McAfee Scan Engine

Integration and Configuration of the McAfee Virus Scanner in iQ.Suite Watchdog

Document Version 2.0

iQ.Suite for IBM Domino, Version 17
iQ.Suite for Microsoft Exchange/SMTP, Version 13

Contents

1 Introduction

The virus scanner from McAfee reliably protects emails from malicious software. The McAfee virus scanner acts as a Scan Engine for the iQ.Suite Watchdog module, which is why it ideally integrates with the existing components of the iQ.Suite, effectively protecting your system environment from viruses, Trojans as well as spyware and malware.

When email is checked, both the email body and attached files are scanned for patterns of known malicious software. Whenever a matching pattern is found, the corresponding email is not delivered to the recipient; instead, it is securely placed in iQ.Suite Quarantine.

Feature range of the virus scanner:

- High virus detection rate
- Fast execution
- Automatic virus pattern updates
- Virus patterns are checked for functionality before use
- Archives are checked
- A return code is supplied for password-protected files

You can use the McAfee virus scanner as **integrated McAfee Scan Engine** immediately after iQ.Suite installation. The required McAfee license is part of the iQ.Suite licencing.

Notes:

For further information on installation and configuration of the virus scanner, please refer to the iQ.Suite manuals. McAfee modifications are described in the Release Notes until the update of this document.

In multi-server environments, we recommend to use the **iQ.Suite Update Manager** as central update service. For further information, please refer to the separate document concerning the iQ.Suite Update Manager (TechDoc). Download on www.gbs.com.

1.1 System Requirements

Note: When using iQ.Suite for Microsoft Exchange/SMTP: The iQ.Suite uses worker threads to process emails. For each worker thread one or more instances are created depending on the email volume (maximum of six), and they are deleted once no longer needed. Note that each instance of the McAfee virus scanner requires approx. 350 MB and that in the standard configuration of iQ.Suite three worker threads are activated.

2 iQ.Suite Configuration for IBM Domino

Perform the steps outlined below to use McAfee as an integrated virus scanner in the iQ.Suite:

1. Enable the configuration document of the McAfee Scan Engine and perform the desired settings, if required: *WATCHDOG -> UTILITIES -> VIRUS SCANNER ENGINES -> MCAFEE SCAN ENGINE*.
2. Optional: If you use a proxy server, make sure that a corresponding proxy server document is enabled (GLOBAL -> PROXY SERVER) and this document is selected for use in the McAfee Scan Engine.
3. Configure a corresponding virus scanner document under WATCHDOG -> UTILITIES -> VIRUS SCANNER. A preset job document is available. Select in the **Basics** tab the enabled 'McAfee Scan Engine'. If not already enabled, enable the McAfee virus scanner. The document is already enabled if the McAfee virus scanner has been selected in the iQ.Suite setup dialog.
4. Configure a Watchdog virus scanning job and enable the document.

   All virus patterns of McAfee are downloaded initially. Depending on your system environment, the download may take a few minutes.
5. By default, the McAfee download area will be checked for the latest pattern versions each 60 minutes and new patterns are downloaded. You can modify the download time interval in the Engine configuration document.

Note: If an error occurs on future incremental pattern downloads, for troubleshooting set the log level in the global parameter `ToolKit_SubsysLogLevel` to the value '7'.

If required, virus patterns can be updated **manually**:

1. Ensure the iQ.Suite or the iQ.Suite Grabber has been deactivated.
2. If you use a proxy server, enter the connection data in the script *test_download.cmd* (Windows) or *test_download.sh* (Unix) under `mcafee3/update`.
3. Execute the script.

Unix: The script has to be executed in the context of the Domino user. Otherwise errors may occur on further pattern updates, due to missing authorization.

3 iQ.Suite Configuration for MS Exchange/SMTP

Perform the steps outlined below to use McAfee as an integrated virus scanner in the iQ.Suite:

1. Activate the new McAfee Scan Engine: BASIC CONFIGURATION -> UTILITY SETTINGS -> SCAN ENGINES -> MCAFEE SCAN ENGINE. If required, perform further configurations.
2. Configure a new Virus Scanning Job and select in the **Scan Engines** tab the activated 'McAfee Scan Engine'.
3. To use a proxy server for the updates, define the connection settings*:* BASIC CONFIGURATION -> GENERAL SETTINGS -> PROXY SERVERS.
4. If you have the McAfee Scan Engine already in use as an external Engine, disable it as well as the corresponding job.
5. Save the configuration.

   Future virus pattern updates are performed automatically based on the configured time interval. The time interval can be configured under MCAFEE SCAN ENGINE -> UPDATE TAB. By default, the McAfee download area will be checked for more recent virus patterns each 60 minutes. New pattern versions will be downloaded.
6. Optional: If required, virus patterns can be updated **manually**: IQ.SUITE MONITOR -> SERVERS -> <SERVER NAME> -> SERVER STATUS -> TEST TAB -> **ENGINES UPDATE** -> START.

   All virus patterns of McAfee are downloaded initially. Depending on your system environment, the download may take a few minutes.

   If the update process ends successfully, the message 'OK' is displayed; if an error occurred, 'Error' is shown instead. The update process is documented in the event log.
7. Click on IQ.SUITE MONITOR -> SERVERS -> <SERVER NAME> -> SERVER STATUS -> TEST TAB -> **ENGINES TEST**-> START.

   The Engine and pattern scanning is started. A test without errors is confirmed with 'OK', Errors are indicated with 'Error'.

Note: In case of errors, delete the *update.ini* file and click on **ENGINES UPDATE** to download the initial virus patterns again.

4 Technical Description

4.1 Functionality of the McAfee Scan Engine and the Virus Pattern Update

To be able to download the virus patterns for virus scanning, the iQ.Suite has to be configured as described in the chapters above[1]. After the configured Watchdog virus scanning job has been enabled and saved, it is initialized. With the job initialization, the virus patterns are initially downloaded.

After the initial download, future pattern updates are initialized automatically according to the time interval defined in the iQ.Suite.

McAfee provides the current pattern versions for the virus scanner in a download area. iQ.Suite cyclically compares the version of the virus pattern it is using with the current version in the McAfee download area. Whenever more current files are detected in the download area, iQ.Suite performs an update by automatically downloading the new virus patterns during ongoing operation. The incremental update procedure is designed such that only between 200 and 500 KB of data is downloaded each time, keeping the strain on the network to a minimum and ensuring speedy downloads.

If you are using iQ.Suite Update Manager as central update service, please refer to the separate document concerning the iQ.Suite Update Manager (TechDoc) to obtain information on the functionality. Download on www.gbs.com.

[1] Refer to iQ.Suite Configuration for IBM Domino and iQ.Suite Configuration for Exchange/SMTP.

4.2 iQ.Suite for IBM Domino

4.2.1 Directory Structure

The configuration data of the integrated McAfee Scan Engine (*tk_mcafee3.dll*) is stored in the `mcafee3` directory. Path:

Under Windows: `<Program path>\iQSuite\mcafee3`
Under Unix: `<Program path>/iqsuite/mcafee3`

Under Unix, please note that the iQ.Suite must be installed individually on each server.

The structure of the Scan Engine's directory is described in the following chapter.

Note: Do not delete files or subdirectories from the `mcafee3` directory. Otherwise unexpected and undesired effects may occur. The parameters required for automatic virus pattern updates are preset and don't need to be adjusted.

4.2.2 Description of the Components

Initially, the `mcafee3` directory comprises the following files and subdirectories:

	Files under Windows	Files under Unix, AIX, Solaris	Task
Files under `mcafee3`:			
1	*soap.tk_mcafee3.dll* *tk_mcafee3.dll.exe* *soap.tk_mcafee3.dll.defaults.ini* *soap.tk_mcafee3.dll.ini*	*soap.tk_mcafee3.dll* *tk_mcafee3.dll.exe* *soap.tk_mcafee3.dll.defaults.ini* *soap.tk_mcafee3.dll.ini*	GROUP.Sandbox components [2]
2	*config.dat*	*config.dat*	Element of the McAfee Scan Engine
3	*mcscan32.dll*	*Linux: liblnxfv.so and liblnxfv.so.4* *AIX: libaixfv.a* *Solaris: libsunfv.so and libsunfv.so.4*	DLL of the McAfee Scan Engine
4	*tk_mcafee3.dll*	*tk_mcafee3.dll*	GROUP Interface DLL used through (**1**).
5	*tk_mcafee3_ref.cfg*	*tk_mcafee3_ref.cfg*	Configuration file evaluated through (**1**).
6	*tk_mcafee3_maint.cmd* *tk_mcafee3_maint.lock*	*tk_mcafee3_maint.sh* *tk_mcafee3_maint.lock*	Files that initiate the incremental pattern update.
7	*test_download.cmd*	*test_download.sh*	File that can be executed manually to download the current virus patterns.
8	*tk_mcafee3_upd.bat*	-	Update file

[2] The functionality and configuration of GROUP.Sandbox is described in a separate document. Download on www.gbs.com.

9	*tk_mcafee3_upd_process.bat*	-	Update file
Files under `mcafee3/update`:			
10	*mcafee_start_update.cmd*	*mcafee_avupdate.sh*	File that is called up by (**7**) and automatically launches (**11**).
11	*mcafee_update.exe*	*tk_mcafee_update*	File that starts the pattern update.
3	*mcscan32.dll*	*Linux: liblnxfv.so and liblnxfv.so.4* *AIX: libaixfv.a* *Solaris: libsunfv.so and libsunfv.so.4*	DLL of the McAfee Scan Engine
2	*config.dat*	*config.dat*	Element of the McAfee Scan Engine

If the automatic download fails, you can use (**7**) to manually initiate the download of the virus patterns required for virus scanning (**13**).

The virus patterns are first downloaded from the McAfee download area to the temporary `upd_tmp` directory, where a functionality test is performed. They are then extracted to the `mcafee3/update/extract`, and the `upd_tmp` directory is deleted. GROUP.Sandbox regularly copies functioning data from `mcafee3/update/extract` to the `mcafee3` directory to make it available to the Scan Engine.

If a faulty pattern is detected, the data is not copied to `extract`. Emails are checked using the accumulated patterns located in the `mcafee3` directory.

The first virus pattern update extends the directories as follows:

	Files under Windows	Files under Unix	Task
Files under `mcafee3`:			
14	*<xy>.dat*	*<xy>.dat*	Virus pattern files copied from `extract`. The patterns located here are used by the Scan Engine.
Files under `mcafee3/update`:			
12	*update.ini*	*update.ini*	File containing important download information. If this file does not exist, all existing patterns are downloaded, even those that were already downloaded initially.
Files under `mcafee3/update/extract`:			
13	*<xy>.dat*	*<xy>.dat*	Virus pattern files extracted from `tempDownload`.

The first incremental virus pattern update extends the directories as follows:

	Files under Windows	Files under Unix	Task
Files below `mcafee3`:			
15	*update_tmp*	*update_tmp*	Temporary update file
Files below `mcafee3/update`:			
16	*tk_mcafee3_client.log* *tk_mcafee3_client.log.old* *tk_mcafee3_server.log* *tk_mcafee3_server.log.old*	*tk_mcafee3_client.log* *tk_mcafee3_client.log.old* *tk_mcafee3_server.log* *tk_mcafee3_server.log.old*	Various log files that document the pattern update.
Files below `mcafee3/update_tmp`:			
	<empty>		Temporary directory for the virus pattern update.

Note: To change the checking procedure of the virus scanner, modify the Engine parameters under WATCHDOG -> UTILITIES -> VIRUS SCANNER -> MCAFEE SCAN PARAMETERS -> SETTINGS TAB. For a detailed parameter description, please refer to the **Comments** tab of the Engine document.

4.3 iQ.Suite for Microsoft Exchange/SMTP

4.3.1 Directory Structure

The directory `<Program Path>/GBS/iQ.Suite/Bin/mcafee3` contains the configuration data for the integrated McAfee Scan Engine (*ntk_mcafee3.dll*).

The directory structure of the Scan Engine is described in the next section.

Notes:

Do not delete any files or subdirectories from the `mcafee3` directory. Otherwise, undesired and unexpected effects may occur. The parameters required for the update are preset and do not need to be changed.

Do not modify the batch files or configuration files, hence, these changes might be overwritten with an iQ.Suite update. Change the desired settings only in the iQ.Suite administration console.

4.3.2 Description of the Components

Initially, the `mcafee3` directory consists of the following files and subdirectories:

	Files under Windows	Task
Files below `mcafee3`:		
1	*config.dat*	Element of the McAfee Scan Engine
2	*mcscan32.dll*	DLL of the McAfee Scan Engine
3	*tk_mcafee3.dll*	GROUP Interface DLL
4	*tk_mcafee3_ref.cfg*	Configuration file
5	*tk_mcafee3_upd.bat*	File that runs the pattern update. The file does not need to be executed manually.
6	*tk_mcafee3_upd_process.bat*	File that is automatically executed through (**5**).
Files below `mcafee3/Update`:		
7	*mcafee_start_update.cmd*	Executable file that launches (**8**). The file does not need to be executed manually.
8	*mcafee_update.exe*	File that starts the pattern update.
2	*mcscan32.dll*	DLL of the McAfee Scan Engine
1	*config.dat*	Element of the McAfee Scan Engine
Files below `mcafee3/Update/Extract`:		
	<empty>	

Given the large size of the virus pattern files required to perform a virus scan, they are not part of the initial iQ.Suite installation. After iQ.Suite installation and configuration, the McAfee virus patterns (**13**) are automatically downloaded from the McAfee download area (approx. 120 MB).

The virus patterns are first downloaded from the McAfee download area to the temporary `tempDownload` directory and are then extracted to `mcafee3/Update/Extract`. The `tempDownload` directory is deleted, and the virus patterns are checked for functionality. Functioning data is copied to the `mcafee3` directory to make it available to the Scan Engine. If a faulty pattern is detected, the data is not copied to `mcafee3`.

The download process is logged in (**11**), and important download information is written to (**12**). Note that this file must be available to ensure that future pattern updates can be performed. The virus patterns available in the `Extract` directory are used for scanning emails.

The first virus pattern update extends the directories as follows:

	Files under Windows	Task
Files below `mcafee3`:		
9	*<xy>.DAT*	Log file that documents the initial pattern download.
10	*tk_mcafee3_ref.cfg.timestamp*	Internal processing file.
11	*tk_mcafee3_UPD.<>.log*	Log files documenting the virus pattern download.
Files below `mcafee3/Update`:		
12	*update.ini*	File containing key download information. If this file does not exist, the entire patterns is downloaded in full.
Files below `mcafee3/Update/Extract`:		
13	*<xy>.dat*	Virus pattern files extracted from `tempDownload`.

The first incremental virus pattern update extends the directories as follows:

	Files under Windows	Task
Files below `mcafee3`:		
15	*update_tmp*	Temporary update file
Files below `mcafee3/update-temp`:		
	<empty>	Temporary directory for the virus pattern update.

5 About GBS

GROUP Business Software is a leading supplier of solutions and services for the IBM and Microsoft collaboration platforms. With the Competence Centers Security, Modernization, Mobility and Portal & BPM, GBS enables its customers to manage the challenges of today and tomorrow faster, easier and more efficiently. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia. The European headquarters is located in Frankfurt/Germany, and the North American headquarters is based in Atlanta.

Further information at www.gbs.com.

European Headquarters
GROUP Business Software AG
MesseTurm
60308 Frankfurt / Germany
Phone: +49 69 789 8819-0
Fax: +49 69 789 8819-99

Email Main Office
GROUP Business Software
Ottostrasse 4
76227 Karlsruhe / Germany
Phone: +49 721 4901-0
Fax: +49 721 4901-199

North American Headquarters
GROUP Business Software (GBS)
585 Molly Lane
Woodstock, GA 30189 / USA
Phone: +1 404-891-1711
Fax: +1 770 720-1335

GROUP Business Software (GBS)
19 Allstate Parkway
Suite 120
Markham, Ontario / Canada - L3R 5A4
Phone: +1 905 475-4064
Fax: +1 905 475-4134

UK Office
GROUP Business Software (UK) Ltd.
Manchester Business Park
3000 Aviator Way
Manchester M22 5TG / UK
Phone: +44 161 266 1066
Fax: +44 700 604 1480

info@ gbs.com
http://www.gbs.com