ePO 4.6 Best Practices

Hardware configuration

- McAfee ePolicy Orchestrator can manage up to 50,000 nodes with basic server hardware and reasonable planning. Once you pass 50,000 nodes it becomes much more important how you configure your McAfee ePO server hardware for the best possible performance.
- Environments up to 5,000 or 10,000 nodes can have the McAfee ePO server and SQL Server installed on one physical server to save hardware, IT, and energy costs.
- Disk performance will decrease when using VM’s and node count is over 25,000

<table>
<thead>
<tr>
<th>Node count</th>
<th>ePO and SQL on one server</th>
<th>Use VM server</th>
<th>ePO DB on shared SQL Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>100-5,000</td>
<td>OK</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>5,000-25,000</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>25,000-75,000</td>
<td>Not recommended</td>
<td>Not recommended</td>
<td>Not recommended</td>
</tr>
<tr>
<td>75,000 or more</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Hard disk configuration

- Fewer than 5000 nodes, one server
- 5000 to 25000 nodes, one server
- 25000 to 75000 nodes, two servers
- More than 75000, two servers
SAN Usage
- Tier 1 SAN — The most expensive, fastest, and redundant storage array. If you have 75,000 nodes or more, use a tier 1 SAN to store your SQL database.
- Tier 2 SAN — Used to store critical data that requires redundancy. Plus, this data is accessed often but does not perform excessive transactions on the SAN.
- Tier 3 SAN — Used for databases that do not require much space and have little I/O.

Server hardware
- The fewer servers used for ePO the easier it will be to maintain your environment.
- Use 64-bit operating systems wherever possible.
- McAfee recommends you exceed the minimum recommendations wherever possible.
- The following table lists the hardware recommend for the various organization sizes.

<table>
<thead>
<tr>
<th>Organization size</th>
<th>Node count</th>
<th>McAfee ePO server</th>
<th>SQL Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CPU processors</td>
<td>RAM</td>
</tr>
<tr>
<td>Small</td>
<td>100 – 5,000</td>
<td>2</td>
<td>4 GB</td>
</tr>
<tr>
<td>Medium</td>
<td>5,000 – 25,000</td>
<td>2</td>
<td>4 – 8 GB</td>
</tr>
<tr>
<td>Large</td>
<td>25,000 – 75,000</td>
<td>4</td>
<td>8 – 16 GB</td>
</tr>
<tr>
<td>Very large</td>
<td>75,000 – 150,000</td>
<td>8</td>
<td>16 – 32 GB</td>
</tr>
</tbody>
</table>

Repository types
- FTP repositories
  - You might already have FTP servers in your environment and you can allow McAfee content to reside there as well.
  - Using FTP servers your clients do not need authentication and can use anonymous logon to pull their content.
  - No authentication reduces the chance a client might fail to pull its content.
- HTTP repositories
  - You can use an HTTP server to host a distributed McAfee ePO server repository.
  - Your HTTP servers allow clients to pull their content without authentication.
  - No authentication reduces the chance a client might fail to pull its content.
- UNC share repositories
  - If you chose to use UNC shares, you must:
    - Create the folder
    - Adjust share permissions
    - Change the NTFS permissions
    - Create two accounts, one with read and another with write access
  - All of these tasks increase the chance of failure since these processes must be completed manually risking human errors.
- Your agents might not properly update if your agents cannot authenticate to your UNC share because they are not part of the domain or the credentials are incorrect.

- SuperAgent repositories
  - SuperAgents have many advantages and is recommended for the ePO repository
  - Steps to creating a SuperAgent
    - Create a new SuperAgents Policy
    - Create a new group in the system tree, for example named SuperAgents
    - Assign the new SuperAgents policy to the new SuperAgents group.
    - Drag a system into the new "SuperAgents" group.
  - Creating a new SuperAgent policy
    - From the Policy Catalog, click McAfee Agent and from the Category list, select General to create a new policy.
    - From the General tab, click Convert agents to SuperAgents and Use systems running SuperAgents as distributed repositories, then type a folder path location for the repository.

- Creating a new group in the system tree
  - With a SuperAgent group in your System Tree you can assign the SuperAgent policy to the group. Create a new group in the System Tree called 1_SuperAgents.
  - From the System Tree, click System Tree Actions | New Subgroup and give it a distinctive name, for example 1_SuperAgents.
Click **OK**. The new group appears in the System Tree list.

- Assigning the new SuperAgent policy to the new SuperAgents group
  - From the SuperAgent group you created, click the **Assign Policies** tab and select **McAfee Agent** from the Product list.
  - From the Actions column, click **Edit Assignments**. The McAfee Agent : General dialog box appears.
  - Click **Break inheritance and assign the policy and settings below**, select the SuperAgent policy you created from the Assigned Policy list, and click **Save**.

- Dragging a system into the new SuperAgents group
  - In the System Tree, click the **Systems** tab and find the system you want to change to a SuperAgent repository.
  - Drag that row with the system name and drop it into the new SuperAgent group you created in the System Tree. Once the system communicates with the McAfee ePO server it changes to a SuperAgent repository.
  - To confirm the system is now a SuperAgent repository, click **Menu | Software | Distributed Repositories** and select **SuperAgent** from the Filter list. The new SuperAgent repository appears in the list.
- How many repositories to use

<table>
<thead>
<tr>
<th>Server hardware</th>
<th>Nodes updated</th>
<th>Dedicated or shared client hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single 3 Ghz processor with 4 GB of memory</td>
<td>3,000</td>
<td>Shared with other applications</td>
</tr>
<tr>
<td>Server class hardware, dual-quad processor and 8 GB of RAM</td>
<td>3,000 – 7,000</td>
<td>Dedicated</td>
</tr>
<tr>
<td></td>
<td>5,000 – 7,000</td>
<td>Dedicated</td>
</tr>
</tbody>
</table>

- Improving agent update performance
  - Open the Policy Catalog.
  - From the Product list, select McAfee Agents then from the Category list, select General.
  - Click Edit Setting and the Repositories tab.
  - From the Repositories list find the McAfee ePO server and click Disable in the Actions column.
  - Click Save and the McAfee ePO server repository is disabled.

- Upgrading ePO software
  - You can perform an in-place McAfee ePO server upgrade, or a clean installation of the McAfee ePO server.
  - In-place upgrade tips
    - Back up your infrastructure. This includes your SQL database and any agent keys. See KnowledgeBase article KB66616 for detailed backup procedures.
    - Make any hardware changes or remove any repositories that you want to decommission.
    - Make sure your hardware and bandwidth meet the minimum requirements before upgrading.
    - Confirm you have the required software, such as the newer version of the McAfee Agent. Remove any unsupported software. For example, Rogue System Detection or System Compliance Profiler.
    - Go through your users on the McAfee ePO server and remove any unneeded accounts.
    - Clean out all unused policies.
    - Remove any old client tasks you no longer use. For example, old deployment tasks or old patch installation tasks. If the task is not in use remove it.
    - Validate your tree and remove any agents that have not communicated with the ePO server in 14 days. In addition, remove any shell machines that were imported into ePO from Active Directory.
    - Purge events that are not needed. Try to delete any events older than 60 days.
    - Backup, reindex, and check your disk space on the SQL Server. Confirm you have plenty of disk space for the SQL database.
- Remove old versions of software that you are not using. For example, patches for older versions of products that are no longer used.
- Test your upgrade in a VM environment with a copy of your SQL database to make sure the upgrade works smoothly.
- Validate all your settings to confirm they are in place after the upgrade.

**Move the server**
- Make sure to back up the following:
  - The SQL database (critical)
  - Agent keys which secure the communication between the server and all your agents
  - Software checked into the master repository
  - Extensions to manage all your product policies
  - Secure Sockets Layer (SSL) certificates
  - Server settings such as communication ports

**Moving McAfee Agents between servers**
- Install a new McAfee ePO server. See McAfee ePolicy Orchestrator 4.5 Installation Guide for detailed instructions.
- Export and import the following from the old McAfee ePO server to the newly built McAfee ePO server:
  - Export your product policy files in XML.
  - Export your tree structure in a txt file (ePO version 4.5 only).
  - Export any custom queries you have created.
  - Import your tree structure on your new McAfee ePO server.
  - Import the product policies and make sure they get assigned to the right groups.
  - Import any custom queries that you want to preserve.
- All of the following items, you previously configured, must be re-created manually:
  - Client tasks including deployment, update, and on demand tasks
  - Server tasks, including the McAfee content pull and replication
  - McAfee ePO server administrators and permission sets

**Using Transfer systems**
- Use the ePolicy Orchestrator 4.5 Transfer Systems task to move your agents from the old McAfee ePO server to the new McAfee ePO server.
- Tasks:
  - On the old McAfee ePO server, configure the new McAfee ePO server as a registered server. See McAfee ePolicy Orchestrator 4.5 Product Guide, Setting up registered servers for details.
  - On the old McAfee ePO server, click Menu | Systems | System Tree and the Systems tab to open a list of systems.
  - Select the systems to move to the new McAfee ePO server and click Actions | Agents | Transfer Systems. The Transfer Systems dialog box appears.
Select the server from the drop-down menu and click OK.

The McAfee Agent and your System Tree

- Deploying Agents
  - There are many ways to deploy the agent
    - A logon script
    - Manual execution
    - The McAfee ePO server
    - Third-party tools
    - An image with the agent as part of the image
  - You must first create your own specific agent before deployment
    - Click Menu | System | System Tree, from the System Tree pane, click System Tree Actions | New Systems. The New Systems dialog box appears.
    - Click Create and download agent installation package, complete the credentials needed, and click OK.
- From the Download File dialog box, save the files to a local machine.
  - Make the agent part of your image
    - Option 1 — Include the agent in your Windows image before freezing or finalizing the image.
    - Option 2 — Run the agent executable after your image is created using a repeatable script.
  - Confirm you deleted the agent GUID before freezing the image

What is the System Tree
- The System Tree is the logical representation of your managed network within the ePolicy Orchestrator console.
- Your system tree dictates:
  - How your policies for different products are inherited
  - How your client tasks are inherited
  - What groups your machines go into
  - What permissions your administrators have to access and change the groups in the System Tree.
- Creating tree for the first time, primary options are:
  - Using Active Directory (AD) synchronization
  - Dynamically sorting your machines
- Dynamically sorting your machines
  - GEO — Geographic location
  - NET — Network location
  - BU — Business unit
  - SBU — Sub business unit
  - FUNC — Function of the system (web, SQL, app server)
  - CHS — Chassis (server, workstation, laptop)
  - Policy Assignment — Will you have many different custom product policies to assign to groups based on chassis or function? Will certain business units require their own custom product policy?
  - Network Topology — Do you have sensitive WANs in your organization that can never risk being saturated by a content update? Or do you only have major locations and this is not a concern?
  - Client Task Assignment — When it comes time to create a client task, such as an on-demand scan, will you need to do it at a group level, such as a business unit, or system type, like a web server?
  - Content Distribution — Will you have an agent policy that specifies certain groups must go to a specific repository for content?
  - Operational Controls — Will you need specific rights delegated to your ePolicy Orchestrator administrators that will allow them to administer specific locations in the tree?
  - Queries — Will you need many options when filtering your queries to return results from a specific group in the System Tree. This is another factor that may be important when designing your tree.

Managing agent policies
- Agent to server communication interval (ASCI)
  - The agent-to-server communication interval (ASCI) dictates how often every McAfee Agent calls the McAfee ePO server, and is one of the most important settings under the agent policy.

<table>
<thead>
<tr>
<th>Node count</th>
<th>Recommended ASCI interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 – 1,0000</td>
<td>60 – 120 minutes</td>
</tr>
<tr>
<td>10,000 – 50,000</td>
<td>120 – 240 minutes</td>
</tr>
<tr>
<td>50,000 or more</td>
<td>240 – 360 minutes</td>
</tr>
</tbody>
</table>

- Sending a policy change immediately
  - Execute an agent wake-up call
If you need to wake-up thousands of systems, stagger the process by waking up a few thousand at a time.

**Configuring ASCI**

- Click **Menu | Policy | Policy Catalog**, then select **McAfee Agent** from the **Product list** and **General** from the **Category list**.
- Click the **General** tab, and type the **Agent-to-server communication interval** as shown in the following figure.
- Configuring the policy enforcement interval
  - Click **Menu | Policy | Policy Catalog**, then select **McAfee Agent** from the Product list and **General** from the Category list.
  - Click the **General** tab, and type the **Policy enforcement interval** as shown in the following example.

- Deploying packages
  - Click **Menu | Configuration | Server Settings**, then in the Settings Category pane click **Repository Packages**, The following dialog box appears

- Using Client and Server tasks in your managed environment
  - **Client tasks**
    - **Product deployment** — Tells the agent which products you want it to deploy to the client
    - **Product update** — Uses the McAfee Agent update content such as VirusScan signatures, engine, or product patches
  - **Deploying products**
    - Click **Menu | Systems | System Tree | Client Tasks**, then select a group in the System Tree.
    - Click **Actions | New Task**. The Client Task Builder wizard opens.
    - Type a name, select **Product Deployment** from the list, and click **Next**. The Client Task Builder page appears.
    - Configure the **Target platforms** and **Products and components**.
- Optional. Click **Run at every policy enforcement**.
- Click **Next** to configure scheduling product deployment with randomization.
  - Schedule product deployment with randomization
- Updating products
  - Click Menu | Systems | System Tree and click My Organization in the System Tree pane.

  - From the Client Tasks tab, click Actions | New Tasks and the Client Task Builder dialog box appears.
  - Type a name, for example Daily Master Updates, click Product Update from the Type list, and click Next. The Client Task Builder dialog box appears.
Choose the content to update using this task.

Click Next to configure the schedule for this task.
Creating a server task

- Click **Menu | Automation | Server Tasks** and click **Actions | New Task**. The Server Task dialog box appears.
- Give the task a name, for example **Manage Inactive Systems**, and click **Next**. The Actions dialog box appears.
- Configure a weekly report.
  - Click **Run Query** from the Actions list.
  - Click **Managed Inactive Agents** query from the Query list dialog box that appears, then click **OK**.
  - Create a subaction that deletes the inactive agents generated by the report, then click **Next**.
- Schedule the server task to run. For example, on a busy McAfee ePO server make sure you run this task during off hours, either nightly or weekly.

Creating an automatic report email or export
- Click Menu | Automation | Server Tasks, and click Actions | New Task. The Server Task dialog box appears.
- Give the task a name, for example Manage Inactive Systems and click Next. The Actions dialog box appears.
- Configure an email report.
  - Click Run Query from the Actions list.
  - Click Managed Inactive Agents query from the Query list dialog that appears, then click OK.
  - Create a subaction that emails the file as a PDF file to your selected recipients, then click Next.

Choose the custom or preconfigured query that you want to email and enter the email address where you want the email sent. Choose the format you would like for the reports. Optionally, you can zip your files to reduce their size.

- Schedule when the server task should run. For example, on a busy ePO server make sure you run this task during off hours, either nightly or weekly.

- Disabling master repository client pulls
  - Open the Policy Catalog, select McAfee Agents from the Product list, then select General from the Category list.
  - Click Edit Setting and the Repositories tab.
  - From the Repositories list, find the McAfee ePO server and click Disable in the Actions column.
Click **Save** to disable the McAfee ePO server repository.

- Creating a purge events server task
  - Click **Menu | Automation | Server Tasks**, then click **Action | New Task**. The Server Task Builder dialog box appears.
  - Give the task a name, for example **Delete client events**, and from the Actions tab configure the following from the Actions list:
    - **Purge Audit Log** — Purge after 6 months.
    - **Purge Client Events** — Purge after 6 months.
    - **Purge Server Task Log** — Purge after 6 months.
    - **Purge Threat Event Log** — Purge after day.
    - **Purge SiteAdvisor Enterprise Plus Events** — Purge after 10 days.
Schedule the task to run everyday during non-business hours, then click **Save**.

- Purging events by query
  - Configure a query to return the events you want purged. See *Creating custom event queries* for details.
  - Click **Menu | Automation | Server Tasks**, then click **Action | New Task**. The Server Task Builder dialog box appears.
  - Give the task a name, for example *Delete 1059 client events*, and from the **Actions** tab, click **Purge Client Events** from the Actions list.
  - Click **Purge by Query** and select the custom query you created in step 1.

Schedule the task to run everyday during non-business hours, then click **Save**.
- Edit and enable the Inactive Agent Cleanup server task
  o Click Menu | Automation | Server Tasks and click Edit for the Inactive Agent Cleanup Task for 4.5 in the Action column. The Server Task dialog box appears.
  o If needed, change the name, click Enabled next to Schedule status, and click Next. The Actions dialog box appears.

  ![Server Task Builder](image)

  o Optional. Instead of using the default subaction Delete Systems, you can select Move Systems to another Group. This moves the systems found by the query to a designated group in your System Tree in case you want to investigate these systems further
  o Click Next, schedule when you want this server task to run and save the server task.

Reporting on your managed environment with queries
  - Creating custom event queries
    o Click Menu | Reporting | Queries, then Actions | New Query. The Query Wizard appears starting with the Result Types tab.
      - **Threat Events** — In the following, click Systems Events in the Feature Group and Threat Events in the Result Type.

  ![Query Wizard](image)

  - **Managed Systems** — In the following, click Systems Management in the Feature Group and Managed Systems in the Result Type.
You must choose your chart type. There are several chart types to choose from and some are more complex than others. The two simplest charts are the pie chart and the single group summary table. The pie chart is good for comparing multiple values in a graphic format and the summary table is good for viewing a data set with over 20 results. Click Pie Chart under Display Results Type.

You must choose the label or variable that you want the report to display. There are many variables you can choose to have the McAfee Agent reports display. In the Labels are list, click OS Type.
- You can choose the columns that you want to see if you drill down on any of the variables in your report. This is not a critical component when building your query and can be adjusted at a later time. Click **Next** to use the default columns.
- Click **Next** to not create any filters and display all of the operating system types.
- Click **Run** to generate the report and see the results. After you create the reports and display the output you can fine tune your report without starting again from the beginning. To do this, click **Edit Query**. This allows you to go back and adjust your report and run it again within seconds.

### Creating custom table queries
- Click **Menu | Reporting | Queries**, the Queries dialog box appears.
- Click **Actions | New Query** and the Query Wizard appears starting with the **Result Types** tab.
- Click **Events** in the Features Group and **Client Events** in the Result Type.
- Click **Table**, under **List**, in the Display Results As pane to create a simple table format and click **Next**.
Click Next to skip the Columns dialog box. You can choose the columns you want to analyze.

Click Event ID in Available Properties under Client Events to create an Event ID filter. An Event ID row is added in the Filter pane.

Click the plus sign, +, at the right to add another comparison row, add 1051 and 1059 in the Value column, then click Run. This setting filters the query and only returns 1051 and 1059 events as shown in the following output figure.

Optionally, you can select all of these 1051 and 1059 events, click Actions | Purge to purge all of these events in real time.

Create a new server task and give it an appropriate name. For example, Purge of 1051 and 1059 Events Nightly.

Click Purge Threat Event Log from the Actions list, then click Purge by Query.

Find the custom query you just created and click it in the list.

Schedule the task to run every night, then click Save.

Disaster recovery
- Configuring simple disaster recovery
  
The simplest method of disaster recovery is to rebuild the McAfee ePO server and restore the SQL database that you have backed up for safe keeping. This is a good option if you are a small environment (5,000 to 25,000 nodes) and if you have a reasonable tolerance for downtime.

This means if your server has a hardware failure to get your McAfee ePO server up and running again you must:

  - Repair the McAfee ePO server.
  - Reinstall the ePolicy Orchestrator software.
  - Patch the ePolicy Orchestrator software back to the previous levels.
  - Restore the SQL database.

Full restore procedures are covered in KnowledgeBase article KB66616.