, see KB51569.

Proxy servers

If you are using a proxy, bypass the proxy server:

1. From the Internet Explorer **Tools** menu, select **Internet Options**.
2. Select the **Connections** tab and click **LAN Settings**.
3. Select **Use a proxy server for your LAN**, then select **Bypass proxy server for local addresses**.
4. Click **OK**, then click **OK** again.

Ports needed by McAfee ePO for communication through a firewall

McAfee ePO uses ports to communicate with web browsers, SQL Server, managed systems, the network, and other portions of the software.

For the most current information about ports use by **McAfee ePO**, see KB66797.

This table shows the ports needed by **McAfee ePO** for communication through a firewall.

Port	Default	Description	Traffic direction
Agent to server communication port	80	TCP port opened by the **McAfee ePO** server service to receive requests from agents.	Inbound/Outbound connection to/from the **McAfee ePO** server/ Agent Handler.
Agent communicating over SSL (4.5 and later agents only)	443	By default, agents should communicate over SSL (443 by default).	Inbound/Outbound connection to/from the ePO server/Agent Handler.
Agent wake-up communication port	8081	TCP port opened by agents to receive agent wakeup requests	Outbound connection from the **McAfee ePO** server/Agent Handler.

Port	Default	Description	Traffic direction
SuperAgent repository port		from the **McAfee ePO** server. TCP port opened to replicate repository content to a SuperAgent repository.	
Agent broadcast communication port	8082	UDP port opened by SuperAgents to forward messages from the **McAfee ePO** server/ Agent Handler.	Outbound connection from the SuperAgents.
Console-to-application server communication port	8443	HTTPS port opened by the **McAfee ePO** Application Server service to allow web browser UI access.	Inbound connection to the **McAfee ePO** server.
Sensor-to-server communication port	8444	HTTPS port opened by the **McAfee ePO** Application Server service to receive RSD connections. Also, used by the Agent Handler to talk to the **McAfee ePO** server to get required information (like LDAP servers).	Inbound connection to the **McAfee ePO** server. Outbound connection from remote Agent Handlers.
SQL server TCP port	1433	TCP port used to communicate with the SQL server. This port is specified or determined automatically during the setup process.	Outbound connection from the **McAfee ePO** server/Agent Handler.
SQL server UDP port	1434	UDP port used to request the TCP port that the SQL instance	Outbound connection from the **McAfee ePO** server/Agent Handler.

Port	Default	Description	Traffic direction
		hosting the **McAfee ePO** database is using.	
Default LDAP server port	389	LDAP connection to look up computers, users, groups, and Organizational Units for User Based Policies.	Outbound connection from the **McAfee ePO** server/Agent Handler.
Default SSL LDAP server port	646	User Based Policies use the LDAP connection to look up users, groups, and Organizational Units.	Outbound connection from the **McAfee ePO** server/Agent Handler.

Supported virtual infrastructure software

McAfee ePO runs on the most commonly used virtual infrastructure software.

For the most current information about **McAfee ePO** virtual infrastructure support, see KB51569.

Distributed repository requirements

Distributed repositories host copies of your master repository's contents. Consider using distributed repositories and strategically placing them throughout your network to ensure that managed systems are updated and to minimize network traffic.

As you update your master repository, the **McAfee ePO** replicates the contents to the distributed repositories. For more information on distributed repositories, see the **McAfee ePO** product guide. Replication can occur:

- Automatically when specified package types are checked in to the master repository, as long as global updating is enabled.
- On a recurring schedule with replication tasks.
- Manually, by running a Replicate Now task.

Component	Requirement
Free disk space	100 MB on the drive where the repository is stored.

Component	Requirement
Memory	256 MB minimum.

Trellix Agent and McAfee ePO support

Trellix Policy Auditor software supports **Trellix Agent** versions 4.5, 4.6, and 5.0. The available features depend upon the agent version and the **McAfee ePO** software version.

McAfee ePO **server version**	Trellix Agent **version**
5.9	5.5.x, 5.6.x
5.9.1	5.5.x, 5.6.x
5.10	5.5.x, 5.6.x

Trellix Policy Auditor agent platforms and support

The **Trellix Policy Auditor** agent supports many versions of Windows, Linux, and UNIX-based operating systems.

Note

The **Trellix Policy Auditor** agent requires the **Trellix Agent** to be installed on the same system.

For the most current information about supported operating systems, see KB72961.

Hardware and network requirements for Windows systems

These are the minimum requirements for **Trellix Policy Auditor** agent support on Windows systems:

Component	Requirements
Processor	Intel Pentium-class, Celeron, or compatible processor; 166 MHz process or higher
Free disk space for agent	300 MB
Free disk space for other McAfee components	Sufficient disk space on client computers for each McAfee product that you plan to deploy (for

Component	Requirements
	more information, see the corresponding product documentation)
Free memory	20 MB RAM
Network environment	Microsoft or Novell NetWare networks. NetWare networks require TCP/IP
Network interface card (NIC)	10 Mbps or higher

Database considerations and support

Trellix Policy Auditor uses the **McAfee ePO** server database. Before installing **Trellix Policy Auditor**, calculate how much database space you need based on your auditing requirements.

Using Trellix Policy Auditor software with a database

For the most current information about supported SQL database versions, see KB51569.

Database storage requirements

When determining hardware needs for your organization, it is important to estimate the amount of database storage required to use **Trellix Policy Auditor** software.

Trellix has designed the software so that audit results consume the minimum amount of disk space. The amount of database storage you require depends on these factors:

- How frequently benchmark audits are performed
- The number of systems audited
- How long you want to retain audit results

The tables used to calculate server and database requirements are based on tests of the software in the following distributed environment:

Trellix Policy Auditor server

Component	Requirement
CPU	Four-processor, Intel Xeon 2.0 GHz core server
RAM	8 GB

Component	Requirement
Operating system	Windows 2012 Server 64-bit R2
RAID	RAID array 5 hard drive for local storage

Database server

Component	Requirement
CPU	Four-processor, Intel Xeon 2.7 GHz server with hyper threading
RAM	8 GB
Operating system	Windows 2012 Server 64-bit R2
Database software	SQL Server 2012, Service Pack 2 or above
RAID	RAID array 5 hard drive for local storage

Effect of differential auditing results on database size

Trellix Policy Auditor increases database size by an average of 760 KB of space per new system audited. The differential audits feature causes the increase in database size to decrease significantly after the first audit.

The **Index Configuration** server setting also affects the size of the database. If you use the **Minimal Indexing** option, the database will be smaller than if you use one of the other options.

The ultimate database size cannot be calculated accurately prior to deploying **Trellix Policy Auditor**, but can be estimated approximately three months after beginning a phased rollout. Use the database storage sizing estimates to determine the initial database size for new systems and new audits.

Estimate database storage requirements

You can estimate the average amount of hard disk space needed to store new **Trellix** audit results.

Task

1. **Determine the auditing requirements for your organization, including:**
    - The number of audits you will be performing

- The frequency of each audit (for example, 20 audits once per quarter, five audits once per month, or one audit once per week)
- The number of systems covered by each audit

2. **Use the example and the table in *Database storage example and requirements table* to estimate the database space required for each audit.**
3. **Add the values for each audit. The sum is equal to the size of the database that is required to store the audit results for one year.**
4. **Determine the length of time you want to store the audits and adjust the database accordingly. For example, if you intend to store the audit results for two years, double the database size obtained in step 3. If you intend to store the audit results for six months, divide the database size by two.**

Database storage example and requirements table

The requirements table for database sizing can help you calculate the approximate disk space needed for your **Trellix Policy Auditor** database.

Requirements table for database sizing

Use this table to estimate the required size of your database. These estimates are based upon the average size of benchmark audit results. Your needs might vary.

Per system per year		**1,000 systems**	**2,000 systems**	**5,000 systems**	**10,000 systems**	**20,000 systems**	**50,000 systems**
Frequency	**Total audits**	**Database size (GB)**					
1 yearly	1	1	3	7	14	27	68
2 yearly	2	3	5	14	27	55	127
5 yearly	5	7	14	34	68	137	342
10 yearly	10	14	27	68	137	237	684
20 yearly	20	27	55	137	273	547	1,367
1 quarterly	4	5	11	27	55	109	273
2 quarterly	8	11	22	55	109	219	547

Per system per year		1,000 systems	2,000 systems	5,000 systems	10,000 systems	20,000 systems	50,000 systems
Frequency	Total audits	Database size (GB)					
5 quarterly	20	27	55	137	273	547	1,367
10 quarterly	40	55	109	273	547	1,094	2,188
20 quarterly	80	109	219	547	1,094	2,188	5,469
1 monthly	12	16	33	82	164	328	820
2 monthly	24	33	66	164	328	656	1,641
5 monthly	60	82	164	410	820	1,641	4,102
10 monthly	120	164	328	820	1,641	3,281	8,203
20 monthly	240	328	656	1,641	3,281	6,563	16,046
1 weekly	52	71	142	355	711	1,422	3,555
2 weekly	104	142	284	711	1,422	2,844	7,109
5 weekly	260	355	711	1,777	3,555	7,109	17,773
10 weekly	520	711	1,422	3,555	7,109	14,219	35,547

Per system per year		1,000 systems	2,000 systems	5,000 systems	10,000 systems	20,000 systems	50,000 systems
Frequency	Total audits	Database size (GB)					
20 weekly	1040	1,422	2,844	7,109	14,219	28,438	71,094
1 daily	365	499	998	2,495	4,990	9,980	24,951
2 daily	730	998	1,996	4,990	9,980	19,961	49,902

Calculating database storage requirements

A corporation follows this policy for running audits:

- The company retains audit results for one year.
- One audit runs every three days on 2,000 systems. The table does not include this value, so we approximate this to two audits per week running on 2,000 systems.
- Five monthly audits run on 5,000 systems.
- One yearly audit runs on 150,000 systems. The table does not include this value, but it is equivalent to three yearly audits on 50,000 systems.
- Two quarterly audits run on 10,000 systems.

Calculate the approximate database size:

1. Look up the corresponding values in the table under *Requirements table for database sizing*, and note these results:

Audit frequency...	...running on number of systems	=	Database size (GB)
2 weekly audits	2,000 systems		284
5 monthly audits	5,000 systems		410
3 yearly audits	50,000 systems (3 × 68 = 204)		204
2 quarterly audits	10,000 systems		109

2. Calculate the total amount of space needed: **284 + 410 + 204 + 109 = 1,007 GB**

Database storage requirements for File Integrity Monitoring

File Integrity Monitoring (FIM) allows you to designate a set of files to monitor for changes. **Trellix Policy Auditor** software monitors the MD5 and SHA-1 hashes of a file as well as the file attributes and permissions information. When a file changes, the **Trellix Policy Auditor** agent notes the change and sends an event back to the server.

The number of FIM events depends upon the number of files monitored and the frequency of changes to monitored files. The number of events is difficult to predict, but the impact to database storage is minimal.

Each FIM event adds approximately 3 KB to the database. If your organization generates one million events per month, the annual database growth is:

3 KB/event × 1,000,000 events/month × 12 months/year × 0.000001 GB/KB = 36 GB/year

Database storage requirements for file versioning

The File Integrity Monitoring feature of **Trellix Policy Auditor** software allows you to store up to six versions, including the file baseline, of text files from managed systems. The software does not support versioning for non-text files.

Version database sizing chart

This chart helps you calculate the database storage requirements for versioned files. The Monitored file size column is the size of the file, in megabytes, for which you are storing version text. The Versions row is the number of file versions that you are storing.

Versions	**2**	**3**	**4**	**5**	**6**
Monitored file size (MB)	**Database requirement per 1,000 systems (GB)**				
1	0.0573	0.115	0.172	0.229	0.287
2	0.0747	0.149	0/224	0.299	0.374
3	0.0983	0.196	0.294	0.393	0.492
4	0.138	0.276	0.415	0.553	0.691

Calculating versioning database storage requirements

A corporation follows this policy for maintaining file versions:

- Maintains file text for 5 versions of 2 MB files on 200,000 systems.
- Maintains file text for 4 versions of 1 MB files on 20,000 systems.
- Maintains file text for 3 versions of 4 MB files on 140,000 systems.
- Maintains file text for 6 versions of 3 MB files on 100,000 systems.

Calculate the approximate database size:

1. Look up the corresponding values in the table under ***Version database sizing chart***, and note these results:

Versions	Number of systems (thousands)	Monitored file size (MB)	Value from chart	=	Database size (GB)
5	200	(2)	0.299		59.80
4	20	(1)	0.172		3.44
3	140	(4)	0.276		38.64
6	100	(3)	0.492		49.20

2. To determine the database size, multiply the number of systems (in thousands) by the value that you obtained from the ***Version database sizing chart***.
3. Calculate the total amount of space needed: **59.80 + 3.44 + 38.64 + 49.20 = 151 GB**

Installing Trellix Policy Auditor

Installing **Trellix Policy Auditor** includes several components. The installation process also includes updating the **Trellix Policy Auditor** content and installing the **Trellix Policy Auditor** agent.

After you install the **Trellix Policy Auditor** product, update the **Trellix Policy Auditor** content to ensure you have the latest content before you start auditing systems.

The **Trellix Agent** must be installed before you install the **Trellix Policy Auditor** agent. See the **McAfee ePO** product guide for information about installing the **Trellix Agent**.

If you need agents for other operating systems, see Check in additional agent packages.

Install the Trellix Policy Auditor extension

Install the software on **McAfee ePO** as an extension.

Before you begin

You must have local administrator rights for the computer where you plan to install **Trellix Policy Auditor**.

Task

1. **Download the product zip file from the Trellix download site, then uncompress the zip file.**
2. **Select Menu → Software → Extensions.**
3. **Click Install Extension, then click Browse.**
4. **Select the PAPackage.zip file, click Open, then click OK.**
5. **If earlier versions of Trellix Policy Auditor software are installed, a dialog box asks whether you want to perform an upgrade of Trellix Policy Auditor. Click Yes, then click OK.**
6. **Review the Install Package information, then click OK.**
7. **Before rebooting or using Trellix Policy Auditor, update the benchmark and check content.**
   See *Update **Trellix Policy Auditor** content* for instructions.

Results

Trellix Policy Auditor appears in the **Managed Products** list under extensions, and all the extensions installed for the software appear in the right pane.

Update Trellix Policy Auditor content

After installing **Trellix Policy Auditor** on **McAfee ePO**, you must update the content before using the software or rebooting the system.

Note

The content check-in requires about 30 minutes.

Task

1. **Select Menu → Automation → Server Tasks.**
2. **Next to Update Master Repository, click Run.**
    - Do not restart your system or use **Trellix Policy Auditor** or **Trellix** Benchmark Editor while **McAfee ePO** is adding content.
    - Click **Menu → Reporting → Server Task Log** to verify that the new content has been checked in.

Note

In **McAfee ePO**, you can also update the benchmark and editor content using **Schedule Pull**. Go to **Menu → Software → Master Repository**, then clicking **Actions → Schedule Pull** and following the **Server Task Builder** wizard. For more information, see the latest **McAfee ePO** Product Guide.

Check in additional agent packages

When you install **Trellix Policy Auditor**, you need to separately check in agent packages for Windows, Mac OSX, and Linux to the **Master Repository**. Also for Solaris, AIX, or HP-UX systems, you need to separately check in these packages to the **Master Repository**.

For information on deploying the agent to systems in the **System Tree**, refer to ***Install the Trellix Policy Auditor agent*** in the ***Trellix Policy Auditor Product Guide***.

For option definitions, click **?** in the interface.

Task

1. **Download the appropriate agent zip files from the Trellix download site.**
2. **Select Menu → Software → Master Repository, then click Actions → Check In Package.**
3. **For Package type, select Product or Update (.ZIP), browse to and select the package file, then click Open.**
4. **Click Next.**
5. **Confirm or configure the following:**
    - **Package info —** Confirm this is the correct package.
    - **Branch —** Select the branch you want. If there are requirements in your environment to test new packages before deploying them throughout the production environment, **Trellix** recommends using the **Evaluation** branch whenever checking in packages. Once you finish testing the packages, you can move them to the **Current** branch by selecting **Menu → Software → Master Repository**, then click **Change Branch**.
    - **Move the existing package to the Previous branch —** Moves packages in the Master Repository from the **Current** branch to the **Previous** branch when a newer package of the same type is checked in. Available only when you select **Current** in **Branch**.
    - **Package signing —** Specify if the package is signed by **Trellix** or is a third-party package.

- **Conflicting Packages that will be removed** — Displays any conflicting packages. These packages are removed when you check in the selected package.

6. **Click Save, then wait while the package is checked in.**

Results

The new package appears in the **Packages in Master Repository** list on the **Master Repository** tab.

Uninstall Trellix Policy Auditor

You can remove the **Trellix Policy Auditor** program files to re-install another version of the program or to completely remove the program.

Note

If you plan to re-install the software, **Trellix** strongly recommends that you restart your computer after you remove the files.

Task

1. **Select Menu → Software → Extensions, select Trellix Policy Auditor in the Managed Products list.**
2. **In the right pane, click the Remove link of each extension component.**
   It is important to remove the components in the following order:
   - PA Rollup extension
   - **Trellix Policy Auditor** extension
   - Advanced Host Assessment
   - Advanced Host Assessment Content Distributor
   - Findings extension
   - Benchmark Editor Content Distributor extension
   - Benchmark Editor extension
   - PA Core extension
3. **Select Menu → Software → Master Repository.**
4. **In the Actions column of the Audit Engine Content row, click Delete to remove the benchmark and check content.**
5. **To uninstall any remaining Trellix Policy Auditor agent packages:**
   a. **Select Menu → Software → Master Repository.**
   b. **Under the Name column, search for packages named Trellix Policy Auditor agent for <operating system>, such as Trellix Policy Auditor Agent for Windows.**
   c. **Under the Actions column, click Delete for each package.**

Install and uninstall the agent

Managed systems under **Trellix Policy Auditor** must have the **Trellix Agent** and the **Trellix Policy Auditor** agent plug-in.

For information about installing and working with the **Trellix Agent**, see the **McAfee ePO** documentation.

Install the Trellix Policy Auditor agent

Install the **Trellix Policy Auditor** agent before you run audits on managed systems.

Task

1. **On the McAfee ePO console, select Menu → Systems → System Tree, then click the Assigned Client Tasks tab.**
2. **Select the System Tree group with the systems where you want to install the Trellix Policy Auditor agent.**
3. **Click Actions → New Client Task Assignment.**
4. **Select the following Task to Schedule options.**
    - For **Product**, select **Trellix Agent**.
    - For **Task Type**, select **Product Deployment**.
    - For **Task Name**, click **Create New Task**.
5. **Fill in the client task settings, then click Save.**
    - Type a name and an optional description for this task.
    - Select the **Target Platforms**.
    - Select a **Trellix Policy Auditor** agent from the **Product and components** list, then select options from the drop-down lists.
        - **Trellix Policy Auditor for Windows 6.4.0**
        - **Action** — Install
        - **Language** — Language neutral
        - **Branch** — Current
    - Optionally, select **Run at every policy enforcement (Windows only)** to reinstall the **Trellix Policy Auditor** agent if a user has removed the product or component. This is done at the next policy enforcement interval.
    - Optionally, select **Allow end users to postpone this deployment**, then select the settings.
6. **Fill in the rest of the Task to Schedule settings, then click Next.**
    - For **Lock task inheritance**, select **Unlocked** or **Locked**.
    - For **Tags**, select **Send this task to all computers** or **Send this task to only computers which have the following criteria**. If you send based on criteria, click **Edit** to select the criteria.
7. **Configure the schedule, then click Next.**
8. **Review the task settings, then click Save. The task is added to the list of client tasks for the selected group and any group that inherits the task.**
9. **Send a manual wake-up call to the systems to run the client task immediately.**

Uninstall the Trellix Policy Auditor agent

Uninstall the **Trellix Policy Auditor** agent from systems on your network if you do not want them to be managed by **Trellix Policy Auditor** content.

This is useful when you want to convert a managed system to an unmanaged system and reduce the load on system resources.

Task

1. **On the McAfee ePO console, select Menu → Systems → System Tree, then click the Assigned Client Tasks tab.**
2. **Select the System Tree group with the systems where you want to install the Trellix Policy Auditor agent.**
3. **Click Actions → New Client Task Assignment.**
4. **Select the following Task to Schedule options.**
    - For **Product**, select **Trellix Agent**.
    - For **Task Type**, select **Product Deployment**.
    - For **Task Name**, click **Create New Task**.
5. **Fill in the client task settings, then click Save.**
    - Type a name and an optional description for this task.
    - Select the **Target Platforms**.
    - From the **Product and components** list, select a **Trellix Policy Auditor** agent.
    - From the **Action** list, select **Remove**.
    - Optionally, select **Run at every policy enforcement (Windows only)** to reinstall the **Trellix Policy Auditor** agent if a user has removed the product or component. This is done at the next policy enforcement interval.
    - Optionally, select **Allow end users to postpone this deployment**, then select the settings.
6. **Fill in the rest of the Task to Schedule settings, then click Next.**
    - For **Lock task inheritance**, select **Unlocked** or **Locked**.
    - For **Tags**, select **Send this task to all computers** or **Send this task to only computers which have the following criteria**. If you send based on criteria, click **Edit** to select the criteria.
7. **Configure the schedule, then click Next.**
8. **Review the task settings, then click Save. The task is added to the list of client tasks for the selected group and any group that inherits the task.**
9. **Send a manual wake-up call to the systems to run the client task immediately.**

Send a manual wake-up call to a group of systems

Send manual wake-up calls to a **System Tree** group to verify that the **Trellix Agent** and **McAfee ePO** server are communicating. This is useful when you make policy changes and want agents to download the update.

Task

1. **On the McAfee ePO console, select Menu → Systems → System Tree, then select the group.**
2. **Select a group, select the systems from the list, then click Wake Up Agents.**
3. **Verify that the systems appear next to Target systems.**
4. **Next to Wake-up call type, select whether to send an Agent Wake-Up Call or a SuperAgent Wake-Up Call.**

5. **Accept the default Randomization (0–60 minutes) or type a different value.**

   Note

   If you type `0`, agents respond immediately. Consider carefully the number of systems that are receiving the wake-up call and how much bandwidth is available.

6. **By default, Get full product properties is selected. This causes the Trellix Policy Auditor agent to send complete system properties to Trellix Policy Auditor. Deselect this option to send only properties that have changed since the last agent-server communication.**
7. **Click OK to send the wake-up call.**
8. **Verify that the Trellix Policy Auditor agent and McAfee ePO server are communicating. Go to Reporting → Audit Log and search the log for an entry:** Wake Up Agents | Succeeded.

Display the system tray icon on Windows systems

You can configure **Trellix Policy Auditor** to display a system tray icon on Windows systems. The icon is not available for non-Windows systems.

The icon allows the user to see the status of audits, including whether an audit is running, scheduled, not scheduled, or disabled.

Task

1. **On the McAfee ePO console, select Menu → Systems → System Tree, then click the Assigned Policies tab.**
2. **From the Product drop-down list, select Policy Auditor Agent.**
3. **Under the Policy column, click My Default to open the whiteout/blackout page.**
4. **Next to General Options, select Show the Policy Auditor system tray icon (Windows only), then click Save.**

COPYRIGHT

Trellix