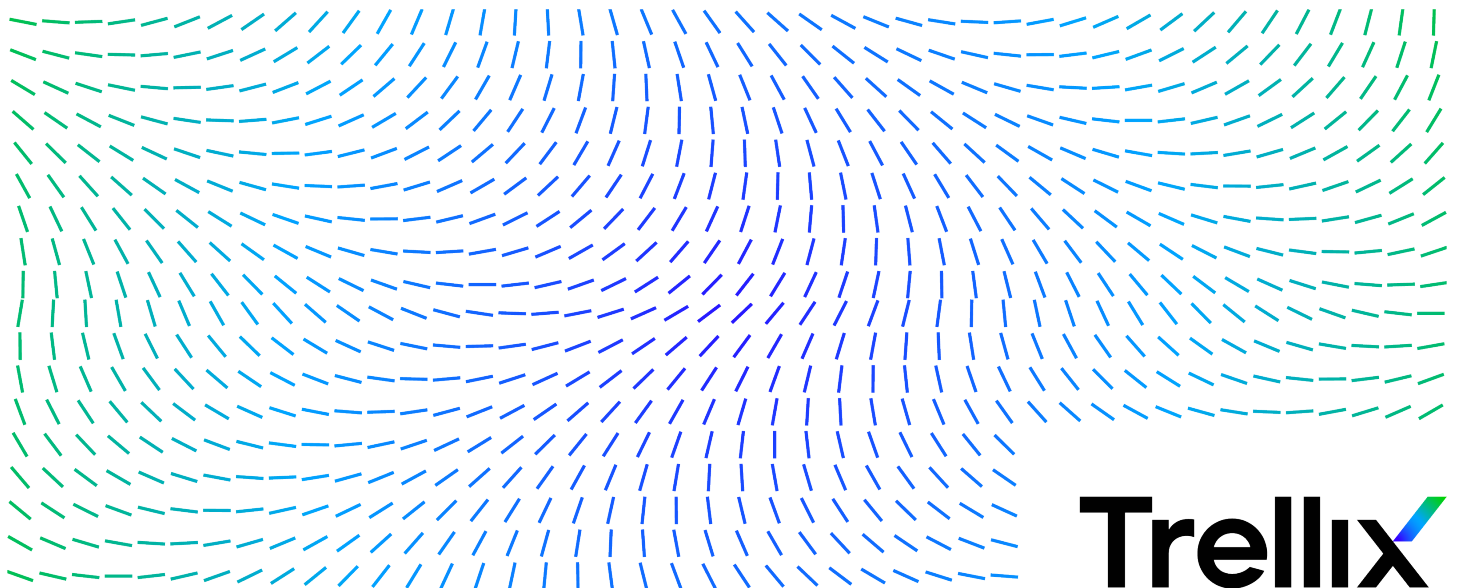


McAfee Endpoint Security Storage Protection 2.0.x Product Guide



Contents

Introduction.....	3
Endpoint Security Storage Protection overview.....	3
How Endpoint Security Storage Protection works.....	3
How scanning of NetApp filer works.....	3
How scanning of ICAP servers works.....	4
Product features.....	5
NetApp configuration.....	6
NetApp configuration on managed endpoints.....	6
Create a NetApp filer policy.....	6
Assign NetApp policies to managed systems.....	10
Configure NetApp scanner server with the NetApp filers (McAfee ePO managed).....	11
NetApp configuration on self-managed endpoints.....	11
Configure NetApp scanner server settings on self-managed endpoints.....	11
Configure NetApp scanner server with NetApp filers (self-managed environment).....	16
ICAP configuration.....	17
ICAP configuration on managed endpoints.....	17
Create an ICAP policy.....	17
Assign ICAP policies to managed systems.....	20
Configure the ICAP scanner server in the McAfee ePO environment with ICAP.....	21
ICAP configuration on self-managed endpoints.....	21
Configure the ICAP server scan settings on self-managed endpoints.....	22
Configure ICAP scanner server in self-managed environment with ICAP storage appliances.....	25
Monitoring Endpoint Security Storage Protection activity in your environment.....	26
Monitoring activity in ePO environment.....	26
View the threat event log in McAfee ePO.....	26
Endpoint Security Storage Protection dashboard and monitors.....	26
Queries and reports.....	30
Monitoring activity in a self-managed environment.....	32
Check the Event Log for recent activity.....	32
View the scan statistics.....	36
Frequently asked questions.....	38

Introduction

Endpoint Security Storage Protection overview

Endpoint Security Storage Protection (ENS SP) detects and removes viruses, malware, and other potentially unwanted software programs from your network-attached storage (NAS) devices.

Endpoint Security Storage Protection (ENS SP) is added to McAfee® Endpoint Security and expands its capability. The software performs remote scanning on NAS devices such as NetApp filers and Internet Content Adaptation Protocol (ICAP) storage appliances.

For a list of supported filer vendors, see [KB94811](#).

You can use Endpoint Security Storage Protection in two ways:

- As a managed product, using McAfee® ePolicy Orchestrator® (McAfee® ePO™) to install, manage, and enforce policies, and to use queries and dashboards for tracking activity and detections.
- As a module added to a standalone installation of McAfee® Endpoint Security Threat Prevention.

How Endpoint Security Storage Protection works

You can deploy this high-performance scanning solution on one or more Windows servers with multi-filer and multi-scanner configuration.

Endpoint Security Storage Protection supports two types of filers.

- NetApp filers — Filers that work on RPC-based protocols.
- ICAP — Filers that work on ICAP-based protocols.

Endpoint Security Storage Protection scans files in real time when they are accessed, stored, or modified on storage devices. For the ICAP protocol, the filer decides the appropriate action for infected files. For filers such as NetApp that work on RPC-based protocols, the McAfee Anti-Malware Engine takes appropriate actions.

For a list of supported filer vendors, see [KB94811](#).

How scanning of NetApp filer works

Endpoint Security Storage Protection performs scanning operation when a scan request is received from registered filers.

For Cluster-Mode scanning, Endpoint Security Storage Protection requires Clustered Data ONTAP Antivirus Connector software. The software must run on the same scanner server, where Endpoint Security Storage Protection is running. When the loop-back IP address (127.0.0.1) is added to the scanner server, the scanner establishes connection with the software.

Note

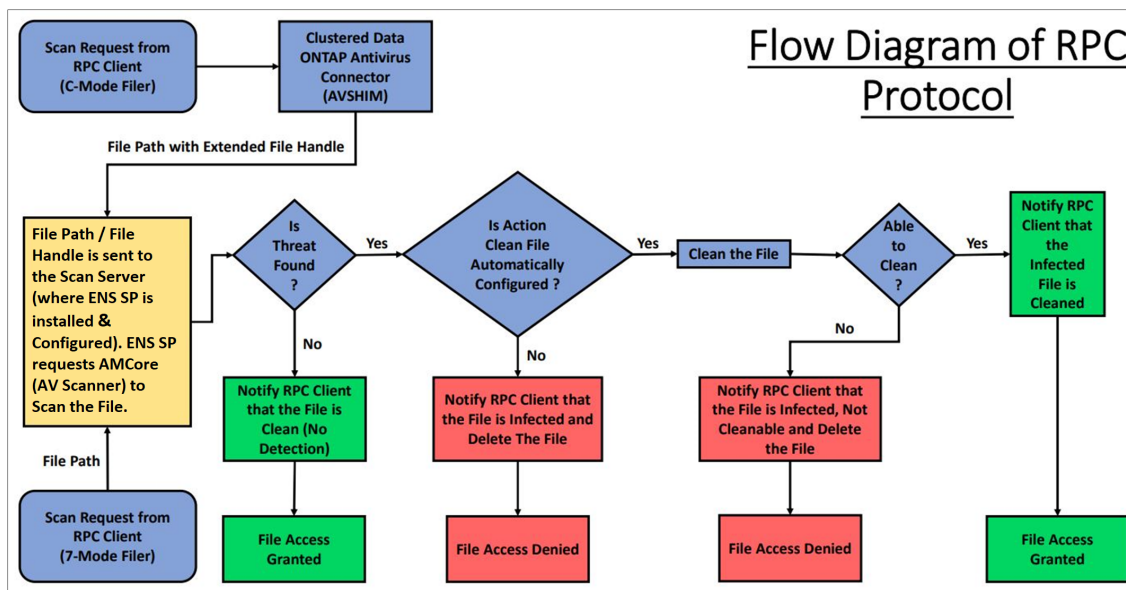
Endpoint Security Storage Protection requires Data ONTAP Antivirus Connector software from NetApp only if Data ONTAP 8.2.1 and later version filers configured in Cluster-Mode are connected.

For more information about adding the loop-back IP address to the scanner server, see [Configure NetApp filers scan settings \(managed or self-managed\)](#).

Note

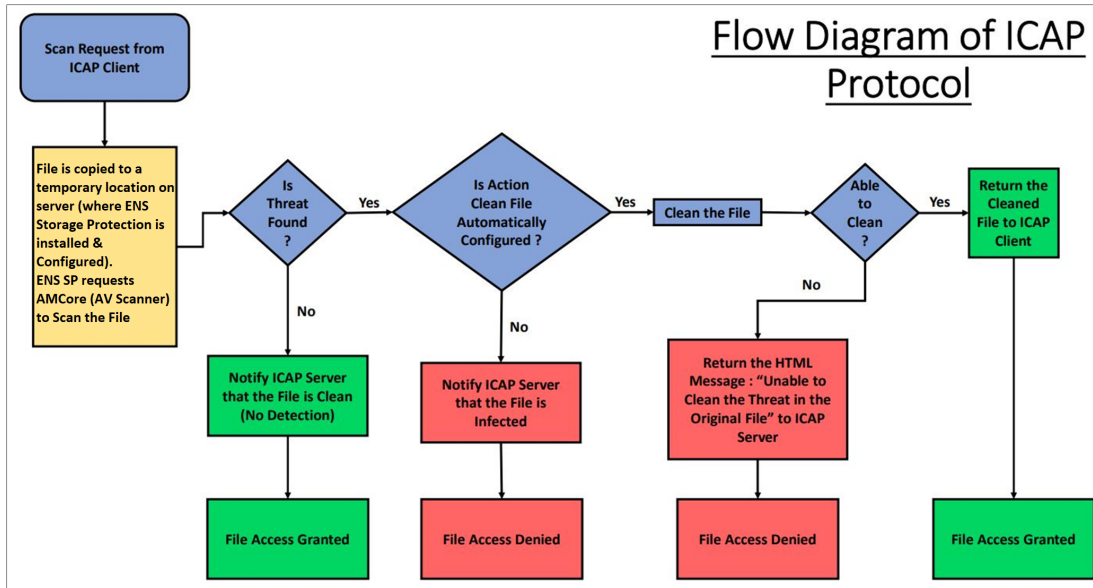
For more information about downloading Clustered Data ONTAP Antivirus Connector software and technical assistance, contact NetApp support.

This diagram presents an overview of the scanning process when reading, writing, and copying a file from or to the NetApp filer.



How scanning of ICAP servers works

Endpoint Security Storage Protection scans Internet Content Adaptation Protocol servers. The ICAP client is a Network Attached Storage (NAS) device.



Note

Endpoint Security Storage Protection adheres to RFC-3507 for ICAP scanning. As part of the ICAP use, ENS SP supports only Response Modification (RESPMOD) and Request Modification (REQMOD) commands. RESPMOD commands must also be in specific formatting as well. For more information on determining if an ICAP client meets the pre-requisites for communication with ENS SP, refer to [KB75543 \(Storage compatibility testing with ICAP-based NAS appliances\)](#).

Product features

The Endpoint Security Storage Protection features help you to configure, protect, and manage your network-connected storage devices.

- **On-Access Scan protection** — Protects your NAS devices from malware threats while files are being accessed, copied, or written to the server, including files hidden in compressed files. It protects data from malware before signatures are developed.
- **Quarantine** — Quarantines malware items (or suspected malware-related behavior) so that they can't be opened or executed.
- **Protection from spyware** — Detects hidden spyware programs that can track your Internet use, and can access business-critical data.
- **Central management of software** — Manages and controls systems centrally from a single management console using McAfee ePO.
- **Optimization of security and performance** — Deploys multi-scanner to multi-filer configurations that increase the load-balancing capacity and failover security.
- **Standard solution for multiple vendors** — Protects multiple storage systems and devices, and works on different storage environments and configurations.
- **Support for Clustered Data ONTAP 8.2.1 and later Cluster-Mode scanning** — Supports scanning of Clustered Data ONTAP <Version> using Clustered Data ONTAP Antivirus Connector, a NetApp product.

NetApp configuration

NetApp configuration on managed endpoints

Configure Endpoint Security Storage Protection with NetApp filers and scan the filers using the NetApp server.

1. Make sure Endpoint Security Storage Protection (Threat Prevention and Storage Protection modules) is installed on your managed systems.
2. Make sure that Clustered Data ONTAP Antivirus Connector software is installed and running on the systems where Endpoint Security Storage Protection is installed.
3. Create NetApp policies on McAfee ePO.
4. Assign the NetApp policies to the managed endpoints.
5. Configure the NetApp scanner server with the NetApp filers.

Create a NetApp filer policy

Create NetApp filer policies to define parameters for scanning file types, and to manage the list of NetApp filers connected to Endpoint Security Storage Protection.

Task


1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu** → **Policy** → **Policy Catalog**.
3. Select **Endpoint Security Storage Protection** as the product, then select **NetApp Policies** as the category.
4. Under **NetApp Policies**, edit **My Default**.

or


Click **New Policy**, type a name for the policy, then click **OK**.

5. On the **Filers** tab of the policy page, configure the filers list that the scan server protects, and create a user account with proper permissions such as, read, write, and backup for all filers:

In...	Define...
Filers list	<ul style="list-style-type: none">• Overwrite client filer list — Processes scan requests only for filers defined in the policy.• Filers — Use the plus and minus signs to add and remove filers.

In...	Define...
These settings apply to all filers	<ul style="list-style-type: none"> • Enable 'keep-alive' probes — To make sure that the filer and scanner-server are in communication. • Reset filer's clean file cache after each DAT or Engine update — Clears the cache of files already scanned after the scanner-server sends a DAT or engine update. This makes all files available for scanning with the latest DAT and engine files. <p> Tip: McAfee recommends that you enable these two options for all filers.</p>
Administrator account common to all filers	<p>Use the following account on all filers — If this option is not selected, you must set up an individual account for each locally installed Endpoint Security Storage Protection connection.</p> <ul style="list-style-type: none"> • To specify a user account with proper permissions (read, write, and backup) to all filers, enter the User name, Password and Confirm Password. • Domain — Domain name of the NetApp filer.

6. On the **Scan Items** tab, define the type of files to scan for malware threats and to detect unwanted programs:

In...	Define...
Scanning	<ul style="list-style-type: none"> • Enable Scanning — Enable or disable the NetApp scanner.
File types to scan	<ul style="list-style-type: none"> • All files — Scans all files regardless of the file extension. • Default + specified file types — Scans files with the default list of extension and the additional extension you specify. The default list is defined by the current DAT file. <ul style="list-style-type: none"> • Include files with no extension — Scans files that do not contain an extension. • Also scan for macros in all files — Scans for macro threats added in the files. • Specified file types only — Scans the list of user-specified extensions. You can also remove any extensions that you added previously. <p> Tip: You can add more file types by typing the file extensions separated by spaces.</p> <ul style="list-style-type: none"> • Include files with no extension — Scans files that do not contain an extension.

In...	Define...
Options	<ul style="list-style-type: none"> • Detect unwanted programs — Scans for unwanted programs installed on the server. • Decode MIME encoded files — Decodes the MIME encoded files. • Scan inside archives (e.g. .ZIP) and compressed executables — Scans compressed and archived executable files for threats.
Heuristics	<ul style="list-style-type: none"> • Find unknown unwanted programs and Trojans — Scans for unwanted programs and trojans on the server. • Find unknown macro threats — Scans for unknown macro threats.

7. On the **Exclusions** tab, configure the files and folders to exclude from scanning:

In...	Define...
What not to scan	<p>a. Click Add to specify the details for the exclusion:</p> <ul style="list-style-type: none"> • By pattern — Type the pattern in the text box. Separate multiple entries with a space. If needed, select Also exclude subfolders. • By file type — Type the file type in the text box. Separate multiple entries with space. • By file age — Select the access type (Modified, Created, or Accessed), then specify a minimum age in days. <p>b. Click Ok.</p> <p>You can edit, remove, or clear the exclusions.</p>
How to handle client exclusions	<ul style="list-style-type: none"> • Overwrite client exclusions (only exclude items specified in this policy) — Exclude the items specified in this policy. If this option is not selected, the exclusion items defined in the local system are used.

8. On the **Performance** tab, configure the scanning duration options to improve the performance.

In...	Define...
Maximum scan time (seconds)	Specifies the maximum scan time for files in seconds. The default scan time is 60 seconds. If a scan exceeds the time limit, the scan stops and logs a message. Allowed scan time is from 10-9999 seconds.
Number of anti-virus scan threads	Specifies the number of anti-virus scan threads. The default scan thread is 100 threads. Allowed scan thread is 1-800 threads.

9. On the **Actions** tab, define the primary and secondary actions to perform when a threat is detected:

In...	Define...
When a threat is found	<p>Perform this action first — Select the first action that you want the scanner to take when a threat is detected.</p> <ul style="list-style-type: none"> • Clean Files Automatically — The scanner tries to remove the detected threat from the file. • Delete Files Automatically — The scanner deletes files with potential threats as soon as it detects them. • Continue Scanning — A clean or delete action is not attempted on the threatened file. The filer is notified of the threat and the action is logged. <p>If the first action fails, then perform this action — Select the next action you want the scanner to take if the first action fails.</p> <ul style="list-style-type: none"> • Continue Scanning — A clean or delete action is not attempted on the threatened file. The filer is notified of the threat and logged. • Delete Files Automatically — The scanner deletes files with potential threats as soon as it detects them.
When an unwanted program is found	<p>Perform this action first — Select the first action that you want the scanner to take when an unwanted program is detected.</p> <ul style="list-style-type: none"> • Clean Files Automatically — The scanner tries to remove the detected threat from the file. • Delete Files Automatically — The scanner deletes files with potential threats as soon as it detects them. • Continue Scanning — A clean or delete action is not attempted on the infected file. The filer is notified of the threat and logged. <p>If the first action fails, then perform this action — Select the next action you want the scanner to take if the first action fails.</p>

In...	Define...
	<ul style="list-style-type: none"> • Continue Scanning — A clean or delete action is not attempted on the threatened file. The filer is notified of the threat and logged. • Delete Files Automatically — The scanner deletes files with potential threats as soon as it detects them.

10. On the **Reports** tab, configure these log activities preferences:

In...	Define...
Activity log	<ul style="list-style-type: none"> • Enable scan activity logging — Enables ICAP's scan activity logs in the default file location. Default log file location is as per the Endpoint Security Common policy.
Log file size	<ul style="list-style-type: none"> • Limit the size of log file — Enable to provide the maximum log file size. • Maximum log file size — Sets the maximum size of the log file in MB. Allowed log file size is 1–999 MB.
Log file format	Defines the log file format such as ANSI, Unicode UTF8, or Unicode UTF16.
What to log in addition to scanning activity	<ul style="list-style-type: none"> • Session settings — Logs the session details. • Session summary — Logs the session summary. • Failure to scan encrypted files — Logs the scan failure details for encrypted files.

11. Click **Save**.



Tip

For best practices about how to configure Endpoint Security Storage Protection settings to support NetApp filers in Cluster-Mode, see the [KB84086](#) (Cluster-Mode).

Assign NetApp policies to managed systems

After you create or modify the NetApp policies, assign them to the McAfee ePO managed systems.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu** → **Systems** → **System Tree**.
3. Click **Systems** tab, then select a group under **System Tree**.
4. In the **Assigned Policies** tab, select Endpoint Security Storage Protection from the **Product** list, select the NetApp policy, then click **Edit Assignment**.
5. Select appropriate inheritance options, select the policy to assign, then click **Save**.
6. In the **System Tree** tab, select a group or systems, then click the **Wake Up Agents**.
7. In the **Force policy update**, select **Force complete policy and task update** and click **OK**.

The policy is now assigned to the endpoints. To check the policy is assigned to the endpoints, open the Endpoint Security Storage Protection settings and confirm.

Configure NetApp scanner server with the NetApp filers (McAfee ePO managed)

You can scan the files on filers for viruses, malware, and other security threats by integrating Endpoint Security Storage Protection with NetApp filer through the Remote Procedure Protocol (RPC).

Before sending files to be scanned on the NetApp scanner server, configure the scanner server details (server where the ENS SP is installed) in your Clustered Data ONTAP Antivirus Connector software. For more information about how to configure the NetApp scanner server details with Data ONTAP, refer the respective NetApp filer guide.

After the NetApp scanner server scans the file, it informs the NetApp filer whether the file is a threat and then repairs the malicious file. All generated events are sent to McAfee ePO and it can be reviewed under **Threat Event Log**.

NetApp configuration on self-managed endpoints

Configure Endpoint Security Storage Protection with NetApp filers and scan the filers using the NetApp scanner server.

1. [Make sure Endpoint Security Storage Protection \(Threat Prevention and Storage Protection modules\) is installed on your systems.](#)
2. Make sure that Clustered Data ONTAP Antivirus Connector software is installed and running on the systems where Endpoint Security Storage Protection is installed.
3. [Configure NetApp scanner server settings.](#)
4. [Configure NetApp scanner server with NetApp filers.](#)

Configure NetApp scanner server settings on self-managed endpoints


Configure the NetApp filer AV scanner options such as, add filers, define file types to scan or exclude, and define actions for threat items. These configurations are applied to the NetApp filers that are connected to Endpoint Security Storage Protection.

Before you begin

Make sure that Clustered Data ONTAP Antivirus Connector software is installed and running on the endpoint to connect the scanner server to the Cluster-Mode filer.


To verify this, on the Windows taskbar, click **Start** → **Control Panel** → **Administrative Tools** → **Services**, then double-click **ONTAP AV Connector**. The status of the service appears as **Running**.

Task

- 1. Open the Endpoint Security Client.
- 2. On the top-right corner, click  and then select **Settings**.
- 3. On the left pane, click **Storage Protection**.
- 4. On the top-right corner, click **Show Advanced**.
- 5. Under **NETAPP Filer**, select **Enable NetApp Filler** to enable the NetApp scanner.
- 6. In the **Connections** section, configure the filers list that the scan server protects, and create a user account with proper permissions such as, read, write, and backup for all filers:

In...	Define...
IP Address	<p>Add the IP address of the NetApp filers.</p> <ul style="list-style-type: none">• Default Administrator Account<ul style="list-style-type: none">• To specify a user account with proper permissions (read, write, and backup) to all filers, enter the User name, Password, and Confirm Password.• Domain — Domain name of the NetApp filer. <p>Test Connection – Click to check the filer connection by providing the credentials.</p> <ul style="list-style-type: none">• Enable 'keep-alive' probes — To make sure that the filer and scanner-server are in communication.• Reset filer's clean file cache after each DAT or Engine update — Clears the cache of files already scanned after the scanner-server sends a DAT or engine update. This makes all files available for scanning with the latest DAT and engine files.

- 7. In the **Scan Items** section, define the type of files to scan for malware threats and to detect unwanted programs:

In...	Define...
File Types to Scan	<ul style="list-style-type: none"> • All Files — Scans all files regardless of the file extension. • Default + additional file types — Scans files with the default list of extension and the additional extension you specify. The default list is defined by the current DAT file. <ul style="list-style-type: none"> • Also scan for macros in all files — Scans for macro threats added in the files. • Specified file types only — Scans the list of user-specified extensions. You can also remove any extensions that you added previously. <p> Tip: You can add more file types by typing the file extensions separated by spaces.</p> <ul style="list-style-type: none"> • Include files with no extension — Scans files that do not contain an extension.
Options	<ul style="list-style-type: none"> • Detect Unwanted Programs — Scans for unwanted programs installed on the server. • Scan inside Archives (e.g. .ZIP) — Scans compressed and archived executable files for threats. • Decode MIME encoded files — Decodes the MIME encoded files.
Heuristics	<ul style="list-style-type: none"> • Find unknown program threats — Scans for unwanted programs and trojans on the server. • Find unknown macro threats — Scans for unknown macro threats.

8. In the **Exclusions** section, click **Add** to configure the files and folders to exclude from scanning:

In...	Define...
What to exclude	<ul style="list-style-type: none"> • File name or path (can include* or wildcards) — Provide the file name or browse the file. If needed, select Also exclude subfolders. • File type (can include the ? wildcards)— Type the file type. Separate multiple entries with space. • File age — Select the access type (Modified, Created, or Accessed), then specify a minimum age in days.
When to exclude	<p>When writing to disk or reading from disk —</p> <p>When performing file write operation, it excludes the files given in What to exclude.</p>

In...	Define...
	<p>When reading from disk — When performing file read operation, it excludes the files given in What to exclude.</p> <p>When writing to disk or reading from disk — When performing file read or write operation, it excludes the files given in What to exclude.</p>

9. In the **Performance** section, configure the scanning duration options to improve the performance:

In...	Define...
Maximum Scan Time (seconds)	Specify the maximum scan time for files in seconds. The default scan time is 60 seconds. If a scan exceeds the time limit, the scan stops and logs a message. Allowed scan time is from 10–9999 seconds.
Number of Scan Threads	Specify the number of antivirus scan threads. The default scan thread is 100 threads. Allowed scan thread is 1–800 threads.

10. In the **Actions** section, define the primary and secondary actions to perform when a threat is detected:

In...	Define...
Threat Detection First Response	<p>Select the first action that you want the scanner to take when a threat is detected.</p> <ul style="list-style-type: none"> • Clean — The scanner tries to remove the detected threat from the file. • Delete — The scanner deletes files with potential threats when it detects them. • Continue Scanning — A clean or delete action is not attempted on the threatened file. The filer is notified of the threat and the action is logged.
If the first response fails	<p>Select the next action if the first action fails.</p> <ul style="list-style-type: none"> • Delete — The scanner deletes files with potential threats as soon as it detects them. • Continue Scanning — A clean or delete action is not attempted on the threatened file. The filer is notified of the threat and logged.
Unwanted Programs first response	<p>Select the first action that you want the scanner to take when an unwanted program is detected.</p> <ul style="list-style-type: none"> • Clean — The scanner tries to remove the detected threat from the file. • Delete — The scanner deletes files with potential threats when it detects them.

In...	Define...
	<ul style="list-style-type: none"> • Continue Scanning — A clean or delete action is not attempted on the malicious file. The filer is notified of the threat and logged.
If the first response fails	<p>Select the next action you want the scanner to take if the first action fails.</p> <ul style="list-style-type: none"> • Delete — The scanner deletes files with potential threats when it detects them. • Continue Scanning — A clean or delete action is not attempted on the threatened file. The filer is notified of the threat and logged.

11. In the **Reports** section, configure these log activities preferences:

In...	Define...
Log Files	<ul style="list-style-type: none"> • Enable Scanner Activity logging — Enables NetApp scan activity logs in the default file location. Default log file location is according to the Endpoint Security Common policy. • Limit log file size (MB) — Enable to set the maximum log file size. Allowed log file size is 1–999 MB.
Log File Format	Select the log file format such as ANSI, Unicode UTF8, or Unicode UTF16.
What to log, in addition to scanning activity	<ul style="list-style-type: none"> • Session Settings — Logs the session details. • Session Summary — Logs the session summary. • Failure to scan encrypted files — Logs the scan failure details for encrypted files.

12. Click **Apply** to save the configuration.



Tip

You can view the filer connection status from the scan statistics page. For more information, see [View filers scan statistics](#).



Tip

For best practices about how to configure Endpoint Security Storage Protection settings to support NetApp filers in Cluster-Mode, see the [KB84086](#) (Cluster-Mode).

Configure NetApp scanner server with NetApp filers (self-managed environment)

You can scan the files on filers for viruses, malware, and other security threats by integrating Endpoint Security Storage Protection with NetApp filer through the Remote Procedure Protocol (RPC).

Before sending files to be scanned on the NetApp scan server, configure the scan server details (server where the ENS SP is installed) in your Clustered Data ONTAP Antivirus Connector software. For more information about how to configure the NetApp scanner server details with Data ONTAP, refer the respective NetApp filer guide.

After the NetApp scanner server scans the file, it informs the NetApp filer whether the file is a threat and it repairs the malicious file. All generated events are sent to **Event Log**.

ICAP configuration

ICAP configuration on managed endpoints

Configure Endpoint Security Storage Protection with ICAP storage appliances and scan the storage appliances using the ICAP scan server (server where ENS SP is installed).

- 1. Make sure Endpoint Security Storage Protection (Threat Prevention and Storage Protection modules) is installed on your systems.
- 2. Create ICAP policies.
- 3. Assign the ICAP policies to the managed systems.
- 4. Configure ICAP scanner server with ICAP storage appliances.



Note

Endpoint Security Storage Protection adheres to RFC-3507 for ICAP scanning. As part of the ICAP use, ENS SP supports only Response Modification (RESPMOD) and Request Modification (REQMOD) commands. RESPMOD commands must also be in specific formatting as well. For more information on determining if an ICAP client meets the pre-requisites for communication with ENS SP, refer to [KB75543 \(Storage compatibility testing with ICAP-based NAS appliances\)](#).

Create an ICAP policy

Create ICAP server scan policies to define the file types to be scanned, and to manage the list of ICAP appliances connected to Endpoint Security Storage Protection.



Task

- 1. Log on to the McAfee ePO server as an administrator.
 - 2. Click **Menu** → **Policy** → **Policy Catalog**.
 - 3. Select **Endpoint Security Storage Protection** as the product, then select **ICAP Policies** as the category.
 - 4. Under **ICAP Policies**, edit **My Default**.
- or
- Click **New Policy**, type a name for the policy, then click **OK**.
- 5. On the **Connections and Server** tab, configure IP addresses of the storage that can accept ICAP scan requests, the bind address (the IP address of the computer where Endpoint Security Storage Protection is installed), and the port number:

In...	Define...
Connection list	Specify the ICAP server configuration and the list of IP addresses to accept connections from

In...	Define...
	<ul style="list-style-type: none"> • Overwrite client's connection list — Overrides the client list of IP addresses and accept ICAP requests only from the listed IP address. • Accept connections and scan requests from these IP addresses only — Defines the list of IP addresses for which connections and scan requests can be accepted. • IP Address — Provide the IP address of the storage appliance. Use the plus and minus signs to add and remove IP address.
ICAP Server Configuration	<ul style="list-style-type: none"> • Overwrite ICAP server configuration on each client — Overrides the server configuration on each client. • Bind address — Provide the IP address of the scan server where Endpoint Security Storage Protection is installed. • Port number - Provide the port number or use the default (1344).

6. On the **Scan Items** tab, configure the file types to scan, detect for unwanted programs:

In...	Define...
Scanning	Enable Scanning — Enable or disable the ICAP scanner.
File types to scan	<ul style="list-style-type: none"> • All files — Scans all files regardless of the file extension. • Default + specified file types — Scans default and specified files. <div>  Tip: You can add more file types by typing the file extensions separated by spaces. </div> <ul style="list-style-type: none"> • Include files with no extension — Scans files that do not contain an extension. • Also scan for macros in all files — Scans for macros added in the file. • Specified file types only — Scans only files you specify. <div>  Tip: You can add more file types by typing the file extensions separated by spaces. </div> <ul style="list-style-type: none"> • Include files with no extension — Scans files that do not contain an extension.
Options	<ul style="list-style-type: none"> • Detect unwanted programs — Scans for unwanted programs installed on the server.

In...	Define...
	<ul style="list-style-type: none"> • Decode MIME encoded files — Decodes the MIME encoded files. • Scan inside archives (e.g. .ZIP) and compressed executables — Scans the compressed and archived executable file for threats.
Heuristics	<ul style="list-style-type: none"> • Find unknown unwanted programs and Trojans — Scans for unwanted programs and trojans on the server. • Find unknown macro threats — Scans for unknown macro threats.

7. On the **Performance** tab, configure the scanning duration options to improve performance.

In...	Define...
Maximum scan time (seconds)	Specifies the maximum scan time for files in seconds. The default scan time is 60 second. If a scan exceeds the time limit, the scan stops and logs a message. Allowed scan time is from 10–9999 seconds.
Number of anti-virus scan threads	Specifies the number of antivirus scan threads. The default scan thread is 100 threads. Allowed scan thread is 1-800 threads.

8. On the **Actions** tab, define the primary and secondary action to perform when a threat is detected:

In...	Define...
When a threat is found	<ul style="list-style-type: none"> • Perform this action first — Select the first action that you want the scanner to take when a threat is detected. <ul style="list-style-type: none"> • Clean File Automatically — Cleans the item that contains a threat then Continue Scanning as secondary action. • Continue Scanning — Continues scanning without taking any action when a threat is found. • If the first action fails, then perform this action — Select the next action you want the scanner to take if the first action fails. <ul style="list-style-type: none"> • Continue Scanning — Continue scanning when a threatened file is detected.

In...	Define...
When an unwanted program is found	<ul style="list-style-type: none"> • Perform this action first — Select the first action that you want the scanner to take when a threat is detected. • Clean File Automatically — Cleans the item that contains threat then Continue Scanning as secondary action. • Continue Scanning — Continues scanning without taking any action when a threat is found.

9. On the **Reports** tab, configure these log activities preferences:

In...	Define...
Activity log	<ul style="list-style-type: none"> • Enable scan activity logging — Enables ICAP's scan activity logs in the default file location. Default log file location is as per the Endpoint Security Common policy.
Log file size	<ul style="list-style-type: none"> • Limit the size of log file — Enable to provide the maximum log file size. • Maximum log file size — Sets the maximum size of the log file in MB. Allowed log file size is 1–999 MB.
Log file format	Defines the log file format such as ANSI, Unicode UTF8, or Unicode UTF16.
What to log in addition to scanning activity	<ul style="list-style-type: none"> • Session settings — Logs the session details. • Session summary — Logs the session summary. • Failure to scan encrypted files — Logs the scan failure details for encrypted files.

10. Click **Save**.



Tip

For best practices about how to configure ICAP settings for Endpoint Security Storage Protection, see [KB81933](#).

Assign ICAP policies to managed systems

After you create or modify the ICAP policies, assign them to the McAfee ePO managed systems.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu** → **Systems** → **System Tree**.
3. Click **Systems** tab, then select a group under **System Tree**.
4. In the **Assigned Policies** tab, select Endpoint Security Storage Protection from the **Product** list, select the NetApp policy, then click **Edit Assignment**.
5. Select appropriate inheritance options, select the policy to assign, then click **Save**.
6. In the **System Tree** tab, select a group or systems, then click the **Wake Up Agents**.
7. In the **Force policy update**, select **Force complete policy and task update** and click **OK**.
The policy is now assigned to the endpoints. To check the policy is assigned to the endpoints, open the Endpoint Security Storage Protection settings and confirm.

Configure the ICAP scanner server in the McAfee ePO environment with ICAP

You can scan the files on ICAP storage appliances for viruses, malware, and other security threats by integrating with Endpoint Security Storage Protection through the Internet Content Adaptation Protocol (ICAP).

Before you send files to be scanned on an ICAP scanner server, configure the scanner server details (server where the ENS SP is installed) in your ICAP storage appliances. For more information about how to configure the ICAP scanner server, refer to the respective ICAP storage appliance guide.

Note

Endpoint Security Storage Protection adheres to RFC-3507 for ICAP scanning. As part of the ICAP use, ENS SP supports only Response Modification (RESPMOD) and Request Modification (REQMOD) commands. RESPMOD commands must also be in specific formatting as well. For more information on determining if an ICAP client meets the pre-requisites for communication with ENS SP, refer to [KB75543 \(Storage compatibility testing with ICAP-based NAS appliances\)](#).

After an ICAP scanner server scans the file, it informs the ICAP storage appliance whether the file is a threat according to ICAP 1.0 standards. The ICAP scanner server repairs the malicious file based on the ICAP storage appliance's configuration. All generated events are sent to McAfee ePO and it can be reviewed under **Threat Event Log**.

ICAP configuration on self-managed endpoints

Configure Endpoint Security Storage Protection with ICAP storage appliances and scan the storage appliances using the ICAP scanner server (server where ENS SP is installed).

1. [Make sure Endpoint Security Storage Protection \(Threat Prevention and Storage Protection modules\) is installed on your systems.](#)
2. [Configure ICAP scanner server settings.](#)

3. Configure ICAP scanner server with ICAP storage appliances.



Note

Endpoint Security Storage Protection adheres to RFC-3507 for ICAP scanning. As part of the ICAP use, ENS SP supports only Response Modification (RESPMOD) and Request Modification (REQMOD) commands. RESPMOD commands must also be in specific formatting as well. For more information on determining if an ICAP client meets the pre-requisites for communication with ENS SP, refer to [KB75543 \(Storage compatibility testing with ICAP-based NAS appliances\)](#).

Configure the ICAP server scan settings on self-managed endpoints



Configure the server connection for scan requests, file types to scan or exclude, action for threat items, and log settings.

Task

- 1. Open the Endpoint Security Client.
- 2. On the top-right corner, click and then select **Settings**.
- 3. On the left pane, click **Storage Protection**.
- 4. On the top-right corner, click **Show Advanced**.
- 5. Under **ICAP Scanner**, select **Enable ICAP Scanner** to enable the ICAP scanner.
- 6. In the **Connections** section, configure IP addresses of the storage that can accept ICAP scan requests, the bind address (the IP address of the endpoint where Endpoint Security Storage Protection is installed), and the port number:

In...	Define...
Accept scan request from these ICAP Clients only	Enable to configure the list of ICAP storage appliances that the scan server protects. IP Address — Add the IP address of the ICAP storage appliances.
ICAP Server Configuration	Bind address — Provide the IP address of the scan server where Endpoint Security Storage Protection is installed. Port — Provide the port number or use the default (1344).

- 7. In the **Scan Items** section, configure the file types to scan, detect for unwanted programs:

In...	Define...
File Types to Scan	<ul style="list-style-type: none"> • All files — Scans all files regardless of the file extension. • Default + additional file types — Scans default and specified files. <p> Tip: You can add more file types by typing the file extensions separated by spaces.</p> <ul style="list-style-type: none"> • Also scan for macros in all files — Scans for macros added in the file. • Specified file types only — Scans only files you specify. <p> Tip: You can add more file types by typing the file extensions separated by spaces.</p> <ul style="list-style-type: none"> • Include files with no extension — Scans files that do not contain an extension.
Options	<ul style="list-style-type: none"> • Detect Unwanted Programs — Scans for unwanted programs installed on the server. • Scan Inside Archives (e.g. .ZIP) — Scans the compressed and archived executable file for threats. • Decode MIME encoded files — Decodes the MIME encoded files.
Heuristics	<ul style="list-style-type: none"> • Find unknown program threats — Scans for unwanted programs and trojans on the server. • Find unknown macro threats — Scans for unknown macro threats.

8. On the **Performance** section, configure the scanning duration options to improve performance.

In...	Define...
Maximum Scan Time	Specify the maximum scan time for files in seconds. The default scan time is 60 seconds. If a scan exceeds the time limit, the scan stops and logs a message. Allowed scan time is from 10-9999 seconds.
Number of Scan Threads	Sets the maximum number of scan threads. The default scan thread is 100 threads. Allowed scan thread is 1-800 threads.

9. In the **Actions** section, define the primary and secondary action to perform when a threat is detected:

In...	Define...
Threat Detection First Response	<ul style="list-style-type: none"> • Clean — Cleans the item that contains a threat then Continue Scanning as secondary action. • Continue Scanning — Continues scanning without taking any action when a threat is found.
If the first response fails	<p>Select the next action you want the scanner to take if the first action fails.</p> <p>Continue Scanning — Continue scanning when a threatened file is detected.</p>
Unwanted Programs first response	<p>Clean — Cleans the item that contains threat then Continue Scanning as secondary action.</p>
If the first response fails	<p>Continue Scanning — Continues scanning without taking any action when a threat is found.</p>

10. In the **Reports** section, configure these log activities preferences:

In...	Define...
Log Files	<ul style="list-style-type: none"> • Enable Scanner Activity Logging — Enables ICAP's scan activity logs in the default file location. Default log file location is according to the Endpoint Security Common policy. • Limit log file size (MB) — Enable to set the maximum log file size. Allowed log file size is 1–999 MB.
Log File Format	<p>Defines the log file format such as ANSI, Unicode UTF8, or Unicode UTF16.</p>
What to log, in addition to scanning activity	<ul style="list-style-type: none"> • Session Settings — Logs the session details. • Session Summary — Logs the session summary. • Failure to scan encrypted files — Logs the scan failure details for encrypted files.

11. Click **Apply** to save the configuration.

**Tip**

You can view the ICAP connection status from the scan statistics page. For more information, see [View filers scan statistics](#).

**Tip**

For best practices about how to configure ICAP settings for Endpoint Security Storage Protection, see [KB81933](#).

Configure ICAP scanner server in self-managed environment with ICAP storage appliances

You can scan the files on ICAP storage appliances for viruses, malware, and other security threats by integrating with Endpoint Security Storage Protection through the Internet Content Adaptation Protocol (ICAP).

Before you send files to be scanned on an ICAP scan server, configure the scan server details (server where the ENS SP is installed) in your ICAP storage appliances. For more information about how to configure the ICAP scanner server with ICAP storage appliances, refer your ICAP storage appliance guide.

**Note**

Endpoint Security Storage Protection adheres to RFC-3507 for ICAP scanning. As part of the ICAP use, ENS SP supports only Response Modification (RESPMOD) and Request Modification (REQMOD) commands. RESPMOD commands must also be in specific formatting as well. For more information on determining if an ICAP client meets the pre-requisites for communication with ENS SP, refer to [KB75543 \(Storage compatibility testing with ICAP-based NAS appliances\)](#).

After an ICAP server scans the file, it informs the ICAP storage appliance whether the file is a threat according to ICAP 1.0 standards. The ICAP scan server repairs the malicious file based on the ICAP storage appliance's configuration. All generated events are sent to **Events Log**.

Monitoring Endpoint Security Storage Protection activity in your environment

Monitoring activity in ePO environment

View the threat event log in McAfee ePO

You can view threat events for all managed systems from the **Reporting** menu.

The **Threat Event Log** is a log file of all threat events that McAfee ePO receives from managed systems. To view the log files, click **Menu → Reporting → Threat Event Log**.

In McAfee ePO, you can define which events are forwarded to the McAfee ePO server. To display the complete list of events in McAfee ePO, select **Menu → Configuration → Server Setting**, select **Event Filtering**, then click **Edit**.

Set up a **Purge Threat Event Log**, server task to purge the **Threat Event Log** periodically.

For information about **Automatic Responses** and working with the **Threat Event Log**, see the [McAfee ePO Product Guide](#).

Endpoint Security Storage Protection dashboard and monitors

You can watch the status of your managed systems and any threats in your environment using your dashboard.

Dashboards are collections of monitors that track activity in your McAfee ePO environment.

Endpoint Security Storage Protection provides default dashboard and monitors for both ICAP server and NetApp filers. Depending on your permissions, you can use them as is, modify them to add or remove monitors, or create custom dashboards using McAfee ePO.

Default dashboards and monitors of NetApp filers

The predefined dashboards and monitors of NetApp filers.

Dashboard	Monitor	Description
Endpoint Security Storage Protection NetApp: Current Detections	Endpoint Security Storage Protection NetApp: Filers with Threats Detected per Week	Run queries or reports to get current malware or thread trend on configured NetApp filers.

Dashboard	Monitor	Description
	Endpoint Security Storage Protection NetApp: Top 10 Detected Threats	
	Endpoint Security Storage Protection NetApp: Summary of Threats Detected in the Last 24 Hours	
	Endpoint Security Storage Protection NetApp: Threat Names Detected per Week	
	Endpoint Security Storage Protection NetApp: Threats Detected per Week	
	Endpoint Security Storage Protection NetApp: Summary of Threats Detected in the Last 7 Days	
Endpoint Security Storage Protection NetApp: Filer Performance	Endpoint Security Storage Protection NetApp: Scan Requests Accepted	Run queries or reports to get summary of NetApp scanner server statistics.
	Endpoint Security Storage Protection NetApp: File Access Denied	
	Endpoint Security Storage Protection NetApp: Scan Requests Denied	
	Endpoint Security Storage Protection NetApp: Scans Timed Out	

Dashboard	Monitor	Description
Endpoint Security Storage Protection NetApp: Filer Performance per Scan Server	Endpoint Security Storage Protection NetApp: Scan Requests Accepted Per Server	Run queries or reports to get scan statistics per Netapp scanner server.
	Endpoint Security Storage Protection NetApp: File Access Denied Per Server	
	Endpoint Security Storage Protection NetApp: Scan Requests Denied Per Server	
	Endpoint Security Storage Protection NetApp: Scans Timed Out Per Server	

Default dashboards and monitors of ICAP scanner

The predefined dashboards and monitors of ICAP scan server.

Dashboard	Monitor	Description
Endpoint Security Storage Protection ICAP: Current Detections	Endpoint Security Storage Protection ICAP: Filers with Threats Detected per Week	Run queries or reports to get current malware or thread trend on configured ICAP server.
	Endpoint Security Storage Protection ICAP: Top 10 Detected Threats	
	Endpoint Security Storage Protection ICAP: Summary of Threats Detected in the Last 24 Hours	

Dashboard	Monitor	Description
	Endpoint Security Storage Protection ICAP: Threat Names Detected per Week	
	Endpoint Security Storage Protection ICAP: Threats Detected per Week	
	Endpoint Security Storage Protection ICAP: Summary of Threats Detected in the Last 7 Days	
Endpoint Security Storage Protection ICAP: Server Performance	Endpoint Security Storage Protection ICAP: Scan Requests Accepted	Run queries or reports to get summary of ICAP scanner server statistics.
	Endpoint Security Storage Protection ICAP: File Access Denied	
	Endpoint Security Storage Protection ICAP: Scan Requests Denied	
	Endpoint Security Storage Protection ICAP: Scans Timed Out	
Endpoint Security Storage Protection ICAP: Server Performance per Scan Server	Endpoint Security Storage Protection ICAP: Scan Requests Accepted Per Server	Run queries or reports to get scan statistics per ICAP scanner server.
	Endpoint Security Storage Protection ICAP: File Access Denied Per Server	

Dashboard	Monitor	Description
	Endpoint Security Storage Protection ICAP: Scan Requests Denied Per Server	
	Endpoint Security Storage Protection ICAP: Scans Timed Out Per Server	

Custom dashboards

Depending on your permissions, you can create custom dashboards and add monitors using default Endpoint Security Storage Protection queries. For more information on how to create custom dashboards, refer [McAfee ePO guide](#).

Queries and reports

Use queries to retrieve detailed information about the status of your managed systems and any threats in your environment. You can export, download, or combine queries into reports, and use queries as dashboard monitors.

Queries are questions that you ask McAfee ePO, which returns answers as charts and tables. Reports enable you to package one or more queries into a single PDF document to access outside of McAfee ePO.

Similar information is available by accessing activity logs from the Endpoint Security Client on individual systems.

You can view query data only for resources where you have permissions. For example, if your permissions grant access to a specific **System Tree** location, your queries return data only for that location.

To view and run queries or reports:

1. Click **Menu** → **Reporting** → **Queries & Reports**
2. Select **Queries** tab.

or

Select **Reports** tab.
3. On the left pane, click **McAfee Groups** → **Endpoint Security**
4. Review the queries in the **Queries** tab.

or

Review the reports in the **Reports** tab.
5. Navigate to the required query or reports and click **Run**.

Default NetApp queries

The storage protection module adds default NetApp queries to McAfee Groups. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the McAfee ePO database.

- **Endpoint Security Storage Protection NetApp: Detection Response Summary**
- **Endpoint Security Storage Protection NetApp: File Access Denied**
- **Endpoint Security Storage Protection NetApp: File Access Denied Per Server**
- **Endpoint Security Storage Protection NetApp: Filers with Threats Detected Per Week**
- **Endpoint Security Storage Protection NetApp: Scan Requests Accepted**
- **Endpoint Security Storage Protection NetApp: Scan Requests Accepted Per Server**
- **Endpoint Security Storage Protection NetApp: Scan Requests Denied**
- **Endpoint Security Storage Protection NetApp: Scan Requests Denied Per Server**
- **Endpoint Security Storage Protection NetApp: Scans Timed Out**
- **Endpoint Security Storage Protection NetApp: Scans Timed Out Per Server**
- **Endpoint Security Storage Protection NetApp: Spyware Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection NetApp: Spyware Detected in the Last 7 Days**
- **Endpoint Security Storage Protection NetApp: Summary of Threats Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection NetApp: Summary of Threats Detected in the Last 7 Days**
- **Endpoint Security Storage Protection NetApp: Threat Count by Severity**
- **Endpoint Security Storage Protection NetApp: Threat Names Detected per Week**
- **Endpoint Security Storage Protection NetApp: Threats Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection NetApp: Threats Detected in the Last 7 Days**
- **Endpoint Security Storage Protection NetApp: Threats Detected Over the Previous 2 Quarters**
- **Endpoint Security Storage Protection NetApp: Threats Detected per Week**
- **Endpoint Security Storage Protection NetApp: Top 10 Detected Threats**
- **Endpoint Security Storage Protection NetApp: Top 10 Threats Per Threat Category**
- **Endpoint Security Storage Protection NetApp: Unwanted Programs Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection NetApp: Spyware Detected in the Last 7 Days**

For more details on how to create custom queries and reports, refer [McAfee ePO product guide](#).

Default ICAP queries

The storage protection module adds default ICAP queries to **McAfee Groups**. Depending on your permissions, you can use them as is, modify them, or create custom queries from events and properties in the McAfee ePO database.

- **Endpoint Security Storage Protection ICAP: Detection Response Summary**
- **Endpoint Security Storage Protection ICAP: File Access Denied**
- **Endpoint Security Storage Protection ICAP: File Access Denied Per Server**
- **Endpoint Security Storage Protection ICAP: Filers with Threats Detected Per Week**
- **Endpoint Security Storage Protection ICAP: Scan Requests Accepted**
- **Endpoint Security Storage Protection ICAP: Scan Requests Accepted Per Server**
- **Endpoint Security Storage Protection ICAP: Scan Requests Denied**

- **Endpoint Security Storage Protection ICAP: Scan Requests Denied Per Server**
- **Endpoint Security Storage Protection ICAP: Scans Timed Out**
- **Endpoint Security Storage Protection ICAP: Scans Timed Out Per Server**
- **Endpoint Security Storage Protection ICAP: Spyware Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection ICAP: Spyware Detected in the Last 7 Days**
- **Endpoint Security Storage Protection ICAP: Summary of Threats Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection ICAP: Summary of Threats Detected in the Last 7 Days**
- **Endpoint Security Storage Protection ICAP: Threat Count by Severity**
- **Endpoint Security Storage Protection ICAP: Threat Names Detected per Week**
- **Endpoint Security Storage Protection ICAP: Threats Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection ICAP: Threats Detected in the Last 7 Days**
- **Endpoint Security Storage Protection ICAP: Threats Detected Over the Previous 2 Quarters**
- **Endpoint Security Storage Protection ICAP: Threats Detected per Week**
- **Endpoint Security Storage Protection ICAP: Top 10 Detected Threats**
- **Endpoint Security Storage Protection ICAP: Top 10 Threats Per Threat Category**
- **Endpoint Security Storage Protection ICAP: Unwanted Programs Detected in the Last 24 Hours**
- **Endpoint Security Storage Protection ICAP: Unwanted Programs Detected in the Last 7 Days**

Monitoring activity in a self-managed environment

Check the Event Log for recent activity

The **Event Log** in the Endpoint Security Client displays a record of events that occur on the McAfee-protected system.

Task

1. Open the Endpoint Security Client.
2. Click **Event Log** on the left side of the page.

The page shows any events that Endpoint Security has logged on the system in the last 30 days.

If the Endpoint Security Client can't reach the **Event Manager**, it displays a communication error message. In this case, reboot the system to view the **Event Log**.


3. Select an event from the top pane to display the details in the bottom pane.
To change the relative sizes of the panes, click and drag the sash widget between the panes.
4. On the **Event Log** page, sort, search, filter, or reload events.

5. Navigate in the **Event Log**.

By default, the **Event Log** displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

Event Log page

The **Event Log** page is where you view the activity and debug events in the **Event Log**.

Option	Definition								
Number of events	Indicates the number of events that Endpoint Security logged on the system in the last 30 days.								
	Refreshes the Event Log display with any new event data.								
View Logs Folder	Opens the folder that contains the log files in Windows Explorer. The folder contains log files for: <ul style="list-style-type: none"> Activities Debugging Errors 								
Show all events	Removes any filter.								
Filter by Severity	Filters events by a severity level: <table border="1" data-bbox="394 987 1239 1339"> <tr> <td>Alert</td><td>Shows level 1 severity events only.</td></tr> <tr> <td>Critical and greater</td><td>Shows levels 1 and 2 severity events only.</td></tr> <tr> <td>Warning and greater</td><td>Shows levels 1, 2, and 3 severity events only.</td></tr> <tr> <td>Notice and greater</td><td>Shows levels 1, 2, 3, and 4 severity levels.</td></tr> </table>	Alert	Shows level 1 severity events only.	Critical and greater	Shows levels 1 and 2 severity events only.	Warning and greater	Shows levels 1, 2, and 3 severity events only.	Notice and greater	Shows levels 1, 2, 3, and 4 severity levels.
Alert	Shows level 1 severity events only.								
Critical and greater	Shows levels 1 and 2 severity events only.								
Warning and greater	Shows levels 1, 2, and 3 severity events only.								
Notice and greater	Shows levels 1, 2, 3, and 4 severity levels.								
Filter by Module	Filters events by module. The features that appear in the drop-down list depend on the features installed on the system at the time you opened the Event Log .								
Search	Searches the Event Log for a string.								
Events per page	Selects the number of events to display on a page. (By default, 20 events per page)								
Previous page	Displays the previous page in the Event Log .								

Option	Definition
Next page	Displays the next page in the Event Log .
Page x of x	Selects a page in the Event Log to navigate to. Enter a number in the Page field and press Enter or click Go to navigate to the page.

Column heading	Sorts the event list by...								
Date	Date the event occurred.								
Feature	Feature that logged the event.								
Action taken	<div>Action that Endpoint Security took, if any, in response to the event. The action is configured in the settings.<table><tr><td>Access Denied</td><td>Prevented access to file.</td></tr><tr><td>Allowed</td><td>Allowed access to file.</td></tr><tr><td>Blocked</td><td>Blocked access to the file.</td></tr></table></div>	Access Denied	Prevented access to file.	Allowed	Allowed access to file.	Blocked	Blocked access to the file.		
Access Denied	Prevented access to file.								
Allowed	Allowed access to file.								
Blocked	Blocked access to the file.								
Severity	<div>Severity level of the event.<table><tr><td>Critical</td><td>1</td></tr><tr><td>Major</td><td>2</td></tr><tr><td>Minor</td><td>3</td></tr><tr><td>Warning</td><td>4</td></tr></table></div>	Critical	1	Major	2	Minor	3	Warning	4
Critical	1								
Major	2								
Minor	3								
Warning	4								

Column heading	Sorts the event list by...	
	Informational	5

Endpoint Security Storage Protection log file names and locations

The activity, error, and debug log files record events that occur on systems with Endpoint Security enabled.

All activity and debug log files are stored in the following default location.

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file EndpointSecurityPlatform_Errors.log.

Feature or technology	File name
Platform	EndpointSecurityPlatform_Activity.log EndpointSecurityPlatform_Debug.log
Self Protection	SelfProtection_Activity.log SelfProtection_Debug.log
Errors	EndpointSecurityPlatform_Errors.log Contains error logs for all modules.
Endpoint Security Client	MFEConsole_Debug.log
Scan	OnAccessScan_Activity.log OnAccessScan_Debug.log OnDemandScan_Activity.log

Feature or technology	File name
	OnAccessScan_Debug.log
Threat Prevention	ThreatPrevention_Activity.log ThreatPrevention_Debug.log
Storage Protection	NetAppStats_Activity NetAppScan_Activity ICAPStats_Activity ICAPScan_Activity.log StorageProtection_Activity StorageProtection_Debug
Exploit Prevention	ExploitPrevention_Activity.log ExploitPrevention_Debug.log

View the scan statistics

You can view the statistics of NetApp or ICAP scan servers in Endpoint Security Client. The statistic page provides the details like scanner threads, scanning statistics, and performance statistics.

Task

1. Open the Endpoint Security Client.
2. Click **Storage Scan Statistics** on the left pane.
3. To view the NetApp statistics:
 - a. Click the **NetApp Statistics** tab.
 - b. Under **NetApp Connections**, click **View All Server Scan Statistics** to view the scan statistics summary of all configured NetApp filers.
 - c. To view the scan statistics of a specific filer, click the required server name.
4. To view the ICAP statistics:
 - a. Click the **ICAP Statistics** tab.
 - b. Under **ICAP Connections**, click **View All Server Scan Statistics** to view the scan statistics summary of all configured ICAP scanner servers.
 - c. To view the scan statistics of a specific ICAP scanner server, click the required server name.

You can specify the time limit in the **Statistics update interval (seconds)** to determine the refresh frequency of the **Endpoint Storage Protection Statistics** page. The minimum interval value is 10 seconds. You can set the interval value ranging from 10 to 9999 seconds.

Frequently asked questions

Here are answers to frequently asked questions.

What are the file types that I should exclude from on-access scanning?

Exclude these common file types from on-access scanning. Add other files in the exclusion list according to your environment.

Database files

- .ldb
- .mdb
- .pst
- .pst.tmp
- .nsf

Archives or large files

- .7z
- .cab
- .iso
- .jar
- .rar
- .tar
- .tgz
- .vhd
- .vmdk
- .zip

Why is Endpoint Security Storage Protection not designed to perform on-access scan for database, large, or archived files?

When a system sends a scan file request to the filer, the filer has only 45 seconds of Common Internet File System (CIFS) or Server Message Block (SMB) protocol timeout. This scanning operation must be completed before this duration, otherwise the user is denied access to the file.

There are three performance parameters for an on-access scan solution. Do not use the time-sensitive on-access scanning solution, for:

- **Files that are already scanned by another product** — Email local databases (Example: *.pst*, *.nsf*) and email server or SQL Server databases (Example: *.mdb*, *.mdf*) use large database files. These files should be scanned by email or database scanning software.

McAfee recommends that you configure specialized scanners to scan the database contents upon creation.

- **Archived files** — Scanning archived files such as *.zip*, *.rar*, or *.7z* requires the scan engine to expand the archive folder and its contents before initiating the scanning.

McAfee recommends that you configure on-access scanning to scan the archive content when it is expanded by the user, or schedule an on-demand scan to scan these files.

- **Large-size files** — Files that are larger in size should be scanned using on-demand scanning because it requires more system resources. This is evident in an ICAP on-access scanning solution, where the entire file must be copied to the scanner before the scan is initiated.

McAfee recommends that you schedule an on-demand scan to scan these files.

Scanning these files with the on-access scanning solution increases the frequency of scan timeout. If the filer is set to deny access to files that were not scanned, sometimes users are denied access to files.

Is NetApp scanning configuration complicated?

The NetApp ONTAP design involves these protocols with their dependencies:

- Active Directory
- CIFS/SMB
- Named Pipes
- NetBIOS over TCP/IP
- RPC

These designs choices:

- Confer certain benefits over other designs such as ICAP.
- Require comprehensive prerequisites that must be met by the operating system and Endpoint Security Storage Protection product.
- Require that the vendor scanner server meets the mandatory prerequisites for Endpoint Security Storage Protection and all NetApp mandatory prerequisites.

What is the importance of the scan thread configuration and how does it affect the scanner count?

Consider a scenario where you have *Y* number of physical filers and *Z* number of discrete filer IP addresses that send scan requests.

To deploy ICAP as $2 \times Y$ scanners, you must configure each scanner's ICAP scan thread count as $20 \times Z$ threads. **



Note

** The value must be provided by the filer vendor based on how many outstanding scan requests the filer's operating system issues from the discrete filer IP address.

To deploy NetApp $2 \times Y$ scanners, you must configure the NetApp scan thread count for each scanner as $(50 \times Z)$ threads. **

Note

** The value must be provided by the filer vendor based on how many outstanding scan requests the filer's operating system issues from the discrete filer IP address.

Endpoint Security Storage Protection can be configured with a maximum of 800 threads. One scanner can handle scan requests from a maximum of 16 filers.

In the production environment, if 40 or more threads are used consistently, it represents stress.

If the Stats_ICAP.log threads used + Stats_NetApp.log threads used is ≥ 40 threads consistently, you can add scanners until relief is observed and the thread count remains below 40.

For more information about configuring the number of scanners, see [KB81962](#).

Note

If only ICAP or NetApp filers are scanned by the scanner, you need to consider only the Stats_ICAP.log or Stats_NetApp.log respectively.

For more Frequently Asked Questions, see [KB78672](#).

COPYRIGHT

Copyright © 2022 Musarubra US LLC.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.