



Product Guide

McAfee Performance Optimizer 2.0.0

For use with ePolicy Orchestrator

COPYRIGHT

© 2016 Intel Corporation

TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1	Product overview	5
	What is Performance Optimizer?	5
	Key features	5
	How it works	6
2	Getting started	7
	Requirements	7
	Install Performance Optimizer	8
	Configuring database access for Performance Optimizer	8
	Workflow for configuring permissions	8
	Create a database user account	9
	Specify server settings credentials	9
	Managing the Performance Optimizer Admin permission set	10
	Configuring the assessments	11
	Using Performance Optimizer	12
	Performance Optimizer workflow	13
	Assessments and what they do	15
	How assessment scores work	20
3	Collecting and analyzing data	33
	Collecting data on performance	33
	Server tasks and editable actions	34
	Sending notifications	35
	Configure a notification	36
	Respond to a notification	37
	Default queries and when to use them	38
	Default dashboards	39
	Export information from the dashboard	40
4	Monitoring the health of your environment	41
	Monitoring your database health	41
	Gathering backup information	41
	Configuring database settings	41
	Working with blocked queries	44
	Monitoring CPU usage	44
	Working with deadlocked queries	44
	Monitoring disk space	45
	Monitoring disk performance	45
	Monitoring messages with Orion Log Analyzer	45
	Using identity columns	45
	Monitoring index fragmentation	46
	Verifying database integrity	46
	Measuring memory usage	46
	Collecting server performance counters	46
	Collecting disk usage and row counts	47

Monitoring your McAfee ePO Application Server	47
Monitoring disk usage with McAfee ePO Application Server	47
Monitoring memory usage with McAfee ePO Application Server	47
Monitoring CPU usage with McAfee ePO Application Server	48
A Best practices: Database server provisioning	49
B Use external tools to analyze Performance Optimizer metrics	51
C FAQ	53

1

Product overview

The Performance Optimizer analyzes the performance of your McAfee® ePolicy Orchestrator® (McAfee ePO™) environment with a score and recommendations for improved performance.

Dashboards display the results of the collected data, allowing you to drill down for more detail and to view recommendations. Assessments allow you to view details about your environment. For example, you can view information about unmanaged systems, systems with an inactive McAfee® Agent or Agent Handler, and timestamps of user logons. You can also configure Automatic Responses to send text messages or email notifications when a specific performance area requires examination.

Contents

- [What is Performance Optimizer?](#)
- [Key features](#)
- [How it works](#)

What is Performance Optimizer?

Performance Optimizer identifies issues and provides a recommendation about how to solve the problem.

From the McAfee ePO console, you can monitor and evaluate the health of your environment by viewing the Performance Optimizer dashboards and running assessments using a server task.

A series of assessments gathers data about the health of your environment, then returns a score and recommendations to improve performance.

Key features

Performance Optimizer features allow you to monitor a McAfee ePO database, McAfee ePO Application Server, and use Automatic Responses to send text messages or email notifications.

Use this feature...	To...
Database monitoring	Monitor the health of your McAfee ePO database.
McAfee ePO Application Server monitoring	Monitor the health of your McAfee ePO Application Server.
Automatic Responses	Send text message or email notifications.
Server settings	Control database access and monitor thresholds.
Permission sets	Determine who views the health monitor data.

How it works

These components make up Performance Optimizer.

McAfee ePO console

Performance Optimizer is an extension that uses these McAfee ePO features:

- Server Settings
- Server Tasks
- Server Task Log
- Automatic Responses
- Queries and Reports
- Dashboards

McAfee ePO server

The McAfee ePO server is the system that hosts the McAfee ePO console. Performance Optimizer analyzes metrics about the McAfee ePO server.

McAfee ePO Application Server

McAfee ePO Application Server provides the McAfee ePO console. Performance Optimizer:

- Runs within the McAfee ePO Application Server.
- Analyzes metrics about the McAfee ePO Application Server.

McAfee ePO database

McAfee ePO database is used by the McAfee ePO Application Server to store data. Performance Optimizer:

- Stores its metric data into the McAfee ePO database.
- Collects metrics about the McAfee ePO database and database server.

Database server

Performance Optimizer directly queries the database server that hosts the McAfee ePO database. These queries determine the overall health and performance of the database and server.

2

Getting started

From McAfee ePO, install or upgrade Performance Optimizer to start running assessments to monitor the health of your databases.

Contents

- *Requirements*
- *Install Performance Optimizer*
- *Configuring database access for Performance Optimizer*
- *Managing the Performance Optimizer Admin permission set*
- *Configuring the assessments*
- *Using Performance Optimizer*
- *Performance Optimizer workflow*
- *Assessments and what they do*
- *How assessment scores work*

Requirements

Make sure that your system meets these requirements before you install and use Performance Optimizer.

These are the supported versions:

- Microsoft SQL Server 2008 R2, with Service Pack 1 or later
- ePolicy Orchestrator 5.1.1–5.1.3, 5.3.0–5.3.2

When installing or upgrading Performance Optimizer, a verification process ensures that the SQL Server instance is at least SQL 2008 R2 Service Pack 1 or later. If an older version of SQL Server is found, an error message appears when installing and upgrading the McAfee ePO extension.

Error type	Error message
Installation	Unable to install extension. java.sql.SQLException: Performance Optimizer is supported on SQL Server 2008 R2 Service Pack 1 or higher
Upgrade	Unable to install extension. Installation error: checkCommandsExist: upgrade: [echo] Upgrade called for PerfOptimizer (version 2.0.0.<version>) BUILD FAILED C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\extensions\installed\PerfOptimizer\2.0.0.<version>\install.xml:122: java.sql.SQLException: Performance Optimizer is supported on SQL Server 2008 R2 Service Pack 1

Install Performance Optimizer

Install the extension in McAfee ePO from the Software Manager, then configure the server task settings or use the default settings.

Before you begin

Make sure that your system meets these requirements:

- Microsoft SQL Server 2008 R2, with Service Pack 1 or later
- ePolicy Orchestrator 5.1.1–5.1.3, 5.3.0–5.3.2

Task

- 1 Log on to the McAfee ePO console as administrator.
- 2 Select **Menu | Software | Software Manager**.
- 3 In the Software Manager page Product Categories list, select the **Checked in Software** category, or use the search box to find the Performance Optimizer software.
Performance Optimizer is located below McAfee ePolicy Orchestrator in the Software Manager.
- 4 When you have located the correct software, click **Check In**.
- 5 On the Check In Software Summary page, review and accept the product details and End User License Agreement (EULA), then click **OK**.

Configuring database access for Performance Optimizer

You can configure Performance Optimizer through server settings in McAfee ePO.

Data Retention

Allows a value between 0–30. This value is used in the **Performance Optimizer: Purge assessment data** server task to remove metric data that is older than the number of days specified.

When the value is set to 0, all metric data is purged when the **Performance Optimizer: Purge assessment data** server task runs.

Orion Log Analyzer

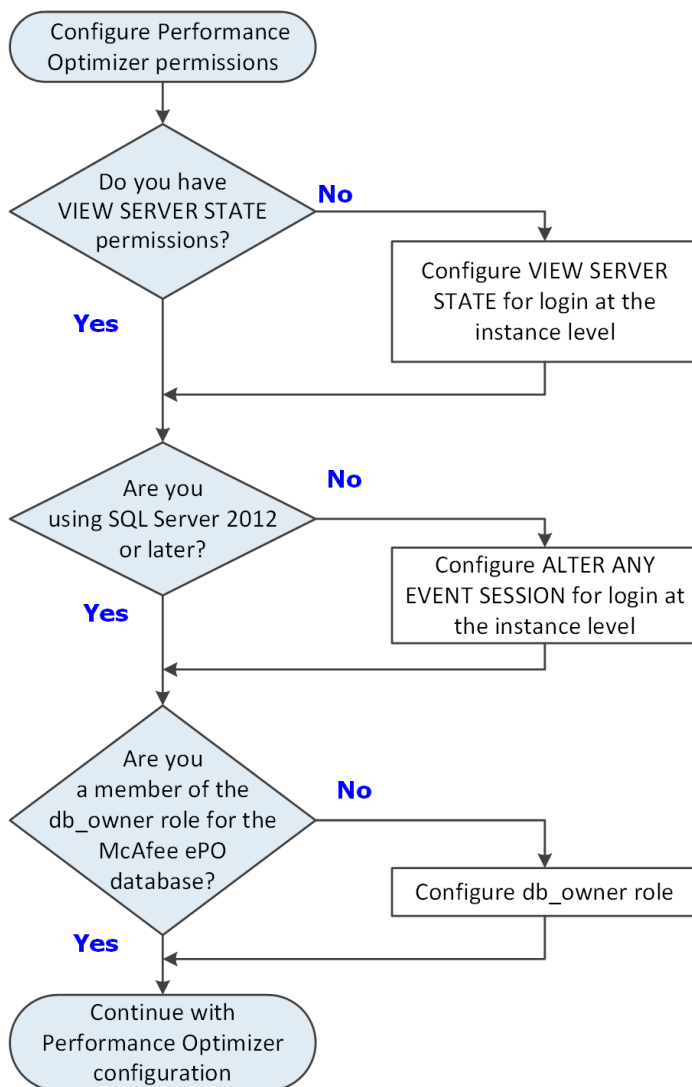
Specifies the monitoring level. The analysis processes records activity based on the level selected or higher. For example, if the **Warn** level is selected, all activity at the **Warn** level or higher is recorded.

Separate database user

Allows a separate database user account for use by Performance Optimizer only. No other managed products use the credentials specified in this section of the server settings. Select **Test Default ePO Database User** to see if the McAfee ePO database account already has sufficient permissions.

Workflow for configuring permissions

The separate database user account requires specific permissions.



Create a database user account

A SQL Server script allows you to create a database user account for Performance Optimizer. Prepare the script so you can use it for database user provisioning. For more information, see [KB87360](#).

Specify server settings credentials

Specify the database user information in the server settings.

Before you begin

Prepare the script so you can use it for database user provisioning. For more information, see [KB87360](#).

Select **Test Default ePO Database User** to see if the McAfee ePO database account already has sufficient permissions.

Task

- 1 Log on to the McAfee ePO console as administrator.
- 2 Select **Menu | Configuration | Server Settings**.
- 3 Select **Performance Optimizer**.
- 4 In the lower-right corner, click **Edit**.
- 5 Enter the database user information based on the account type:
 - SQL authenticated user
 - Windows user with access to a SQL Server
- 6 Click **Test New ePO Database User**.

If a permission is missing, a notification appears describing the items you must add.

Managing the Performance Optimizer Admin permission set

With administrator permissions, users are granted administrator access to the metric data generated by Performance Optimizer.

Use this permission set to interact with the Performance Optimizer data, but not the McAfee ePO System Tree.

Here are the available roles:

- Administrator permissions for Performance Optimizer data
- No permissions

Action	Steps
View the permission set	<ol style="list-style-type: none">1 Log on to the McAfee ePO console as administrator.2 Select Menu User Management Permission Sets.3 Select Performance Optimizer Admin.
Add a user to the permission set	<ol style="list-style-type: none">1 Log on to the McAfee ePO console as administrator.2 Select Menu User Management Users.3 Click New User.4 Select whether to enable or disable the logon status of this account. If this account is for someone who is not yet a part of the organization, you might want to disable it.5 Select the account's authentication method, then provide the required credentials, or browse to and select the certificate.6 Provide the user's full name, email address, phone number, and a description in the Notes text box.7 Make the user an administrator, or select the appropriate permission sets for the user.8 Click Save. <p>The new user appears in the Users list on the User Management page.</p>

For more information about managing permission sets and user accounts, see the *McAfee ePolicy Orchestrator Product Guide*.

Configuring the assessments

You can adjust the settings to learn specific details about the performance and health of a particular function.

Some assessments allow additional configuration. Here are examples of parameters that you can adjust at anytime:

- **Priority** — Set the level to reflect the priority of an assessment. The level you set does not affect the score.
- **Acceptable score (0-10)** — Keep the default settings or adjust the number, depending on your environment.

Using Performance Optimizer

From the McAfee ePO console, you can monitor and evaluate the health of your environment by viewing the Performance Optimizer dashboards and running assessments using a server task.

Running an assessment

Use a server task to run an assessment — From the Server Tasks page, click **Edit | Actions** to see the list of assessments. Several assessments are preconfigured with default settings, but you can change them at any time.



Performance Optimizer provides additional server tasks that do not offer this type of configuration.

Here is a list of the types of assessments that you can run for the server task **Performance Optimizer: Analyze ePO configuration, database configuration, and database backups**.

- McAfee Agent versions
- Systems with an inactive McAfee Agent
- Unmanaged systems
- Duplicate systems
- Agent Handler system distribution
- Inactive Agent Handlers
- ASCI settings
- Number of threat events
- Number of received threat events
- Number of daily threat events
- Scheduled server task settings
- Server tasks — Length of runtime
- Server tasks — Completion status
- McAfee Agent updates
- Location of distributed repositories
- Timestamp of user logons in last 7 days
- Timestamp of daily logons
- McAfee Agent packages in the Master Repository

Viewing the dashboards

Performance Optimizer: Assessment Summary dashboard — Includes a pie chart that summarizes the score of each assessment and a list of items that require action or have acceptable scores. You can use these default settings, or customize the scores to meet the unique needs of your environment:

Color	Assessment
Red	Action Required
Green	Acceptable

Assessment History dashboard — Displays the history of your assessments by date, time, and score. Select an assessment to drill down for more detail. For example, select **Systems with an inactive McAfee Agent** to drill down and select a specific system, then perform an action.

The acceptable minimum score can be adjusted for the assessments that are included in **Performance Optimizer: Analyze ePO configuration, database configuration, and database backups**.

Viewing assessment scores

Understand the scoring system — By default, the Performance Optimizer uses a range of 0–10 to score an assessment. The optimal score is 10 and means that your environment is not at risk. The assessment for a score below 9 includes a recommendation for how to improve the health and performance of your environment.



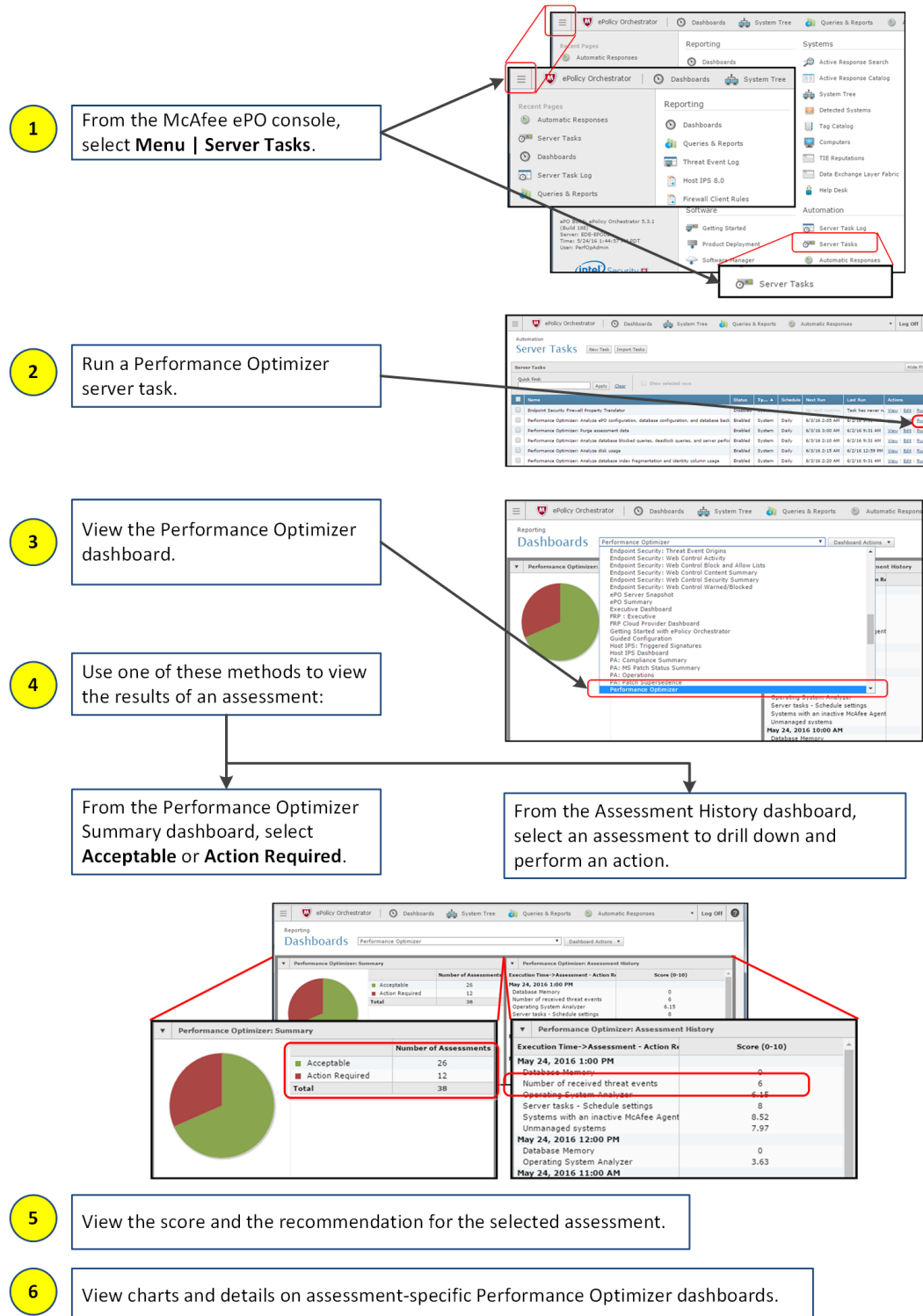
Assessments that receive a score lower than 9 don't always require action. See the corresponding assessment's description and recommendation for more details.

Modify the parameters — Each assessment provides a Priority drop-down list that displays these categories: Critical, High, Medium, and Low. Adjusting the levels allows you to prioritize each assessment, so that you can determine which assessment requires immediate attention and which can wait.

The Priority level does not affect the score of an assessment.

Performance Optimizer workflow

This example workflow demonstrates how all server tasks work. In this scenario, run a server task to view the results from your McAfee ePO dashboard.



Assessments and what they do

The Performance Optimizer assessments return results when you run a server task. Each assessment evaluates a specific function, allowing you to learn about different health-related aspects in your environment.


For more details about a specific recommendation, see the *McAfee ePolicy Orchestrator Product Guide*.

Assessment	How it works	Recommendation
McAfee Agent versions	Retrieves the number of agents, which are grouped by the agent version. Performance Optimizer analyzes the ratio of agents that are upgraded and not upgraded.	Upgrade managed systems to the latest McAfee Agent version. From the McAfee ePO console, in Software Manager, view the latest McAfee Agent version for your endpoint system platform type. From the McAfee Downloads site, review available hotfix releases.
Systems with an inactive McAfee Agent	Gathers the total number of systems where the McAfee Agent has not communicated with McAfee ePO in the number of days you specified, and calculates the ratio of systems with active agents to systems with inactive agents. The default number of days is 15. You can change this number as needed.	Determine why managed systems are inactive. From the System Tree, remove inactive systems if they no longer require management. For information about inactive agents, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Unmanaged systems	Gathers the total number of systems that aren't managed, and analyzes the ratio of managed systems to unmanaged systems.	Determine if the unmanaged systems require a McAfee Agent deployment, then remove unmanaged systems from the System Tree if they no longer require management. For information about unmanaged systems, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Duplicate systems	Gathers the total number of duplicate systems, and calculates the ratio of managed and unmanaged systems.	Remove duplicate systems from the System Tree. For more solutions and information about the queries used to identify duplicate systems, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Agent Handler system distribution	Retrieves the total number of systems, Agent Handlers, and agents managed by each Agent Handler. Also calculates the ratio of agents to Agent Handlers.	Configure Agent Handler assignments to make sure that each Agent Handler manages a similar number of agents. For information about Agent Handler management, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Inactive Agent Handlers	Retrieves the total number of active Agent Handlers and those that have not communicated with McAfee ePO in the number of hours you specified. Also analyzes the ratio of active to inactive Agent Handlers.	Verify that Agent Handlers are communicating with McAfee ePO and that managed systems can communicate with their Agent Handlers. For information about Agent Handler management, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .

Assessment	How it works	Recommendation
ASCI settings	Retrieves the ASCI settings for all policies, and analyzes the potential number of agent-server communications per second.	<p>Modify the ASCI value specified in the McAfee Agent policy if managing a large amount of agents.</p> <p>For information about Agent-to-Server Communication Interval (ASCI), see the <i>McAfee ePolicy Orchestrator Product Guide</i>.</p>
Number of threat events	Retrieves and analyzes the total number of reported threat events.	<p>View the Purge Threat and Client Events Older than 90 Days server task.</p> <p>Configure the server task action settings and schedule to make sure that only the appropriate amount of threat events are retained for online reporting.</p> <p>Review the policy settings for each managed product to make sure that the appropriate events are reported to the McAfee ePO server.</p> <p>For information about configuring policy settings, see the <i>McAfee ePolicy Orchestrator Product Guide</i>. Also, for information about policy settings that might produce events, see the documentation for that specific managed product.</p>
Number of received threat events	Retrieves and analyzes the number of threat events by type.	<p>Review the Event Filtering category in the Server Settings.</p> <p>Review the policy settings for each managed product to make sure that the appropriate events are reported to the McAfee ePO server.</p> <p>For information about configuring policy settings and event filtering, see the <i>McAfee ePolicy Orchestrator Product Guide</i>. Also, for information about policy settings that might produce events, see the documentation for that specific managed product.</p>
Number of daily threat events	Retrieves and analyzes the number of threat events received each day.	<p>Review the Event Filtering category in Server Settings.</p> <p>Review the policy settings for each point product to make sure that the appropriate events are reported to the McAfee ePO server.</p> <p>For information about configuring policy settings and event filtering, see the <i>McAfee ePolicy Orchestrator Product Guide</i>. Also, for information about policy settings that might produce events, see the documentation for that specific managed product.</p>
Server tasks — Schedule settings	Retrieves and analyzes the settings for scheduled server tasks.	<p>Review the scheduled server tasks. If too many server tasks are scheduled to run at the same time, reschedule some tasks to run at a different time.</p> <div data-bbox="889 1602 933 1646" data-label="Image"></div> <p>This assessment examines the disabled server tasks to make sure that a set of results is available.</p> <p>For information about configuring server tasks, see the <i>McAfee ePolicy Orchestrator Product Guide</i>.</p>

Assessment	How it works	Recommendation
Server tasks — Length of runtime	Retrieves and analyzes the duration of each server task reported in the Server Task Log.	Review the server task action settings and schedule. If a server task took more time, reconfigure the task settings, then change the server task schedule to run when other tasks are not running. For information about configuring server tasks, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Server tasks — Completion status	Retrieves the completion status of each server task reported in the Server Task Log. Also analyzes the ratio of successful to failed tasks in the last 30 days.	Review the server task action settings. For information about configuring server tasks, see the <i>McAfee ePolicy Orchestrator Product Guide</i> . If the server task is provided by a managed product, see the documentation for that product to make sure that the configuration settings are correct.
McAfee Agent updates	Retrieves the list of distributed repositories and the number of agent updates performed from each repository. Also analyzes the repository distribution for agent updates.	Review the McAfee Agent repository policy. Reconfigure the McAfee Agent repository settings if too many systems are updated from the same distributed repository. For information about reconfiguring repositories, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Location of distributed repositories	Retrieves the location of the distributed repositories and compares it to the location of the Master Repository.	Change the path of the distributed repositories if they are configured to reference the same path as the Master Repository, then modify the path of the distributed repositories. Distributed repositories are designed as copies of the Master Repository. File locks can cause failures if the same directory path is referenced. For information about distributed repositories, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Timestamp of logons	Retrieves the list of user names and logon times. Also analyzes the number of daily logons.	Review all logon activities and make sure they are authorized and expected. For information about the Audit Log feature, and how logon and logoff activities are recorded, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
Timestamp of daily logons	Retrieves and analyzes all user logons and logoffs during the hours you specified.	Review the times that most users log on to the McAfee ePO server, and avoid scheduling server tasks to run during that time. For information about the Audit Log feature, and how logon and logoff activities are recorded, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .
McAfee Agent packages in the Master Repository	Retrieves the list of packages in the Master Repository and analyzes the package version of the McAfee Agent.	Use the latest and most recent versions of the McAfee Agent. Check in the latest McAfee Agent version to the Current branch of the Master Repository. For information about repositories, see the <i>McAfee ePolicy Orchestrator Product Guide</i> .

Assessment	How it works	Recommendation
Database backup	Collects information about database and log backups.	<p>Run database backups frequently.</p> <p>Transaction log backups must also be performed if the McAfee ePO database is using the full or bulk logged recovery model.</p> <p>For information about managing SQL databases, see the <i>McAfee ePolicy Orchestrator Product Guide</i>.</p>
Database CPU	Collects information about database CPU usage.	<p>High CPU usage on the database server indicates that more CPU resources must be allocated. Make sure that no other applications or databases are overusing CPU resources. It might also indicate that memory is insufficient and the operating system is paging information to disk.</p> <p>For additional information, see the <i>McAfee ePolicy Orchestrator Hardware Sizing and Bandwidth Usage Guide</i> on the McAfee Knowledge Center site.</p>
Database disk usage	Collects information about database disk usage.	<p>High disk usage can lead to service interruptions. Make sure that there is enough space on the disks hosting the McAfee ePO database files. Make sure that there are no other applications or databases on the database that might also be using a lot of disk space resources.</p> <p>For additional information, see the <i>McAfee ePolicy Orchestrator Hardware Sizing and Bandwidth Usage Guide</i> on the McAfee Knowledge Center site.</p>
Database memory usage	Collects information regarding database memory usage.	<p>High memory usage on the database server indicates that more memory resources must be allocated. Make sure that no other applications or databases are overusing memory resources.</p> <p>For additional information, see the <i>McAfee ePolicy Orchestrator Hardware Sizing and Bandwidth Usage Guide</i> on the McAfee Knowledge Center site.</p>
Database table disk usage	Collects information about database table disk usage.	<p>Tables with high disk usage require more disk, CPU, and memory resources to load the data into memory for usage by the application.</p> <p>To determine if high disk usage is normal and review recommended optimizations, see the <i>McAfee ePolicy Orchestrator Guide</i> and the documentation for that specific point product.</p>
Database index fragmentation	Collects information about database index fragmentation.	<p>Rebuild indexes with fragmentation greater than 30%. Reorganize fragmentation between 20–30%. Optimal index performance is achieved when fragmentation is removed on a regular schedule. See KB67184 for more information.</p>
Database table identity columns	Collects information about database table identity column usage.	<p>Identity columns use sequential integer number to populate data. If the identity column reaches the maximum value for the integer type, an error occurs and the database table must be modified.</p> <p>Contact Support for assistance if an identity column reaches 75% usage or higher.</p>

Assessment	How it works	Recommendation
Database file I/O statistics	Collects statistics about database file I/O.	Database I/O is a common cause of poor database query performance. These metrics distinguish where the I/O occurs and whether it is performing as expected. For additional information, see the <i>McAfee ePolicy Orchestrator Hardware Sizing and Bandwidth Usage Guide</i> on the McAfee Knowledge Center site.
Database integrity check	Verifies the integrity of a database.	DBCC CheckDB command verifies the integrity of a database. Restore the McAfee ePO database from a backup if the assessment displays that integrity errors were found. If a backup isn't available, try to repair the database with the help of Microsoft Support. In addition to the error information displayed in the Server Task Log, there is a new text file written to the database server log directory (for example, <SQL install dir>\MSSQL\Log).
Database and server configuration checks	Verifies: <ul style="list-style-type: none"> • Auto shrink, AutoClose, and Auto Update Statistics configuration. • Database file growth settings for the McAfee ePO database and tempdb configuration. • Database files are placed on separate disks. • Common server settings configuration. 	Use these settings: <ul style="list-style-type: none"> • AutoUpdate and AutoClose must be set to "false" • Auto Update Statistics must be set to "true" • File growth must be set to "auto-grow" by 256 MB for data files and 128 MB for log files <div>  Do not use "auto-grow" by percentage because it can lead to larger file growths. Data files and log files must be placed on separate disks for maximum I/O throughput. </div>
Database server performance counters	Collects the database performance counters from the McAfee ePO database server.	Performance counters are not given a score. They are for informational or advanced troubleshooting purposes and do not necessarily indicate that an action is required. Many of the metrics can be trended over time to see if values have changed significantly. Collect these counters more frequently to have a more accurate representation of the system performance.
Database blocking queries	Collects summary statistics about blocking queries. Also indicates queries that are blocked for long durations with too many tasks that are running simultaneously, or an external database user locked an object in the database.	Queries that are blocked for long durations can indicate that too many tasks are running simultaneously. Also might indicate that an external database user has locked an object in the database. If blocked query durations or counts increase, review the Server Tasks and other scheduled tasks to see if they can be scheduled to run at non-overlapping times. The blocking query details are printed to the Server Task Log.
Database deadlock queries	Collects information about deadlocked queries in the last 24 hours.	Deadlocked queries can indicate that task schedules must be modified so they are not overlapping. The deadlock details are printed to the Server Task Log.

Assessment	How it works	Recommendation
Orion Log Analyzer	Adds a listener to the Log4j logging component to collect and categorize the log messages recorded in orion.log.	Log messages at the ERROR level or higher must be investigated to ensure that the corresponding extension behavior is working as expected. The drill-down information displayed by Performance Optimizer indicates the exception message, which might have details about how to correct the problem without contacting Support. When contacting Support, it is a minimum requirement to provide a MER of the McAfee ePO server system.
McAfee ePO Application Server Java Memory Analyzer	Collects information about Java memory usage.	Java heap memory usage is high. Make sure that enough memory is allocated to the Java process. See KB71516 for more information.
McAfee ePO Application Server Operating System Analyzer	Collects information about Operating System and Java process OS utilization.	High CPU usage on the application server can lead to slower performance and indicates that more CPU resources must be allocated. Make sure that there are no other applications running on McAfee ePO Application Server that might be using a lot of CPU resources.
McAfee ePO Application Server Garbage Collection Analyzer	Collects information about Java garbage collection.	High JVM garbage collection metrics could indicate insufficient memory. To make sure that there is enough heap memory allocated to the Java process, see KB71516 . Make sure that sufficient CPU resources are allocated to the system hosting the McAfee ePO Application Server.
McAfee ePO Application Server Disk Analyzer	Collects information about disk usage on the McAfee ePO Application Server.	High disk usage can lead to service interruptions. Make sure that there is enough space on the disks that are hosting the McAfee ePO Application Server components.
McAfee ePO Application Server Page File Analyzer	Collects information about page file usage on the McAfee ePO Application Server.	Place the page file on the fastest disk available. The metric that measures the current usage can be monitored to see if the page file must be increased. Page file usage must match the guidelines provided in Microsoft KB2860880.


How assessment scores work

Performance Optimizer generates a score for most assessments run by server tasks.

The resulting scores can be viewed from the Performance Optimizer dashboard, and by using a McAfee ePO query or report. The score is a value between 0–10 with the lower scores indicating an issue that requires an action. Each assessment measures different criteria when calculating scores.

* Indicates that the threshold can be modified in the **Performance Optimizer: Runs assessments and calculates performance scores server task**.

Assessment	Definition	Calculation	Score	Score value threshold for action required
Agent Handler system distribution	Retrieves the total number of systems, Agent Handlers, and agents managed by each Agent Handler. Also calculates the ratio of agents to Agent Handlers.	$(1 - ((\# \text{ of systems mostly managed by a AH}) - (\text{total systems} / \text{total AHs})) / \text{total system}) * 10$ Example: $(1 - ((100,000) - (250,000 / 5)) / 250,000) * 10 = 8.0$	0-10	score < 9 *
ASCI settings	Retrieves the ASCII settings for all policies, and analyzes the potential number of agent-server communications per second.	10: (Number of Agents / ascii) <= 5 ASC/second 9: (Number of Agents / ascii) > 5 ASC/second 8: (Number of Agents / ascii) > 7.5 ASC/second 7: (Number of Agents / ascii) > 10 ASC/second 6: (Number of Agents / ascii) > 12.5 ASC/second 5: (Number of Agents / ascii) > 15 ASC/second 4: (Number of Agents / ascii) > 17.5 ASC/second 3: (Number of Agents / ascii) > 20 ASC/second 2: (Number of Agents / ascii) > 22.5 ASC/second 1: (Number of Agents / ascii) > 25 ASC/second 0: (Number of Agents / ascii) > 30 ASC/second	0-10	score < 9 *
Database CPU	Measures total CPU utilization and calculates scores based on comparisons.	Total CPU ≤ 50	10	score < 10
		Total CPU ≤ 75	9	
		Total CPU ≤ 85	8	
		Total CPU ≤ 90	4	
		Total CPU ≤ 95	2	
		Total CPU > 95	0	
Database Disk	Measures the remaining data files belonging to the McAfee ePO database or the system database tempdb. The score is adjusted if one of the data files satisfies these conditions.	% Remaining > 30	10	score ≤ 8
		% Remaining ≤ 30	8	
		% Remaining ≤ 15	4	
		% Remaining ≤ 5	0	
Data Memory	Measures the remaining memory on the database server and calculates a score based on these comparisons.	% Memory Remaining ≥ 50	10	score ≤ 8
		% Memory Remaining ≥ 25	8	

Assessment	Definition	Calculation	Score	Score value threshold for action required
		% Memory Remaining \geq 15	4	
		% Memory Remaining \geq 5	2	
		% Memory Remaining $<$ 5	0	
Database Table Disk Usage	<p>No calculation is done for this assessment because it validates a larger number of tables. The score is set to a default value of 10.</p> <div>  <p>For scores reflecting the remaining disk space available, see the "Database Disk" assessment section in this table.</p> </div>	No calculation	Default score is 10	No threshold for values because metrics vary too much across different environments.
Database and server configuration checks	<p>The scores is for this assessment is 10 or 0 because it represents configurations that must be implemented.</p> <p>The score is set to 0 if the assessment requires a change.</p>	No calculation	0 or 10	score = 0
Database backup	<p>A score of 0 indicates that a database backup hasn't occurred in the last 7 days.</p> <p>A database in full or bulk-logged recovery model receives a score of 0 if a transaction log backup hasn't occurred in the last 24 hours.</p>	No calculation	0	score = 0
Database blocking queries	<p>A score of 2 indicates that one of these conditions are met:</p> <ul style="list-style-type: none"> • Number of blocked SQL queries is greater than 5 • Average query wait time in seconds is greater than 30 • Maximum block depth is greater than 2 <p>A score of 10 is given if none of these conditions are met.</p>	No calculation	See definition	score \leq 2

Assessment	Definition	Calculation	Score	Score value threshold for action required
Database deadlock queries	A score of 2 indicates that the count of deadlocked queries is greater than 10 over the last 24 hours. A score of 10 indicates that this condition doesn't occur.	No calculation	Either 2 or 10	score \leq 2
Database file growth settings	The scores is for this assessment is 10 or 0 because it represents configurations that must be implemented. The score is set to 0 if the assessment requires a change.	No calculation	10 or 0	score = 0
Database file I/O statistics	No calculation is done for this assessment because the I/O activity and latencies are specific to each environment. The default score is 10.	No calculation	Default score is 10	No threshold for values because metrics vary too much across different environments.
Database file locations	The scores is for this assessment is 10 or 0 because it represents configurations that must be implemented. The score is set to 0 if the assessment requires a change.	No calculation	10 or 0	score = 0
Database index fragmentation	Reviews if one or more indexes are fragmented and provides the percentage.	% Fragmentation \geq 90	2	score \leq 8
		% Fragmentation \geq 50	4	
		% Fragmentation \geq 30	6	
		% Fragmentation \geq 20	8	
		% Fragmentation $<$ 20	10	
Database instance configuration settings	The scores is for this assessment is 10 or 0 because it represents configurations that must be implemented. The score is set to 0 if the assessment requires a change.	No calculation	10 or 0	score = 0
Database integrity check	Reviews if errors are returned from <code>DBCC CHECKDB</code> command. A score of 10 indicates that if there are no errors.	No calculation	10 or 0	score = 0

Assessment	Definition	Calculation	Score	Score value threshold for action required
Database server performance counters	The calculation for this assessment is not performed due to the large number of metrics collected. Each environment has different acceptable values. The default score for this assessment is 10. This assessment doesn't provide a calculation.	No calculation	Default score is 10	No threshold for values because metrics vary too much across different environments.
Database settings for AutoShrink, AutoClose, and Auto Update Statistics	The scores is for this assessment is 10 or 0 because it represents configurations that must be implemented. The score is set to 0 if the assessment requires a change.	No calculation	10 or 0	score = 0
Database table identity columns	Reviews if one or more identity columns used a high percentage of identity values that are already in use.	% Identity values used \geq 90	2	score \leq 8
		% Identity values used \geq 75	5	
		% Identity values used \geq 50	8	
		% Identity values used $<$ 50	10	
Duplicate systems	Gathers the total number of duplicate systems, and calculates the ratio of managed and unmanaged systems.	$(1 - (\# \text{ of duplicated systems}) / (\# \text{ of total systems})) * 10$	0–10	score $<$ 9 *
Orion Log Analyzer	Runs in the background; no calculated score.	No calculation	None	None
ePO Application Server Disk Analyzer	Provides a value between 0–10 reflecting the ratio between the used disk space and the total disk space.	$10 - ((\text{Total Space} - \text{Usable Space}) / \text{Total Space}) * 10$	0–10	score $<$ 2
ePO Application Server Garbage Collection Analyzer	Provides a value between 0–10 reflecting the ratio of the previous and current garbage collection duration.	$10 - (\text{Current GC Duration} / (\text{Prev GC Duration} * 5))$	0–10	score $<$ 5
ePO Application Server Java Memory Analyzer	Provides a value between 0–10 reflecting the ratio between the used memory in the Java Virtual Machine (JVM) and the overall memory allocated to the JVM.	$10 - (\text{Heap Memory Used} / \text{Heap Memory Committed}) * 10$	0–10	score $<$ 8

Assessment	Definition	Calculation	Score	Score value threshold for action required
ePO Application Server Operating System Analyzer	Reviews the CPU system and process loads. If the system CPU load is greater than 90% the score is 0. Otherwise, the score is a value between 0–10 reflecting the ratio between the process and system CPU load.	$10 - (\text{processCPULoad} / \text{systemCPULoad}) * 10$	0–10	score < 8
ePO Application Server Page File Analyzer	Collects information about page file usage on the McAfee ePO Application Server. Formula: Percentage of page file size in relation to physical memory = (Total MB Page File Size/Total Memory in MB)*100.0	Percentage of page file size in relation to physical memory < 25	2	score < 8
		Percentage of page file size in relation to physical memory < 50	4	
		Percentage of page file size in relation to physical memory < 75	6	
		Percentage of page file size in relation to physical memory < 100	8	
		Percentage of page file size in relation to physical memory = 100	10	
Inactive Agent Handlers	Retrieves the total number of active Agent Handlers and those that have not communicated with McAfee ePO in the number of hours you specified. Also analyzes the ratio of active to inactive Agent Handlers.	$(1 - (\# \text{ of inactive AHs}) / (\# \text{ of total AHs})) * 10$ Example: $(1 - (3 - 10)) * 10 = 7.0$	0–10	score < 9 *
Location of distributed repositories	Retrieves the location of the distributed repositories and compares it to the location of the Master Repository.	10: 0 distributed repository is located the same path of the master repository 0: 1+ distributed repository are located the same path of the master repository	0 or 10	score < 9 *
McAfee Agent packages in the Master Repository	Retrieves the list of packages in the Master Repository and analyzes the package version of the McAfee Agent.	10: current (5.0) 8: 1 version old (4.8) 6: 2 version old (4.6) 4: 3 version old (4.5) 0: 4 version old (4.0-)	0–10	score < 9 *

Assessment	Definition	Calculation	Score	Score value threshold for action required
McAfee Agent updates	Retrieves the list of distributed repositories and the number of agent updates performed from each repository. Also analyzes the repository distribution for agent updates.	$(1 - ((\# \text{ of systems on a single distributed repository}) - (\text{total systems} / \text{total distributed repository})) / \text{total systems}) * 10$ Example: $(1 - ((100,000) - (250,000 / 50)) / 250,000) * 10 = 6.2$	0-10	score < 9 *
McAfee Agent versions	Retrieves the number of agents, which are grouped by the agent version. Performance Optimizer analyzes the ratio of agents that are upgraded and not upgraded.	$1 - (\# \text{ of 4.5- Agents}) / (\# \text{ of total Agents}) * 10$ Example: $(1 - (45,000 / 100,000)) * 10 = 5.5$	0-10	score < 9 *
Number of daily threat events	Retrieves and analyzes the number of threat events received each day.	10: 0 – 1,000,000 events received daily 9: 1,000,001 – 2,000,000 events received daily 8: 2,000,001 – 3,000,000 events received daily 7: 3,000,001 – 4,000,000 events received daily 6: 4,000,001 – 5,000,000 events received daily 5: 5,000,001 – 6,000,000 events received daily 4: 6,000,001 – 7,000,000 events received daily 3: 7,000,001 – 8,000,000 events received daily 2: 8,000,001 – 9,000,000 events received daily 1: 9,000,001 – 10,000,000 events received daily 0: 10,000,001+ events received daily	0-10	score < 9 *

Assessment	Definition	Calculation	Score	Score value threshold for action required
Number of received threat events	Retrieves and analyzes the number of threat events by type.	10: 0 9: 1 eventID received over 100,000 8: 2 eventIDs received over 100,000 7: 3 eventIDs received over 100,000 6: 4 eventIDs received over 100,000 5: 5 eventIDs received over 100,000 4: 6 eventIDs received over 100,000 3: 7 eventIDs received over 100,000 2: 8 eventIDs received over 100,000 1: 9 eventIDs received over 100,000 0: 10+ eventIDs received over 100,000	0-10	score < 9 *
Number of threat events	Retrieves and analyzes the total number of reported threat events.	10: 0 – 1,000,000 threat events in database 9: 1,000,001 – 2,000,000 threat events in database 8: 2,000,001 – 3,000,000 threat events in database 7: 3,000,001 – 4,000,000 threat events in database 6: 4,000,001 – 5,000,000 threat events in database 5: 5,000,001 – 6,000,000 threat events in database 4: 6,000,001 – 7,000,000 threat events in database 3: 7,000,001 – 8,000,000 threat events in database 2: 8,000,001 – 9,000,000 threat events in database 1: 9,000,001 – 10,000,000 threat events in database 0: 10,000,001+	0-10	score < 9 *

Assessment	Definition	Calculation	Score	Score value threshold for action required
Server tasks — Completion status	Retrieves the completion status of each server task reported in the Server Task Log. Also analyzes the ratio of successful to failed tasks in the last 30 days.	$(1 - (\text{number of failed tasks in last 30 days} / \text{total tasks executed in last 30 days})) * 10$ Example: $(1 - (5 / 100)) * 10 = 9.5$	0-10	score < 9 *
Server tasks — Length of runtime	Retrieves and analyzes the duration of each server task reported in the Server Task Log.	10: 0 task running over 1 hour in last 30 days 9: 1 – 10 tasks running over 1 hour in last 30 days 8: 11 – 20 tasks running over 1 hour in last 30 days 7: 21 – 30 tasks running over 1 hour in last 30 days 6: 31 – 40 tasks running over 1 hour in last 30 days 5: 41 – 50 tasks running over 1 hour in last 30 days 4: 51 – 60 tasks running over 1 hour in last 30 days 3: 61 – 70 tasks running over 1 hour in last 30 days 2: 71 – 80 tasks running over 1 hour in last 30 days 1: 81 – 90 tasks running over 1 hour in last 30 days 0: 91+ tasks running over 1 hour in last 30 days	0-10	score < 9 *

Assessment	Definition	Calculation	Score	Score value threshold for action required
Server tasks — Schedule settings	Retrieves and analyzes the settings for scheduled server tasks.	10: 0 – 2 tasks running at the same time 9: 3 – 4 tasks running at the same time 8: 5 – 6 tasks running at the same time 7: 7 – 8 tasks running at the same time 6: 9 – 10 tasks running at the same time 5: 11 – 12 tasks running at the same time 4: 13 – 14 tasks running at the same time 3: 15 – 16 tasks running at the same time 2: 17 – 18 tasks running at the same time 1: 19 – 20 tasks running at the same time 0: 21+ tasks running at the same time	0–10	score < 9 *
Systems with an inactive McAfee Agent	Gathers the total number of systems where the McAfee Agent has not communicated with McAfee ePO in the number of days you specified, and calculates the ratio of systems with active agents to systems with inactive agents. The default number of days is 15. You can change this number as needed.	$(1 - (\# \text{ of inactive Agents}) / (\# \text{ of total systems})) * 10$ Example: $(1 - (6,000 / 250,000)) * 10 = 9.7$	0–10	score < 9 *

Assessment	Definition	Calculation	Score	Score value threshold for action required
Timestamp of daily logons	Retrieves and analyzes all user logons and logoffs during the hours you specified.	10: 0 – 10 user logins in a time window 9: 11 – 20 user logins in a time window 8: 21 – 30 user logins in a time window 7: 31 – 40 user logins in a time window 6: 41 – 50 user logins in a time window 5: 51 – 60 user logins in a time window 4: 61 – 70 user logins in a time window 3: 71 – 80 user logins in a time window 2: 81 – 90 user logins in a time window 1: 91 – 100 user logins in a time window 0: 101+ user logins in a time window	0-10	score < 9 *

Assessment	Definition	Calculation	Score	Score value threshold for action required
Timestamp of logons	Retrieves the list of user names and logon times. Also analyzes the number of daily logons.	10: 0 – 100 logins per day in last 7 days 9: 101 – 200 logins per day in last 7 days 8: 201 – 300 logins per day in last 7 days 7: 301 – 400 logins per day in last 7 days 6: 401 – 500 logins per day in last 7 days 5: 501 – 600 logins per day in last 7 days 4: 601 – 700 logins per day in last 7 days 3: 701 – 800 logins per day in last 7 days 2: 801 – 900 logins per day in last 7 days 1: 901 – 1000 logins per day in last 7 days 0: 1001+ logins per day in last 7 days	0–10	score < 9 *
Unmanaged systems	Gathers the total number of systems that aren't managed, and analyzes the ratio of managed systems to unmanaged systems.	$(1 - (\# \text{ of unmanaged systems}) / (\# \text{ of total systems})) * 10$	0–10	score < 9 *

3

Collecting and analyzing data

Performance Optimizer uses McAfee ePO features to collect and analyze data, and send notifications.

Contents

- ▶ *Collecting data on performance*
- ▶ *Server tasks and editable actions*
- ▶ *Sending notifications*
- ▶ *Default queries and when to use them*
- ▶ *Default dashboards*

Collecting data on performance

Performance Optimizer collects metric data by running server tasks from McAfee ePO.

When you install or upgrade Performance Optimizer, the product's server tasks are created and stored on the McAfee ePO server.

Each task:

- Monitors a specific aspect of your environment's health
- Runs independently
- Runs on a default schedule (hourly, daily, weekly) that you can configure to suit your environment

For example, the default schedule for the database integrity check is set to run weekly because in large database environments this check can take several hours. If it takes less time in your environment, you can change the default schedule to fit into your daily maintenance.

After you install or upgrade the tool, these Performance Optimizer tasks are available on the McAfee ePO server.

Each server task name starts with "Performance Optimizer:"

Server task	Default schedule
Analyze CPU and memory usage on the application and database servers	Hourly
Analyze database blocked queries, deadlock queries, and server performance counters	Daily
Analyze database index fragmentation and identity column usage	Daily
Analyze database integrity using DBCC CheckDB	Weekly
Analyze disk usage	Daily
Analyze ePO configuration, database configuration, and database backups	Daily
Purge assessment data	Daily

Server task	Default schedule
Start orion log analyzer	No default schedule
Stop orion log analyzer	No default schedule



An error message appears when a server setting requires a database user account.

Additional information

In McAfee ePO:

- Purging Performance Optimizer data is separate from other tasks that remove data. For example, the Purge Server Task Log action is separate.
- Default server task schedules are considered minimum schedules for establishing a baseline.

Server tasks and editable actions

Performance Optimizer: Analyze ePO configuration, database configuration, and database backups is the only server task that has additional configuration settings.

You can modify the action settings for this specific server task. On the Actions tab, select the actions you want the task to take.

These are the assessments that you can take.

Assessment	Description
McAfee Agent versions	Gathers the number of agents, which are grouped by the agent version, and analyzes the ratio of agents that are upgraded and not upgraded.
Systems with an inactive McAfee Agent	Gathers the total number of systems where the McAfee Agent has not communicated with McAfee ePO in the number of days you specified, and calculates the ratio of systems with active and inactive agents.
Unmanaged systems	Gathers the total number of systems that don't have computer properties, and analyzes the ratio of managed and unmanaged systems.
Duplicate systems	Gathers the total number of duplicate systems, and calculates the ratio of total systems to duplicate systems.
Agent Handler system distribution	Retrieves the total number of systems, Agent Handlers, and agents managed by each Agent Handler. Also calculates the ratio of agents to Agent Handlers on systems.
Inactive Agent Handlers	Retrieves the total number of active Agent Handlers and those that have not communicated with McAfee ePO in the number of hours you specified. Also analyzes the ratio of active to inactive Agent Handlers.
ASCI settings	Retrieves the ASCI settings for all policies, and analyzes the number of agent-server communications per second.
Number of threat events	Retrieves and analyzes the total number of reported threat events.
Number of received threat events	Retrieves and analyzes the number of threat events by type.
Number of daily threat events	Retrieves and analyzes the number of threat events received each day.
Server tasks – Schedule settings	Retrieves and analyzes the settings for scheduled server tasks.
Server tasks – Length of time	Retrieves and analyzes the duration of each server task reported in the Server Task Log.

Assessment	Description
Server tasks – Completion status	Retrieves the completion status of each server task reported in the Server Task Log. Also analyzes the ratio of successful to failed tasks in the number of days you specified.
McAfee Agent updates	Retrieves the list of distributed repositories and the number of agent updates performed from each repository. Also analyzes the repository distribution for agent updates.
Location of distributed repositories	Retrieves the location of the distributed repositories and compares it to the location of the Master Repository.
Timestamp of logons	Retrieves the list of user names and logon times in the number of days you specified. Also analyzes the number of daily logons in the last number of days you specified.
Timestamp of daily logons	Retrieves and analyzes all user logon and logout times during the hours you specified.
McAfee Agent packages in the Master Repository	Retrieves the list of packages in the Master Repository, and analyzes the package version of the McAfee Agent.

Sending notifications

Performance Optimizer uses Automatic Responses to send notifications when a specific condition is discovered.

The server tasks that collect metric data about the health of the database and McAfee ePO Application Server publish the collected data in an event object. These events trigger the Automatic Responses. Automatic Responses are disabled by default.

Each response includes preconfigured filter criteria. You can review the criteria for each response to make sure that it complies with the requirements of your target environment.

Each Automatic Response starts with "Performance Optimizer:"

Table 3-1 Performance Optimizer Automatic Responses

Automatic Response	Event type
A database disk drive is low on space	Database disk usage
A database file is configured to grow at a very small amount	Database settings for file growth
A database file is experiencing high IO latency	Database file I/O statistics
A database index is fragmented and would benefit from a rebuild operation	Database index fragmentation
A database table column is nearing the limit of its identity values	Database identity column usage
A disk drive on the ePO Application Server machine is low	Physical Disk usage of McAfee ePO Application Server
A query has been blocked for more than 5 minutes	Database blocking queries
Ensure a database backup has been taken within the last week	Database backup
High CPU usage on the database server	Database CPU usage
High CPU usage on the ePO Application Server machine	JVM Operating System MBean
High memory usage on the database server	Database memory usage
High memory usage on the ePO Application Server machine	JVM Memory MBean
OutOfMemoryError has occurred in the ePO Application Server	Log file alert for orion.log

Table 3-1 Performance Optimizer Automatic Responses *(continued)*

Automatic Response	Event type
The database files are on the same physical drive which could lead to slower IO performance	Database file locations
The database has a table that has become very large and may need to be moved to a separate disk drive	Database table disk usage
The database is currently configured to auto shrink, which will decrease performance	Database settings for auto shrink, auto close, and auto update statistics
The database server configuration has a setting that should be modified from the default	Database instance configuration
The database server has reported integrity errors	Database integrity check

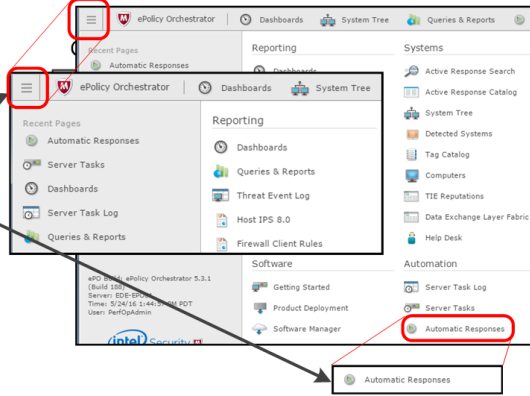
Sending text messages and emails

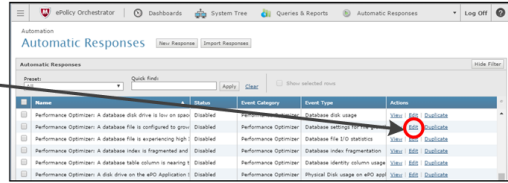
The default action for an Automatic Response is to send an email. You can also send text messages by specifying an email-to-text address such as 1234567890@<your mobile provider>. See your mobile phone provider's website for details about sending email to text.

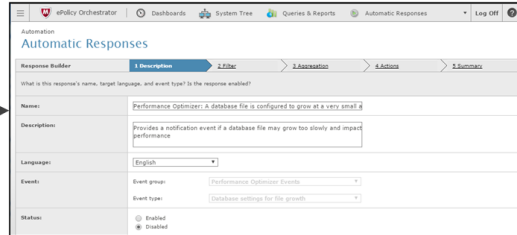
Configure a notification

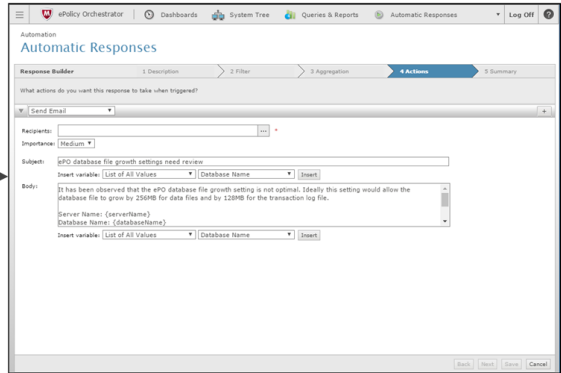
Configure a Performance Optimizer Automatic Response to send an email or text notification when a specific event occurs.

- 1 From the McAfee ePO console, select **Menu | Automatic Responses**.


- 2 Edit a Performance Optimizer Automatic Response.


- 3 In the Response Builder, edit the Description, Filter, and Aggregation settings.


- 4 On the Actions tab, enter the target email or phone number. Edit the subject and body of the message as needed.



Respond to a notification

If you receive an Automatic Response notification, review the recommendation on the dashboard.

- 1 Review the information provided in the notification.
- 2 Locate the dashboard that contains the relevant information for the notification, then review the trending graph for more details.

- 3 From the dashboard, select the item to drill down and view the recommendation.

For some notifications, you must review the Server Task Log to view the task that caused the notification. The Server Task Log page provides a search box to quickly locate the most recent instance of a task.

- 4 Take the recommended action.

Default queries and when to use them

Performance Optimizer includes many default queries that filter for specific metric data. The results are displayed in a trending graph or a summary listing.

Dashboards display queries for an overall picture of the metric data. While default queries are not editable, you can duplicate and change them. For example, if a query includes additional metrics, change the filter list to include that metric by name.

To increase the metric sampling interval, duplicate the query you want to change, then edit the filter criteria.

Each query name starts with "Performance Optimizer:"

Query name	Description
Assessment History	Displays the assessments that require action
Count of database queries that were deadlocked	Displays a trending chart that shows how many queries were deadlocked
Database backup findings	Lists the database recovery model and whether a database backup recently occurred
Database blocked queries	Displays a trending chart that shows statistics about blocked queries in the database
Database current size	Displays a total size of the database files
Database disk latency	Displays a trending chart that shows latencies for individual files on disk
Database disk remaining	Displays a trending chart that shows the amount of disk space remaining on the database server
Database disk usage	Displays a trending chart that shows disk usage and performance on the database server
Database integrity check findings	Indicates whether the most recent integrity check found errors in the database
Database performance counters	Lists some of the database performance counters
Database server configuration recommendations	Lists configuration settings and recommendations
Database server CPU usage	Displays a trending chart that shows CPU usage on the database server
Database server express edition has limitation of 10 GB database size	Indicates whether the express edition of the database server is in use
Database server express edition has limitation of 1 GB memory usage	Indicates whether the express edition of the database server is in use
Database server memory usage	Displays trending chart that shows memory usage on the database server
Database server memory usage (percent)	Displays trending chart that shows memory usage on the database server (percent)

Query name	Description
ePO Application Server CPU usage	Displays trending chart that shows CPU usage in the McAfee ePO Application Server
ePO Application Server JVM memory usage (heap)	Displays trending chart that shows memory usage in the McAfee ePO Application Server (heap)
ePO Application Server JVM memory usage (non-heap)	Displays trending chart that shows memory usage in the McAfee ePO Application Server (non-heap)
ePO Application Server JVM memory usage (percent)	Displays trending chart that shows memory usage in the McAfee ePO Application Server (percent)
ePO Application Server machine disk usage	Displays trending chart that shows disk usage on the McAfee ePO Application Server
Identity columns that are nearing their limit of values	Lists tables and identity columns that might run out of values
Indexes that need to be rebuilt during the next maintenance window	Lists indexes with fragmentation greater than 30% and must be rebuilt during the next maintenance window
Indexes that need to be reorganized during the next maintenance window	Lists indexes with fragmentation between 20%–30% and must be reorganized during the next maintenance window
List of tables by disk usage	Lists tables with their current disk usage
List of tables by row count	Lists tables with their current row counts
Listing of start/stop times for the Orion log analyzer	Displays a listing of all start and stop times to determine if the Orion Log Analyzer is still running
Summary	Displays the total number of assessments that are acceptable and require action
Recent exceptions and warnings from the ePO Application Server	Displays grouped summary listing of the recent exceptions and warnings from McAfee ePO extensions
Recent exceptions and warnings from the ePO Application Server (chart)	Displays bar chart listing of the recent exceptions and warnings from McAfee ePO extensions

Default dashboards

Several dashboards provide a quick view of collected data.

From a dashboard, select a query to drill down and view the recommendation. Dashboards can be duplicated so you can add custom queries.

Default dashboard	Description
Performance Optimizer: Assessment Summary	Displays the assessments that require action
Performance Optimizer: Database backups, integrity, and settings	Provides information about database server configuration, database integrity, and backups
Performance Optimizer: Database blocks and deadlocks	Provides information about blocked and deadlocked queries
Performance Optimizer: Disk usage	Displays trending charts that show current and previous disk usage on the database server and McAfee ePO Application Server
Performance Optimizer: Memory and CPU usage	Displays trending charts that show current and previous memory and CPU usage on the database server and McAfee ePO Application Server

Default dashboard	Description
Performance Optimizer: Database server performance counters	Displays information pulled from the performance counter made available through the database server
Performance Optimizer: Tables and indexes	Provides information about the current sizing and fragmentation for tables and indexes
Performance Optimizer: Top exceptions and warnings from the ePO Application Server	Provides information about recent exceptions and warnings from the McAfee ePO Application Server

Export information from the dashboard

Use the dashboard to export information and send it in an email.

Task

- 1 Log on to the McAfee ePO console as administrator.
- 2 Select **Menu | Dashboards**.
- 3 Use the arrow in the upper-left corner of the dashboard to select **Full Screen**.
- 4 Select **Options | Export Data**.
- 5 Specify the export information, select **Email files as attachments**, then click **Export**.

4

Monitoring the health of your environment

Use assessments to monitor specific areas of your McAfee ePO environment. These assessments allow you to discover potential problems before they occur, and make necessary changes to avoid outages.

Contents

- *Monitoring your database health*
- *Monitoring your McAfee ePO Application Server*

Monitoring your database health

Backing up your database is an essential part of your enterprise's security. Determine the frequency of backups according to your environmental and business needs.

Gathering backup information

Performance Optimizer doesn't schedule or run database backups. It does analyze the backup information that is maintained in the database server's system tables.

When you restore a previous database backup:

- Test a backup on a secondary database server to ensure it can be successfully restored.
- Perform database integrity checks on the restored copy using the `DBCC CHECKDB` command.
- Evaluate the backup schedule based on your tolerance for loss. For example, if your organization can afford to lose one week of data, run the backup schedule weekly. If the tolerance of loss is only one day, run the backup daily.

Performance Optimizer does not schedule and obtain database backups, but instead only analyzes the backup information maintained in the system tables of the database server. For more information, see Microsoft documentation on database backups.

For information about using a query to gather back up information, see *Database backups* in [KB87374](#).

Configuring database settings

The configuration of the database and SQL Server instance can impact performance, so it is important to evaluate the configuration parameters.

For information about using a query to view database settings, see *Auto Shrink, AutoClose, and Auto Update Statistics settings* in [KB87374](#).

Auto Shrink

The Auto Shrink database setting tells the server not to waste any space in the database files. The server automatically shrinks database files to the smallest usable amount of space, based on the amount of data in the tables.

While this functionality saves disk space, it can lead to significant performance issues because the shrink process moves data to unused parts of database files. This process reduces the overall size of the file itself. When the data moves, the index structures are fragmented because the data is no longer contiguous.



Best Practice: Disable Auto Shrink because index fragmentation leads to poor query performance.

Run this SQL command to disable Auto Shrink in your McAfee ePO database:

```
ALTER DATABASE [Enter your ePO database name here] SET AUTO_SHRINK OFF
```

AutoClose

When the last user disconnects from the database, the AutoClose database setting tells the server to close all connections and free up database resources. In the McAfee ePO server environment, this setting is unlikely to have a negative effect because the McAfee ePO Application Server maintains a constant database connection pool. However, when the AutoClose process runs, it removes data objects from the SQL Server buffer cache and removes query plans from the plan cache. The buffer cache in the memory and query plan cache also must repopulate with data and query plans, which causes a noticeable performance impact for larger databases. When the McAfee ePO Application Server tries to connect to the database, the SQL Server starts the database to make it available again online. To disable the AutoClose in your McAfee ePO database, run this SQL command:

```
ALTER DATABASE [Enter your ePO database name here] SET AUTO_CLOSE OFF
```



Best Practice: Disable the AutoClose database setting.

Auto Update Statistics setting

The Auto Update Statistics database setting tells the server to update statistical information about each table used in the database.

This can occur when the table is queried and the database server determines an appropriate query plan. The query plan optimizer then determines if the statistics about the number of rows and the types of data stored might be outdated for a particular table. These statistics naturally become outdated when data is changed in a table. A best practice is to allow the query plan optimizer to automatically update statistics. In rare instances where the calculation of statistics hinders performance, we recommend turning off Auto Update Statistics. For the McAfee ePO database environment, we recommend turning on Auto Update Statistics. To enable Auto Update Statistics in your McAfee ePO database, run this SQL Server command:

```
ALTER DATABASE [Enter your ePO database name here] SET AUTO_UPDATE_STATISTICS ON
```

File Growth

Performance Optimizer reviews the settings for file growth, then recommends what to do for files that might grow too frequently. If the database files grow too large too quickly, the database writers are blocked while the file is expanded. This blocking process leads to a performance decrease on the server for both data files and the transaction log file.

We recommend specifying that the database files grow in MB specified sizes. For example, for data files specify a fixed growth of 256 MB. For transaction log files specify a fixed growth of 128 MB. This is preferred over the growth in percentage, because the file growths are always the same predictable size instead of an ever-increasing amount that would result from using a percentage.

For information about using a query to gather file growth information, see "File growth" in [KB87374](#).



File locations

Performance Optimizer reviews the locations of the database and transaction log files to ensure that I/O is distributed across multiple devices. This benefits the performance because it allows SQL Server to request data for multiple objects, and the data is loaded in parallel by the separate I/O devices. The query used to determine file locations is similar to the query used for file growth. The PhysicalFileName column shows the drive location and is used to compare if multiple files are on the same I/O device.

We recommend separating the data files for the McAfee ePO database from the transaction log. Also, separate the tempdb data and transaction log files for optimal performance.

Database instance settings

Performance Optimizer reviews several key instance-level settings to recommend what you can do to improve application performance.

Database instance setting	Recommendation
affinity I/O mask	Make the default setting 0 so all CPUs can perform I/O.
affinity 64 I/O mask	Make the default setting 0 so all CPUs can perform I/O.
affinity 64 mask	Make the default setting 0 to use all CPUs.
backup compression default	Change the default setting to 1 so backup compression is used instance-wide.
blocked process threshold	Make the setting either = 0 or ≥ 5 so the deadlock monitor is not constantly running.
cost threshold for parallelism	Make the setting higher than 5 (for example, set it to 50) so the query optimizer doesn't use parallelism for small queries.
lightweight pooling	Make the default setting 0 because fiber mode scheduling in CPUs is rare.
locks	<p>Make the default setting 0 so that the maximum number of locks is not limited.</p> <div>  This recommendation is based on the assumption that memory can be increased. </div>
max degree of parallelism	<p>Make the default setting ≤ 8.</p> <div>  Best Practice: Set the "max degree of parallelism" to number of cores when a system has 8 cores or less. </div>
max server memory (MB)	Make the setting < 2147483647 and ≥ 8192 (8 GB), and leave 10% for OS.
max worker threads	Make the default setting 0 to avoid thread starvation.
network packet size (B)	Make the setting ≤ 8060 to avoid unexpected memory usage by SQL Server.

For information about using a query to view the current configured values, see *Database instance settings* in [KB87374](#).

Working with blocked queries

Microsoft SQL Server is a relational database, so blocking occurs while database sessions try to read and write data.

Blocking protects data to ensure that multiple processes can interact with the same data without having unexpected side effects. But, in some situations a blocking query can become a performance problem if that query can't complete in a timely manner. Make sure to evaluate how long the query is blocking a process, and whether it is hindering other processes from continuing.

Performance Optimizer identifies the blocking query details in the Server Task Log entry. The information includes:

- Session ID
- SQL text
- Depth of blocking
- Duration of the block

For information about blocking queries, see *Queries that are blocked or are blocking others* in [KB87374](#).

Stop the query session that is blocking others by running this command as the database system administrator:

```
KILL <session ID>
```

The <session ID> is available from the Server Task Log output.



Best Practice: Begin with closing the root blocking session because often the sessions blocked by that root process can complete.

Monitoring CPU usage

Monitoring systems for high CPU usage lets you know if a particular system requires more CPU resources.

It can also mean that a system is experiencing memory pressure and is paging information to disk. Compare CPU usage information to Server Task activities and other scheduled processes in McAfee ePO.



Best Practice: Reduce CPU contention by changing task schedules to run at different times.

For information about using a query to monitor CPU usage, see *Database server CPU usage* in [KB87374](#).

Working with deadlocked queries

Deadlocked queries indicate that two database sessions are trying to lock the same resources. SQL Server provides a deadlock monitor process that looks for sessions with scenarios that are deadlocked.

When this scenario happens, the deadlock monitor process:

- Selects a session to close and rolls back any changes.
- Chooses the session to rollback based on the lowest impact to the system and if a session sets a deadlock priority.

Performance Optimizer provides deadlock information so that the occurrences are trended over time.



Best Practice: If deadlocks occur often, schedule tasks to run at separate times to reduce content at the database level. Identify which products are part of the deadlock to verify that your data isn't corrupted.

Monitoring disk space

Disk space on the database server is important to monitor because the database write activity stops functioning if there is no disk space available.

Performance Optimizer monitors the used space, available space, and total space for the drives that the McAfee ePO database and tempdb database are using. When disk space is running low, allocate more space to the disk drives displayed for the database files.

SQL Server Express database can use 10 GB of space. When 10 GB is exceeded, SQL Server Express Edition displays an error message warning that the disk drive is out of space.



This error message means that SQL Server Express Edition database size reached the 10 GB limit.

For information about using queries to monitor the McAfee ePO and tempdb databases, see *Database server disk usage* in [KB87374](#).

Monitoring disk performance

Disk I/O performance is critical for database applications using Microsoft SQL Server. Performance Optimizer reports on the read and write activity for each I/O device in use, and the average latencies.



Best Practice: Monitor these items to determine if the I/O device is responding slowly to I/O requests. Use high performance storage, such as Solid State Drives (SSDs), for database file storage.

For information about using a query to monitor disk I/O performance, see *Database server disk performance* in [KB87374](#).

Monitoring messages with Orion Log Analyzer

The Orion Log Analyzer monitors messages that are written to the orion.log.

The Orion Log Analyzer examines the level when the log message is written. If the level is equal to or higher than the level specified in the Server Settings, the level is recorded in the McAfee ePO database. When the analyzer is running, CPU usage on the system hosting the McAfee ePO database and the Application Server process is impacted. The memory usage and disk I/O impact is minor as well.



Run the Orion Log Analyzer when troubleshooting errors, and stop during peak server usage times.

Using identity columns

Identity columns give you an integer-based value that can be automatically increased.

An *identity column* is a column (also known as a field) in a database table that is made up of values generated by the database. Products running within the McAfee ePO Application Server use identity columns to store information in the database tables.

Defining a column with an integer type that is less than the expected data set can result in errors. For example, if you use the `INTEGER` or `SMALLINT` data types and the amount of data exceeds 2,147,483,647 and 32,767, an error can occur and data can't write to that table.

For information about using a query to monitor identity column values, see *Database identity column usage* in [KB87374](#).

Monitoring index fragmentation

Index fragmentation occurs when data is changed in the table, making pages out of order.

Index fragmentation can impact performance when indexes are used to scan for rows requested by a query reader. Performance degradation occurs when the index scan requires that data is fetched from disk into memory before the query can process. For more information, search for *Detecting Index Fragmentation* on Microsoft's MSDN website.

Index fragmentation results in larger database backups, larger amounts of transaction log space, and more memory utilized to store and process the fragmented database pages.

For information about using a query to collect index fragmentation information, see *Database index fragmentation* in [KB87374](#).

Verifying database integrity

Validation of McAfee ePO database integrity is performed in multiple steps.

Performance Optimizer uses the SQL Server command `DBCC CHECKDB`. The `CHECKDB` command ensures validity of catalog information, disk space allocations, and table structures. This validation is critical for monitoring potential corruption that can occur in the database structures and files.

The validation output is printed to the Server Task Log. If errors are displayed, you can manually run the `DBCC CHECKDB` command with an option to repair the problem.



Best Practice: Restore from a database backup if corruption errors are printed to the Server Task Log.

Measuring memory usage

Memory usage in SQL Server is a critical measurement because data is only manageable if first moved from disk to memory.

SQL Server instances often require more memory. Performance can improve when SQL Server doesn't have to fetch data pages from disk and can access them from memory.



Best Practice: Add more memory if the usage is always near the limits of physical memory.

For information about using queries, see *Database server memory usage* and *Database server buffer cache memory usage* in [KB87374](#).



Best Practice: If another database is using most of the memory cache, move the McAfee ePO database to a separate database server.

Collecting server performance counters

Performance Optimizer collects the performance counters that are available through SQL Server.

These counters are similar to the Performance Monitor tool provided by Microsoft. Various categories of metrics create trending graphs and monitor in-depth features of SQL Server.

For information about viewing the query used to collect the performance counters, search for **SQL Server performance counters** on Microsoft's MSDN website.

Collecting disk usage and row counts

Collecting disk usage and row counts is helpful when troubleshooting an issue and determining growth patterns for a table in the McAfee ePO database.

This information is also useful when deciding if a table must move to a new I/O device using a different file group. For more information about the query used to collect disk usage and row counts, search for **SQL Server table disk usage** on the Microsoft website.

Monitoring your McAfee ePO Application Server

Resource usage of disk, memory, and CPU is collected at regular intervals. With these metrics, you can discover potential problems before they occur, and make necessary changes to avoid outages.

The McAfee ePO Application Server is the component that provides the McAfee ePO console. The McAfee ePO server and the system it runs on require monitoring that is similar to the database server, ensuring reliable performance and proactively resolving problems.

Monitoring disk usage with McAfee ePO Application Server

Monitor disk usage on the system that hosts the McAfee ePO Application Server.

Often this system also hosts an Agent Handler process and the McAfee ePO Event Parser. This system must not run out of disk space, so review the metrics regularly to ensure that space is sufficient. Here are common causes of excessive disk usage on the McAfee ePO Application Server:

- Event file accumulation for the McAfee ePO Event Parser
- Accumulation of MER files for troubleshooting
- Orion.log files that were configured for a larger size and contain multiple rollover copies
- Heap dump files from the Java Virtual Machine (JVM) that runs on the McAfee ePO server

Monitoring memory usage with McAfee ePO Application Server

Monitor memory usage from the Java Virtual Machine (JVM) that runs the McAfee ePO Application Server.

The JVM represents the set of memory that the McAfee ePO Application Server can use. The metrics describe both the *heap* (runtime objects) and *non-heap* (metadata and local method objects) utilization. Make adjustments as needed to increase the allocation memory.

The JVM memory setting is located in the Windows registry at this location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\MCAFEETOMCATSRV530\Parameters\Java\JvmMx
```

Before increasing the allocation memory to the JVM, make sure that the operating system has sufficient memory. It must retain about 10% of the available memory resources. If the same system is used for an Agent Handler and Event Parser, leave enough memory for those processes to function optimally.

For more information about the recommended memory settings for the JVM, see [KB71516](#).

Monitoring CPU usage with McAfee ePO Application Server

CPU usage is a critical performance metric to monitor. High CPU usage can cause slow logon times and delay page loads.

Performance Optimizer collects metrics to determine if high CPU usage is caused by the application server process or from other processes on the system. If other processes are using high CPU, review if there are any McAfee ePO components, such as an Agent Handler or Event Parser.

A

Best practices: Database server provisioning

When provisioning a server, follow these recommendations to minimize resource use and maximize performance.

Instant File Initialization process

Microsoft SQL Server initializes all files used for storing data. This initialization process can be a long-running task if the files are large. Enable the Instant File Initialization process on the McAfee ePO database server so that SQL Server does not use extra resources to initialize the data files.



When enabled, the Instant File Initialization process is only applicable for data files. The transaction log file can't use this feature because SQL Server mandates that the file is initialized, so that leftover file fragment data isn't interpreted incorrectly as valid transaction data.

Disk sector size

There are significant enhancements to hard drive read and write performance through the support of larger disk sector sizes. When using McAfee ePO databases, make sure that the appropriate sector (block) size is used for the I/O subsystem that services the database and transaction files for both the McAfee ePO database and the tempdb database. You must also verify that the partition alignment is optimal.

Windows Power Configuration setting

The Windows Power Configuration **Balanced** setting can have a negative impact on the McAfee ePO server systems that include the server hosting the database. To avoid this negative impact, change **Balanced** to **High Performance**.

Virtual Log File management

The McAfee ePO database transaction log contains internal management structures called *Virtual Log Files* (VLF).

We recommend that you keep the total count of VLFs to a small number. Each of these internal structures allow for transactions to change data in the database and to protect the database if an unexpected outage occurs.

For example, if a transaction is committed but not yet written to disk, a record of that transaction is listed in the transaction log. The record is contained inside a VLF structure in that file. If the SQL Server instance shutdown and restarted, the instance reads the transaction log and replays the committed transaction against the internal memory structures that hold data. The only record of the data change was in the transaction log.

It is also possible that a large number of VLFs (thousands and more) can cause a slowdown for normal write activity occurring in the database. This is because the number of internal structures in the transaction log is so high that SQL Server is forced to evaluate more conditions than it would if the number of VLFs were small.

To view the VLF information, run this SQL command as a sysadmin:

```
DBCC LOGININFO('ePO database name here')
```

The output of the command is a list of rows, each representing a VLF.

If the total count of rows is greater than 50:

- Change the growth parameters on the McAfee ePO database transaction log so that fewer VLFs are created.
- Rebuild the transaction log to reduce the number of VLFs.

For more information, search for **Reduce VLFs** on Microsoft's MSDN website.

B

Use external tools to analyze Performance Optimizer metrics

Third-party tools can extract the metrics provided by Performance Optimizer.

Follow these steps to enable the JMX interface on the McAfee ePO Application Server.

Task

For option definitions, click ? or Help in the interface.

- 1 From the McAfee ePO console, navigate to the Services Control Panel to stop the McAfee ePO Application Server.
- 2 Open the regedit.exe file and navigate to: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\MCAFEETOMCATSRV530\Parameters\Java\Options
- 3 Double-click the key to edit the value.
- 4 Scroll to the bottom of the page, then copy and paste the appropriate text:
 - For JMX configuration, use these values:

```
-Dcom.sun.management.jmxremote.port=8082
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djava.rmi.server.hostname=<enter the ePO server name or IP address here>
```



This configuration provides unsecured access to the metric data from JMX. Use the values listed below if SSL configuration is required.

- For SSL configuration, use these values:

```
-Dcom.sun.management.jmxremote.ssl=true
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl.need.client.auth=true
-Djava.rmi.server.hostname=<enter the ePO server name or IP address here>
-Djavax.net.ssl.keyStore=<location of keystore>
-Djavax.net.ssl.keyStorePassword=<enter keystore password here>
-Djavax.net.ssl.trustStore=<location of truststore>
-Djavax.net.ssl.trustStorePassword=<enter truststore password here>
```

The third-party tool must also specify the keystore and truststore information. For more information, see the tool's documentation.

- 5 From the Services Control Panel, restart the McAfee ePO Application Server.

When the JMX tool is enabled, see your third-party monitoring tool for information about how to connect to the JMX interface in McAfee ePO.

The name of the management bean is

com.intel.epa.jmx:name=performanceOptimizerMBean,type=PerformanceOptimizerMBean.

These operations are also available:

- reload()
- getNumericMetric(String metricsName, int count)
- getNumericMetric(String metricsName, String afterThisTime)
- getTextMetric(String metricsName, int count)
- getTextMetric(String metricsName, String afterThisTime)

The metrics collected by Performance Optimizer are made available as JMX attributes. The attribute names are the same as the metric names viewed in McAfee ePO.



Each additional metric that is monitored externally adds load to the McAfee ePO server. Monitor performance when configuring the set of metrics for external monitoring.

C **FAQ**

Here are answers to frequently asked questions.

See [KB87340](#).

