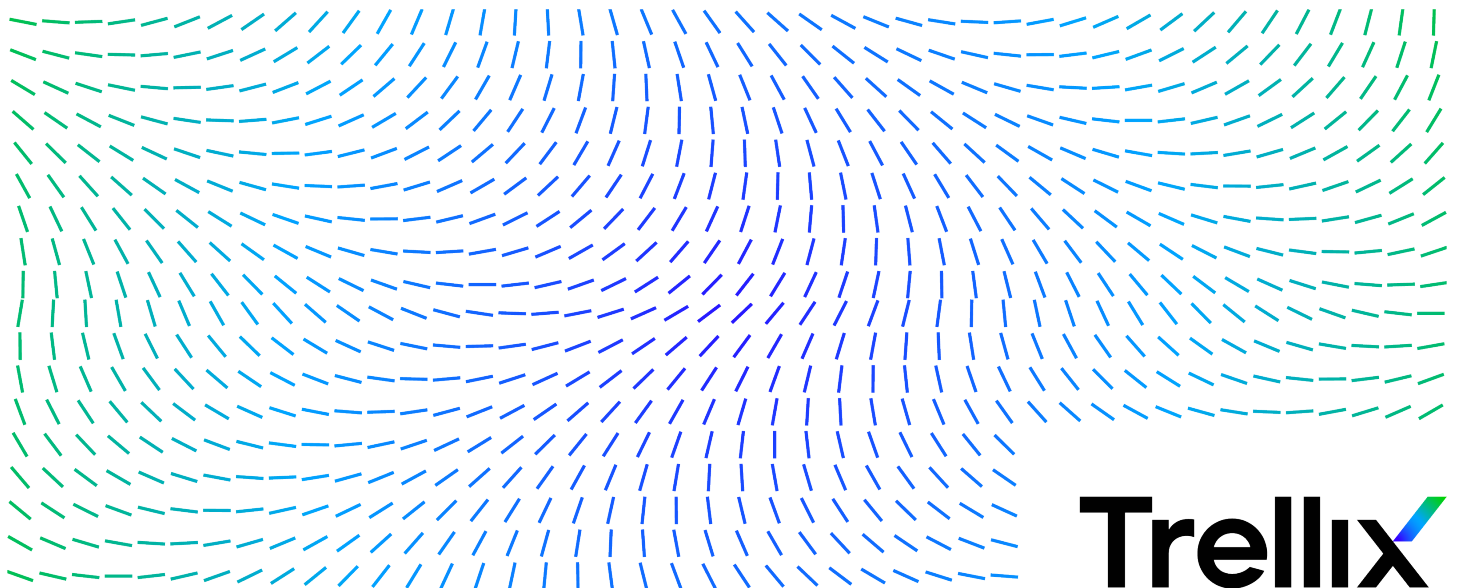


McAfee Active Response 2.4.x Interface Reference Guide



Trellix

Contents

- Interface Reference. 3**
 - Server Deployment page. 3
 - Registered Servers - Details tab. 5
 - General policy configuration. 6
 - Network Flow policy configuration. 7
 - File Hashing policy configuration. 8
 - Trace policy configuration. 13
 - Logger policy configuration. 14
 - Active Response Permission Sets. 15

Interface Reference

Server Deployment page

You can configure the details required to automatically deploy **Active Response**, **TIE**, and **DXL** services to single or multiple appliances. Automatic deployment is supported only on a VMware virtual infrastructure. Manual deployment is still supported on all VMs.

Option definitions

Option	Definition
VMware vCenter Access URL , User Name , and Password	The URL and credentials to access your virtual machine server. The VMware user must have the required permissions to allocate space, assign network, add a new disk, configure advanced settings, and to import. You can set these permissions by selecting the All Privileges option in VMware.
Validate Certificate Access URL	This option is displayed when the Access URL starts with https. Click the Validate Certificate link to display the fingerprint of the vCenter server certificate. Follow the instructions on the screen and verify whether the displayed fingerprint matches with the one on vSphere web client. When the Access URL starts with http, then the option Allow insecure connection (http) checkbox is displayed.
Data center	A unique name for the data center.
Host/Cluster	The host or cluster that the virtual machine belongs to in the virtual infrastructure. The VMware host or cluster must have sufficient resources to meet the requirements for the appliance (8 CPU Cores and 16-GB RAM).
Datastore	The device in the vCenter that can be used as a storage space for your virtual machine. The datastore must have at least 200 GB of available space.

Option	Definition
Network	The networking interface that is used for connectivity. VMware network must have unassigned addresses (when using DHCP) that do not require tagging.
Folder	The folder created on vCenter for your virtual machine. The default folder name is McAfee . The folder name must be unique. Make sure that the folder is already created in the data center.
Virtual Machine Name	The name assigned to the virtual machine. This name must be unique. The name must not exist in the data center and must meet VMware requirements.
ePO credentials User Name and Password	The user name and password to access McAfee ePO .
Hostname	The IP address of the virtual machine in which McAfee ePO is installed.
Port	The port number used to connect McAfee ePO extensions to the server hosting Active Response , DXL , and TIE . The default port is 8443.
Wake up port	The port that is used to send wake-up calls to McAfee Agent . The default port is 8082.
Validate Certificate	Displays the fingerprint of the server. Follow the instructions on the screen and verify whether the displayed fingerprint matches the one on McAfee ePO .
New Server Credentials Root Password , User Name , and Password	Enter a user name, password, and root password for the new server that is set up to host Active Response , DXL , or TIE .
New server network Hostname	Create a name for the server appliance.

Option	Definition
Domain	Enter the domain name for the server.
Mode	<p>Sets the mode to network IP address to the server. The 2 modes available are: DHCP and Manual. If Manual mode is selected, enter the:</p> <ul style="list-style-type: none"> IPv4 Address — The IP address of the server. Mask — The masked IP address for the network assigned to the server. Gateway — Enter the network gateway that is used by the server to send data back and forth. DNS — The server hosting the naming service.
NTP	Set the time servers to synchronize timezones of the server. The default entry lists 0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org . You can enter up to 3 servers, using comma as a separator.
DXL port	The port that DXL uses to connect to other DXL brokers outside the server. The default port is 8883. This field is displayed only if the DXL checkbox is selected.
Services	Select the services that you want to deploy to the server. The services that can be deployed are TIE , MAR , and DXL . You can select multiple services and deploy them to the server. TIE and DXL are selected by default. When you select MAR , TIE is also selected.
Deploy	Starts the deployment process to the server.

Registered Servers - Details tab

Configure connection to the **Active Response** server.

Option definitions

Option	Definition
Active Response Server Version	Shows the version of the connected Active Response server.
Active Response Server Location	Sets the URL to the Active Response server. For example: <code>https://10.0.0.1/mar/api</code>
Active Response License	Shows if the Active Response server is licensed.

General policy configuration


Configure **Active Response** on managed endpoints.

Option	Definition
Max merge retrieve	Sets the maximum number of results returned by Active Response search expressions. The maximum limit is 512.
Enable triggers	Enables endpoints to execute triggers.
Enable data folder protection	Data folder isn't readable. Only log files are readable when they are enabled. If they are enabled, files in <code>%PROGRAMDATA%\McAfee\MAR\data</code> are readable.
Enable Unattended Content Updates	Enables endpoints to update content without an explicit deployment task.
Unattended Content Updates Timeout	Displays the update frequency in minutes used by endpoint when unattended content updates are enabled.

Network Flow policy configuration

Configure the **Network Flow** plug-in on managed endpoints.

Option definitions

Option	Definition
Enable Plug-in	Enables the NetworkFlow collector and trigger capabilities on the endpoint.
Enable Network Sniffing	Enables you to configure your network-related activities to a granular level. This option is enabled by default. If this option is disabled, certain network activities that require higher resource consumption such as network triggers and network flow collectors are disabled.
Max database size (MB)	The size limit for the NetworkFlow collector database on endpoints. When this limit is reached, oldest records are discarded from the database.
Max database size %	The percentage of endpoint storage that the NetworkFlow collector database can use.
Max rows retrieve	Maximum number of result rows returned by the NetworkFlow collector. The maximum number of rows retrieved is 512.
Collect TCP/UDP System process information (Windows only)	<p>Collects TCP/UDP connection information generated by system processes on endpoints running Windows. It determines if an application tried to connect to a particular host or IP address. Disabling this option collects only user space application connections.</p> <div> Note: If you do not need to collect TCP/UDP information, do not enable this feature.</div>

Option	Definition
Ignore Process for collection of TCP/UDP information - (Use ';' as separator) (Windows only)	Excludes processes from the NetworkFlow monitoring to reduce resource consumption and performance impact in systems that are web servers.
Display Message on Quarantine actions	Sends notifications to endpoints when the endpoints are quarantined.
Quarantine Endpoint notification message	The default notification message that is sent to an endpoint when it is quarantined. This message can be customized.
Remove Quarantine Endpoint notification message	The default notification message that is sent when the quarantine status is removed from an endpoint. This message can be customized.


File Hashing policy configuration




Configure the **File Hashing** plug-in on managed endpoints.

Option definitions

Option	Definition
Enable Plug-in	Enables the Files collector and trigger capabilities on the endpoint.
Max database size (MB)	The size limit for the Files collector database on endpoints. If the value exceeds the Max database size (MB) , then Active Response tries to get as close as possible to the maximum storage target by removing information about deleted files from the database.
Max database size %	The maximum storage target size that the File Hashing plug-in database tries to keep. If the value exceeds the Max database size % value, then Active Response tries to get as close as possible to the

Option	Definition
	maximum storage target by removing information about deleted files from the database.
Max rows retrieve	Maximum number of result rows returned by the Files collector.
Hash Strategy	<p>Selects the priority of the file hashing process. A lower priority uses less endpoint resources.</p> <ul style="list-style-type: none"> • Low — This is the recommended setting. Uses the least endpoint resources. • Normal — The operating system alone decides priority. • Medium — Incremented priority. • High — Top priority. • Auto — Switches between Low and Normal strategies depending on endpoint usage.
Pause on battery	Pause file hashing when the endpoint is running on battery to preserve battery life.
Seconds to delay hashing after boot	The time in seconds to delay the file hashing process in the Active Response clients after booting the system. The endpoints will start the warm-up procedure for the file hashing component only after the specified delay time is over. The default value is 120 seconds.
Ignore Files on Windows	<p>A list of file paths to ignore. File paths must be complete, indicating full path, file name, and extension. For example, C:\PAGEFILE.SYS.</p> <div data-bbox="784 1570 824 1612" data-label="Image"></div> <p>Note: Unless there is a reason to ignore a specific file, only ignore those files that are repeatedly opened and modified.</p> <p>You can use these system variables to specify ignored files and paths:</p> <ul style="list-style-type: none"> • %systemdrive% • %profilesdirectory%

Option	Definition
	<ul style="list-style-type: none"> • %windir% • %commonprogramfiles% • %commonprogramfiles(x86)% • %comspec% • %homedrive% • %programdata% • %programfiles% • %programfiles(x86)% • %public% • %systemroot% • %temp% • %tmp% <p>Active Response only expands system user variables. Use of variables that point to user paths is not recommended. Avoid using the following variables:</p> <ul style="list-style-type: none"> • %allusersprofile% • %appdata% • %homepath% • %localappdata% • %userprofile% <p>Under certain circumstances, endpoint users with administrator level access can change the destination folders of system variables.</p> <div data-bbox="769 1283 1360 1591">  Tip: If you must use system variables, you can create an Active Response trigger that catches changes to system variables in the Windows registry. The trigger must be of WinRegistry type and watch for changes on this registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment. </div>
Ignore Extensions on Windows	<p>A list of file extensions to ignore. Place a '.' before each extension, separated by semicolons. For example, .swap;.o;.temp;</p>

Option	Definition
	 Note: Unless there is a reason to ignore a specific extension, only ignore those extensions that are repeatedly opened and modified.
Ignore Paths on Windows	<p>Paths and folder names to be ignored. You can specify folder paths in full or partially, using '*' to replace the beginning of a path, or entering '**' to ignore a folder regardless of how many subdirectories it appears.</p> <p>For example:</p> <ul style="list-style-type: none"> • *bar excludes folders bar and foobar anywhere in the file system. • *foo\bar excludes the bar folder inside the foo and snafoo directories, anywhere in the file system. • C:\foo\bar\ excludes only the folder bar inside C:\foo directory. • C:**\bar\ excludes one or more subdirectories where bar is found. For example, ignores c:\foo\bar, c:\snafoo\bar, and c:\snafoo\foo\bar. <div>  Warning: When entering absolute paths, the trailing '\' is mandatory. </div> <p>Removing a path from the ignored list makes the path available for file hashing only after the endpoint system is restarted. Until then, only newly created files are hashed at previously ignored paths.</p> <div>  Note: Unless there is a reason to ignore a specific path, only ignore those paths that are repeatedly accessed. </div>
Ignore Files on Linux	<p>A list of file paths to ignore. File paths must be complete, indicating full path, file name, and extension. For example, /etc/cma.d/lpc.conf;</p> <p>You can use the following system variables to specify ignored files and paths:</p>

Option	Definition
	<ul style="list-style-type: none"> • <code>\$BASH_VERSION</code> • <code>\$HOSTNAME</code> • <code>\$CDPATH</code> • <code>\$HISTFILE</code> • <code>\$HISTFILESIZE</code> • <code>\$HISTSIZ</code> • <code>\$HOME</code> • <code>\$IFS</code> • <code>\$LANG</code> • <code>\$PATH</code> • <code>\$PS1</code> • <code>\$TMOUT</code> • <code>\$TERM</code> • <code>\$SHELL</code> • <code>\$DISPLAY</code> • <code>\$EDITOR</code>
Ignore Extensions on Linux	<p>A list of file extensions to ignore. Place a '.' before each extension, separated by semicolons. For example, <code>.swp;o;.temp;</code></p>
Ignore Paths on Linux	<p>Paths and folder names to be ignored. You can specify folder paths in full or partially, using '*' to replace the beginning of a path. For example:</p> <ul style="list-style-type: none"> • <code>*bar</code> excludes folders <code>bar</code> and <code>foobar</code> anywhere in the file system. • <code>*/bar</code> excludes the <code>bar</code> folder anywhere in the file system. • <code>/foo/bar</code> excludes only the folder <code>bar</code> inside the <code>/foo</code> directory. <p>Removing a path from the ignored list makes the path completely available for file hashing only after the endpoint system is restarted. Until then, only newly created files are hashed at previously ignored paths.</p>
Max File Size for Hashing (Mb)	<p>The maximum file size that Active Response hashes. Files above this limit are excluded from file hashing.</p>

Option	Definition
Ignore Files on macOS	A list of file paths to ignore. You can use ';' as separator.
Ignore Extensions on macOS	A list of file extensions to ignore. You can use ';' as separator.
Ignore Paths on macOS	Paths and folder names to be ignored. You can use ';' as separator.

Trace policy configuration

Configure the **Trace** plug-in on managed endpoints. Trace information is sent to **Active Response** and displayed on the **Threat Workspace** page. This information helps you determine how threats and potential threats move through your environment.

Option definitions

Option	Definition
Enable Plug-in	Enables the Trace plug-in on the Microsoft Windows endpoint.
Enable Plug-in for macOS Endpoints (Beta)	Enables the Trace plug-in on the macOS endpoint. This plug-in is disabled by default.
Report Internal Reputation Failures	When enabled, the Active Response client reports a McAfee ePO threat event due to internal connection issues for the Trace plug-in. This plug-in is disabled by default.
Max database size (MB)	The size limit for the Trace database on the endpoint. When this limit is reached, oldest records are discarded from the database.
Real time notification	Sends trace events as they occur.
Interval to send data	If Real time notification is disabled, specify how often (in seconds) to send trace event notifications. The default value is 30 seconds.


Option	Definition
Log Level	<p>Specify the level of information to include in the Trace log file. Selecting an option includes that information and all options below it. For example, selecting the Trace log level includes trace, info, warning, and error information. Use the lowest log level whenever possible, or disable this feature if you do not need log information.</p> <ul style="list-style-type: none"> • Debug — Detailed debug information. • Trace — Contains most variable value dumps. This can be too verbose to debug problems on production systems. • Info — Logs messages that highlight the progress of the Trace plug-in. • Warning — Information about potentially harmful situations. • Error — Error events that might prevent the Trace plug-in from running. <p>The Trace Log file is located at %PROGRAMDATA%\McAfee\Mar\data\ts_events*.log</p>
Configuration	<p>This text box is used to enter configuration code that can enable or disable Trace features. Enter information in this text box only when working with a Technical Support representative.</p>

Logger policy configuration

Configure how endpoints log **Active Response** client service events.

Option definitions

Option	Definition
Logger format	<p>Select None to stop Active Response from creating logs. Select File to create logs in files. Logs are stored in the following locations:</p> <ul style="list-style-type: none"> • Windows: %systemdrive%\ProgramData\McAfee\Mar\data\marlog.log • Linux: /var/McAfee/Mar/data/marlog.log

Option	Definition
	<ul style="list-style-type: none"> macOS: <code>/var/McAfee/Mar/data/marlog.log</code>
Level	<ul style="list-style-type: none"> Debug — Logs fine-grained events useful to identify problems with Active Response client execution. Trace — Logs almost all variable value dumps. This can be too verbose to debug problems on production systems. Info — The default level. It logs messages that highlight the progress of the Active Response client service. Warning — Logs potentially harmful situations. Error — Logs errors that cause Active Response client service to abort. <div>  Note: Use the lowest log level whenever possible, or disable this feature if you do not need log information. </div>
Buffer Size	The number of messages that the logger holds in a buffer before saving to the log file. If set to 1, Active Response updates the log file immediately after each message is generated.

Active Response Permission Sets

Manage access to **Active Response** objects.

Collectors section

Option	Definition
No permissions	Blocks access to collectors in the Active Response Catalog.
View, use, and export	Allows read

Option	Definition
	access to collectors.
Create, edit, delete, and import	Allows write access to collectors.

Reactions section

Option	Definition
No permissions	Blocks access to reactions in the Active Response Catalog .
View, use, and export	Allows read access to reactions.
Create, edit, delete, and import	Allows write access to reactions.
Apply reactions over search results.	Allows to execute reactions over results from an Active Response search expression.

Triggers section

Option	Definition
No permissions	Blocks access to triggers in the Active Response Catalog .
View, use, and export	Allows read access to triggers.
Create, edit, delete, and import	Allows write

Option	Definition
	access to triggers.

Saved searches section

Option	Definition
No permissions	Blocks access to saved search expression in the Active Response Catalog .
View, use, and export	Allows read access to saved search expressions.
Create, edit, delete, and import	Allows write access to saved search expressions.

COPYRIGHT

Copyright © 2023 Musarubra US LLC.

Trellix, FireEye and Skyhigh Security are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC and their affiliates in the US and /or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

