



Installation Guide

Revision A

McAfee Database Security 4.6.x

COPYRIGHT

Copyright © 2016 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS

Intel and the Intel and McAfee logos, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, TrustedSource, VirusScan are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

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

Contents

Preface	5
About this guide	5
Audience	5
Conventions.....	5
Find product documentation.....	6
1 Introduction	7
Key features	7
Available product versions	8
Deployment	8
Solution components.....	8
Installation workflow	9
2 Server Installation	10
Install the McAfee Database Security server on a Windows platform	10
Install the McAfee Database Security server on a Linux platform	11
Configure McAfee Database Security Manager	12
Configuring the Database Security server in FIPS compliance mode	13
3 Sensor installation	15
Install the McAfee sensor on a Redhat Linux or SUSE platform	15
Install the McAfee Database Security sensor on a Sun Solaris platform	16
Install the McAfee Database Security sensor on an AIX platform	17
Install the McAfee Database Security sensor on an HPUX platform	18
Install the McAfee Database Security sensor on a Windows platform	19
Install the MySQL/MariaDB audit plug-in on a Linux platform	20
SAP HANA monitoring.....	20
SQL Server In-Process Monitoring	21
DB2 monitoring on zOS or iSeries	21
Create database list file.....	21
Monitor DB2 on z/OS using CorreLog	22
Monitor DB2 on iSeries (System i or AS/400) using Raz-Lee iSecurity	22
Troubleshooting the sensor installation.....	23
Troubleshooting procedures	23
Run the Diagnostic Tool.....	25
4 Configuring Operations in the Web Console	27
Access the McAfee Database Security Web Console	27
Approve the sensors	28
MySQL/MariaDB database monitoring	28
Start MySQL database monitoring.....	29
Configure alternative connection properties	29
Use the audit plug-in without alternative connection	29
5 Installation prerequisites and default installation locations	31
Monitored database installations	31
File system requirements	31
Prerequisites and default locations for McAfee Database Security server installations	33

6 Upgrading McAfee Database Security	34
Upgrade the McAfee Database Security server	34
Upgrade McAfee Database Security sensors	35

Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who are responsible for configuring the product options on their systems, or for updating their systems.

Conventions

This guide uses these typographical conventions and icons.

Book title or Emphasis Title of a book, chapter, or topic; introduction of a new term; emphasis.

Bold Text that is strongly emphasized.

User input, Path, or Code Commands and other text that the user types; the path of a folder or program; a code sample.

[Hypertext](#) A live link to a topic or to a website.

Note: Additional information, like an alternate method of accessing an option.

Tip: Suggestions and recommendations.

Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.

Warning/Danger: Critical advice to prevent bodily harm when using a hardware product.

Introduction

Find product documentation

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

- 1 Go to the **Knowledge Center** tab of the McAfee ServicePortal at <http://support.mcafee.com>.
- 2 In the **Knowledge Base** pane, click a content source:
 - **Product Documentation** to find user documentation
 - **Technical Articles** to find KnowledgeBase articles
- 3 Select **Do not clear my filters**.
- 4 Enter a product, select a version, then click **Search** to display a list of documents.

1

Introduction

McAfee® Database Security is an easy-to-deploy software solution that monitors the DBMS Management System (DBMS) and protects it from both internal and external threats.

Contents

- ▶ [Key features](#)
- ▶ [Available product versions](#)
- ▶ [Deployment](#)
- ▶ [Solution components](#)

Key features

McAfee Database Security provides full visibility into DBMS user activity and can issue alerts or terminate suspicious activities based on predefined vPatch rules and custom rules.

In line with the layered defense strategy employed by leading enterprises, McAfee Database Security complements other security measures, such as encryption, network security, and other tools, by providing a hardened security layer surrounding the DBMS itself.

The key advantages of McAfee Database Security include:

- Monitoring of all DBMS activities, including the activities of authorized and privileged users
- Prevention of intrusion, data theft, and other attacks on the DBMS
- Real SQL Injection Protection
- Rule-based policies for users, queries, and DBMS objects
- Quarantine rogue users
- Enterprise level vulnerability assessment for DBMSs
- Quick and easy deployment and configuration

Available product versions

- **McAfee® Database Activity Monitoring** — This version provides monitoring and management of database activity for multiple databases and vPatch service (optional). It also includes prevention, cluster support, third-party integration, compliance modules, and advanced reporting functionality. (This version does not include vulnerability assessment.)
- **McAfee® Vulnerability Manager** — This version provides vulnerability assessment, and an optional security update service. (This version does not include data activity monitoring and vPatch functionality.)

Note

Product features depend on the product version. When a function is unavailable in the version you are using, the UI informs you that a different license is required to enable the feature.

Deployment

The McAfee Database Security solution can be used in support of simple, single DBMS installations and complex, multi-server, multi-DBMS installations without hindering performance.

Solution components

The McAfee Database Security solution comprises three components:

- **McAfee Database Security Sensor** — A small-footprint process that runs on the DBMS host server in a safe, dedicated OS user-space using patent-pending technology. The sensor enables the monitoring of all local and network access to the DBMSs in real time.
- **McAfee Database Security Server** — A J2EE server that communicates with all installed sensors. The McAfee Database Security Server does not require a dedicated computer.
- **McAfee Database Security Web Console** — A rich web-based graphical user interface dashboard that enables the administrator to review alerts, and define rules and policies.

The McAfee Database Security sensor monitors access to the DBMS and sends transaction data to the McAfee Database Security Server. Based on the policies defined using the McAfee Database Security Web Console, the server logs the transaction, issues an alert, and prevents access to the DBMS.

Installation workflow

The McAfee Database Security installation includes these procedures:

- Install the McAfee Database Security Server (see *Database Security Server*)
- Install the sensor (unless you intend to use Vulnerability Manager only)

If you intend to use Vulnerability Manager only:

- Add VA DBMS

Before you begin

Verify that these requirements are met:

- Admin/root for the server installation and for each sensor installation
- One open TCP port (that is not in use on the server) between the sensors and the server (default 1996)

2 Server Installation

This section describes how to install and configure the complete McAfee Database Security package that includes McAfee Database Activity Monitoring and Vulnerability Management functionality.

Tasks

- ▶ [Install the McAfee Database Security server on a Windows platform](#)
- ▶ [Install the McAfee Database Security server on a Linux platform](#)
- ▶ [Configure McAfee Database Security Manager](#)

Install the McAfee Database Security server on a Windows platform

The McAfee Database Security server is a J2EE server that communicates with all installed sensors.

The McAfee Database Security server can be installed on a computer running the Windows 2003 Server and above, or the Windows XP/Vista operating system.

Although McAfee Database Security Server does not require a dedicated computer, for both performance and security reasons, the use of a dedicated server is highly recommended.

Before you begin

Verify that the computer where you plan to install the server meets these minimum requirements:

- 1-GB free RAM
- 2-GB free disk space
- 32-bit JVM (Linux only)

Task

- 1 Double-click the installation file (for example, `McAfee-DBS-Server-installer-<version>-<release>.exe`).

The **Welcome to the McAfee Database Security Setup Wizard** window is displayed.

- 2 Click **Next**.
- 3 Select **McAfee Database Security**, then click **Next**.
- 4 Read the license agreement carefully, then click **I agree** to continue with the installation.
- 5 Enter or browse to the location where you want to install the application, then click **Next**.
- 6 Enter the administrator name and password. (It is recommended that you create a strong password that contains a combination of alphanumeric and other characters.) Remember the name and password; you will need it when you log in to the McAfee Database Security console.

Note

You can add more administrators after you complete the server installation.

- 7 Click **Next**, then configure the server listening ports:
 - In the **HTTP/1.1 Connector Port** and **HTTPS/1.1 Connector Port** fields, enter the management port numbers or leave the default settings unchanged. (We recommend that the default settings be used unless the ports are already taken or a firewall between the databases and the server is set up to drop the traffic.)
 - In the **Shutdown Port** and **Shutdown Key** fields, enter the shutdown port number and key, respectively.
 - In the **Sensor Connector Port** field, enter the number of the port on the server to be used to communicate with the sensor.

- 8 Click **Install**.

When the installation is complete, the **Configuring Backend Database** window is displayed.

- 9 Select the relevant backend database type, then click **Next**.

Note

An internal database can be used for an evaluation installation only.
If you select **Oracle/MSSQL External Database**, see *Working with External Databases* in the *McAfee Database Security Product Guide* before proceeding.

- 10 Click **Next**.

- 11 Verify that the **Run McAfee Database Security Server service** checkbox is selected, then click **Finish**.

The server is successfully installed on your computer and you are prompted to log in to the McAfee Database Security console.

Notes

To uninstall the McAfee Database Security Server, click **Start | All Programs | McAfee Database Security | Uninstall**.

Install the McAfee Database Security server on a Linux platform

The Database Security server is installed on a Linux/UNIX platform using an RPM file.

Task

- 1 Download the self-extracting file for the server from the McAfee website.

Note

The name of the installation file varies according to the version and build, in the format:
mfe-dbs-server-server-jre-<version#>-<build#>.i586.rpm.bin;
for example: mfe-dbs-server-jre-4.4.8-52164.i586.rpm.bin.

- 2 Log in as the root user.

- 3 Run this command:

```
chmod +x mfe-dbs-server-jre-<version#>-<build#>.i586.rpm.bin.
```

Server Installation

Installation workflow

- 4 Run this command to install the server:
`./mfe-dbs-server-jre-<version#>-<build#>.i586.rpm.bin.`
- 5 Follow the on-screen instructions.

After you accept the end-user license agreement, the install script creates and installs the RPM file named `mfe-dbs-server-jre-<version#>-<build#>.i586.rpm.`
- 6 When prompted, configure the admin password, the HTTP and HTTPS listening ports, and the port for sensor communications. If the admin password entered is empty, the default password "admin" is used.

The RPM is installed as a service that can be started and stopped using the command: `/sbin/service` (for example, `service mfe-dbs-server start`). On older distributions, use this command: `/etc/init.d/ mfe-dbs-server start.`
- 7 Following the server installation, the license page is automatically displayed, enabling you to install the license. If the page is not displayed, enter this address in your browser:
<https://<servername>:8443/>

Notes

To uninstall the Database Security Server:

- 1 Log in as the root user, then run this command to uninstall the RPM:
`rpm -e mfe-dbs-server`
- 2 Removal of the RPM does not delete log files and the internal database. To remove these files, delete the directory and all subcontents:
`rm -rf /usr/local/mfe-dbs-server.`

Configure McAfee Database Security Manager

When you complete the server installation process, the McAfee Database Security console prompts you to log in and select your configuration.

Task

- 1 Log in to the McAfee Database Security console using the user name and password specified in the server installation process.
- 2 In the **Choose your configuration** page, click **Configure sensors**. The **Sensors** page is displayed. (For a new installation, no sensors appear in the **Sensors** list.)
- 3 Install the McAfee Database Security sensor, as described in ***Error! Reference source not found.***
- 4 Approve the sensor, as described in *Approve the sensors*.

Configuring the Database Security server in FIPS compliance mode

If you need to run the system in FIPS compliance mode, configure the server and sensor before running the server service for the first time.

Note

To perform a fresh installation of Database Security server in FIPS Compliance Mode, add `/fips` to the installation command.

Tasks

- ▶ [Configure FIPS compliance](#)
- ▶ [Disable FIPS mode](#)

Configure FIPS compliance

You can configure FIPS compliance on an installed server.

Task

- 1 After the server is installed, do not start the service.
- 2 Locate the directory: `<install_dir>\java\jre6\lib\security`
- 3 Use an editor to open `java.security` (as administrator)
- 4 Remove the comment sign (“#”) from the beginning of this line:
`com.rsa.cryptoj.fips140initialmode=FIPS140_MODE`
- 5 Add a comment sign (“#”) at the start of this line:
`com.rsa.cryptoj.fips140initialmode=NON_FIPS140_MODE`
- 6 Comment out all providers under the `NON FIPS PROVIDERS` section.
- 7 Uncomment all providers under the `FIPS PROVIDERS` section.
- 8 If you are using SQL Server back-end DB (with SSL connection), remove the comment sign (“#”) from the beginning of this line:
`com.rsa.ssl.compatibility.layeredsocket.useavailable=enabled`
- 9 In the `<install_dir>\conf\server-custom.properties` file, add this text on a separate line:
`fips140.mode=true`
- 10 Start the Database Security server.

Disable FIPS mode

You can disable FIPS mode on a sensor.

Task

- 1 Go to `<sensor_install_dir>/conf`.
- 2 In an editor, open `vi .mfedbs.conf.public`.
- 3 Change the value of the “FIPS_mode” variable from 1 to 0.
- 4 Restart the sensor.

3

Sensor installation

The McAfee Database Security sensor is installed on the database host server using an installation package.

Before installing the McAfee Database Security sensor, verify that the database host server where you want to install the sensor meets all requirements (see *Installation workflow*).

Note

Installing the sensor creates an OS user on Unix/Linux platforms named "mfedbs", a member of the dba, oinstall groups (if the groups exist).

For more system and database requirements, see *Monitored database installations*.

Tasks

- ▶ [Install the McAfee sensor on a Redhat Linux or SUSE platform](#)
- ▶ [Install the McAfee Database Security sensor on a Sun Solaris](#)
- ▶ [Install the McAfee Database Security sensor on an AIX platform](#)
- ▶ [Install the McAfee Database Security sensor on an HPUX platform](#)
- ▶ [Install the McAfee Database Security sensor on a Windows platform](#)
- ▶ [Install the MySQL/MariaDB audit plug-in on a Linux platform](#)
- ▶ [SAP HANA monitoring](#)
- ▶ [Troubleshooting the sensor installation](#)

Install the McAfee sensor on a Redhat Linux or SUSE platform

The McAfee Database Security sensor is installed on a Redhat Linux or SUSE platform using an RPM.

Notes

- When monitoring MySQL, you need to install both the sensor and the AUDIT plug-in. For details, see [Install the MySQL/MariaDB audit plug-in on a Linux platform](#).
- Debian/Ubuntu Linux is also supported. The installer for Debian/Ubuntu is **/usr/lib/mfedbs.sensor**. All other directories and configurations are similar to RedHat.
- Redhat and SUSE on z/Linux are also supported.

Task

- 1 Download the `rpm.bin` file for the sensor from the McAfee website or select it from the McAfee media kit.
- 2 The name of the installation file varies according to the version and build, in the format: `mfe-dbs-sensor-<version#>-<build#>.<architecture>.rpm.bin`; for example, `mfe-dbs-sensor-2.0.1-3442.x86_64.rpm.bin`.

Sensor installation

Install the McAfee Database Security sensor on a Sun Solaris platform

- 3 Copy the file to the database computer.

- 4 Log in as the root user, then run this command:

```
sh <installation file path>/mfe-dbs-sensor-<version#>-  
<build#>.<architecture>.rpm.bin.
```

- 5 Follow the on-screen instructions:

Optional parameters:

```
Usage: <installation file path>/mfe-dbs-sensor-<version#>-  
<build#>.<architecture>.rpm.bin [-x] [-s] [-h] [-S ip/host] [-P port] [-R path ]
```

-h Display help message.

-S <server IP>

-P <server port>

-x Extract only. Do not proceed to install or update the software.

-s Silent. Do not prompt for anything.

-R Full path to which to install the package (available from version 2.0.1)

After you accept the end-user license agreement, the install script creates and installs an RPM file named `mfe-dbs-sensor-<version #>.rpm`.

- 6 When prompted, enter the McAfee Database Security server's IP address and listening port to ensure communication between the sensor and server.

- 7 Run this command to start the sensor service:

```
/sbin/service mfe-dbs-sensor start
```

Or, on older distributions, run this command:

```
/etc/init.d/mfe-dbs-sensor start.
```

Note

To uninstall the sensor, log in as the root user, then run this command:

```
rpm -e mfe-dbs-sensor
```

The uninstall process removes all relevant files, including registry entries. On Linux/Unix systems, some system-generated files, such as `.sh_history`, may remain in the installation directory. The installation directory and these files can safely be deleted.

Install the McAfee Database Security sensor on a Sun Solaris platform

The McAfee Database Security sensor is installed on a Sun Solaris platform using a PKG file.

Task

- 1 Download the sensor from the McAfee website or select it from the McAfee Media Kit CD.

The name of the installation file varies according to the version and build, in the format:
`mfe-dba-sensor-<version#>-<build#>.<architecture>.pkg.bin`

- 2 Copy the file to the database computer.

- 3 Log in as the root user, then run this command to install the sensor:

```
sh <installation file path>/mfe-dbs-sensor-<version#>-  
<build#>.<architecture>.pkg.bin.
```


4 Follow the on-screen instructions.

Optional parameters:

```
Usage: <installation file path>/mfe-dbs-sensor-<version#>-  
<build#>.<architecture>.rpm.bin [-x] [-s] [-h] [-S ip/host] [-P port] [-R path ]  
-h Display help message.  
-S <server IP>  
-P <server port>  
-x Extract only. Do not proceed to install or update the software.  
-s Silent. Do not prompt for anything.  
-R Full path to which to install the package (available from version 2.0.1)
```

5 When prompted, enter the McAfee Database Security server's IP address and listening port.**6** Run this command to start the service:

```
/etc/init.d/mfe-dbs-sensor start
```

Note

To uninstall the sensor, log in as the root user, then run this command:

```
pkgrm -e mfe-dbs-sensor
```

The uninstall process removes all relevant files, including registry entries. On Linux/Unix systems, some system-generated files, such as `.sh_history`, may remain in the installation directory. The installation directory and these files can safely be deleted.

Install the McAfee Database Security sensor on an AIX platform

The McAfee Database Security sensor is installed on an AIX platform using a BFF package.

Task**1** Download the bin file from the McAfee website or select it from the McAfee media kit.

The name of the installation file varies according to the version and build, in the format:
`mfe.base.sensor<version#>-<build#>.bff.bin`

2 Copy the file to the database computer.**3** Log in as the root user, then run this command to install the sensor:

Sensor installation

Install the McAfee Database Security sensor on an HPUX platform

```
sh <installation file path>/mfe.base.sensor-<version#>-<build#>.bff.bin.
```

4 Follow the on-screen instructions.

Optional parameters:

```
Usage: <installation file path>/mfe-dbs-sensor-<version#>-<build#>.<architecture>.rpm.bin [-x] [-s] [-h] [-S ip/host] [-P port] [-R path ]
```

-h Display help message.

-S <server IP>

-P <server port>

-x Extract only. Do not proceed to install or update the software.

-s Silent. Do not prompt for anything.

-R Full path to which to install the package (available from version 2.0.1)

5 When prompted, enter the McAfee Database Security server IP address and listening port.

6 Run this command to start the service:

```
/etc/rc.d/init.d/mfe.dbs.sensor start
```

Note

To uninstall the sensor, log in as the root user, then run this command:

```
installp -u mfe-dbs-sensor
```

The uninstall process removes all relevant files, including registry entries. On Linux/Unix systems, some system-generated files, such as `.sh_history`, may remain in the installation directory. The installation directory and these files can safely be deleted.

Install the McAfee Database Security sensor on an HPUX platform

The McAfee Database Security sensor is installed on an HPUX platform using a DEPOT file.

Task

1 Download the HPUX for the sensor from the McAfee website or select it from the McAfee media kit.

The name of the installation file varies according to the version and build, in the format:

```
mfe-dbs-sensor-<version#>-<build#>.<architecture>.depot.bin
```

2 Copy the file to the database computer.

3 Log in as the root user, then run this command to install the sensor:

```
sh <installation file path>/mfe-dbs-sensor-<version#>-<build#>.<architecture>.depot.bin.
```

4 Follow the on-screen instructions.

Optional parameters:

```
Usage: sh <installation file path>/mfe-dbs-sensor-<version#>-  
<build#>.<architecture>.depot.bin [-x] [-s] [-h] [-R root_path ]
```

-h Display help message.

-x Extract only. Do not proceed to install or update the software.

-s Silent. Do not prompt for anything.

5 When prompted, enter the McAfee Database Security server's IP address and listening port.**6** Run this command to start the service:

```
/sbin/init.d/mfe-dbs-sensor start
```

Note

To uninstall the sensor, log in as the root user, then run this command:

```
swremove dbssensor
```

The uninstall process removes all relevant files, including registry entries. On Linux/Unix systems, some system-generated files, such as `.sh_history`, may remain in the installation directory. The installation directory and these files can safely be deleted.

Install the McAfee Database Security sensor on a Windows platform

The McAfee Database Security sensor is installed on a Windows platform using a Setup wizard.

Note

You can perform an unattended installation. For details, refer to McAfee KnowledgeBase article [KB75424](#).

Task

1 Download the installation file for Windows from the McAfee website.

2 The name of the installation file varies according to the version and build, in the format:
`MfeSensor-<architecture>.<version>-<build>.exe`

3 Run the installation file.

The **McAfee Database Security Sensor Setup Wizard** is displayed.

4 Click **Next**.

5 Read the license agreement, then select **I agree** to indicate your acceptance of its terms.

6 Select the location where you want to install the sensor (or leave the default setting), then click **Next**.

7 Enter the server IP address and server listening ("connector") port details in the designated fields, then click **Install**.

Sensor installation

Install the MySQL/MariaDB audit plug-in on a Linux platform

When the installation is complete, the **Completing Setup Wizard** window is displayed.

8 Click **Finish**.

Note

To uninstall the sensor, from the **Start** menu, select **Programs | McAfee Database Security Sensor | Uninstall**. When prompted for confirmation, click **Yes**.

The uninstall process removes all relevant files, including registry entries. On Linux/Unix systems, some system-generated files, such as `.sh_history`, may remain in the installation directory. The installation directory and these files can safely be deleted.

Install the MySQL/MariaDB audit plug-in on a Linux platform

When monitoring an MySQL database, the McAfee Database Security Sensor requires the McAfee MySQL audit plug-in to be installed in addition to the sensor. The McAfee MySQL audit plug-in is a separately maintained, open source project.

To download and install the McAfee MySQL audit plug-in, follow the instructions at:

<https://github.com/mcafee/mysql-audit/wiki/Installation>.

Note

There are different plug-ins for MySQL and MariaDB. Make sure that you install the correct one for your database.

SAP HANA monitoring

You can monitor SAP HANA databases running on Linux servers using HANA's auditing feature.

You can monitor a SAP HANA database using a locally installed sensor (on the same machine as the SAP HANA database) or a remote sensor (on any machine accessible using TCP communication).

Note

SAP HANA monitoring is supported only by a Linux 64-bit sensor (local and remote monitoring).

The database sends its activity reports to the syslog infrastructure of the operating system, which then sends this information to the sensor over TCP using a configurable port.

A single sensor can monitor several databases, each on a different port, by changing the database list file.

For information about implementing SAP HANA, see McAfee KnowledgeBase article [KB87337](#).

SQL Server In-Process Monitoring

In-Process Monitoring (IPM) is a DAM method used in MS SQL Server that allows you to monitor SQL Server memory activity in-process. This additional method of monitoring is based on out-of-process memory monitoring.

IPM is achieved through Windows support for loading an application DLL into the SQL Server process. The DLL is responsible for monitoring the SQL Server's activity and communicating with the DAM sensor. This provides deeper insight into SQL Server's activity and reduces performance overhead.

For information about configuring IPM, see McAfee KnowledgeBase article [KB87151](#).

DB2 monitoring on zOS or iSeries

You can configure DB2 monitoring on zOS and iSeries databases.

Tasks

- ▶ [Create database list file](#)
- ▶ [Monitor DB2 on z/OS using CorreLog](#)
- ▶ [Monitor DB2 on iSeries \(System i or AS/400\) using Raz-Lee iSecurity](#)

Create database list file

To bootstrap the integration, a database list is used to indicate to the McAfee Database Security sensor which database events are provided.

The list of databases is read from a directory of known databases (/etc/mfe.dbs/dbs-list.d). Each file in the directory contains the configuration details of a DB instance. File names are free form but must end with the extension ".conf". The sensor scans the directory and listens on the specified "activity-socket" for databases with the 'ACTIVE' monitor-state.

Note

The external data source constantly tries to connect to the "activity-socket." The sensor starts listening on the specified socket once the database has been "approved" in the McAfee Database Security console.

The database configuration details are encoded in the following JSON format:

```
{
  msg-type: "db-conf",
  data-source-version: <string>, //version of providing data source
  socket-protocol-version: "1.0", //if protocol version is different from 1.0
  McAfee Sensor will not listen on the socket. Possibly can be used for upgrade
  scenarios.
  db-type: <string>, //type of database reported
  update-date: <date>, //last date status was updated
  ip: <string>, //db instance ip
  host: <string>, //db instance hostname
  lpar: <string>, //db lpar name (relevant for MF)
  version: <string>, //db version
  instance-name: <string>, //db instance name
  unique-id: <string>, //constant instance unique id (example md5)
  monitor-state: <string: ACTIVE|STOPPED>,
  activity-socket: <string> //socket to communicate with McAfee Sensor
}
```

Sensor installation

DB2 monitoring on zOS or iSeries

Sample configuration record (DB2/zOS):

```
{ "msg-type": "db-conf", "data-source-version": "1.0.0-b172", "socket-protocol-version": "1.0", "db-type": "DB2-MF", "update-date": 1335169871087, "ip": "127.0.0.1", "host": "test.test.com", "lpar": "test-lpar", "version": "9.1.6", "instance-name": "test-instance", "unique-id": "66064bac07c2b3966a0b65df2ad4c708", "monitor-state": "ACTIVE", "activity-socket": "0.0.0.0:2020" }
```

Sample configuration record (DB2/iSeries):

```
{ "msg-type": "db-conf", "data-source-version": "1.0.0-b172", "socket-protocol-version": "1.0", "db-type": "AS400", "update-date": 1335169871087, "ip": "127.0.0.1", "host": "qatest1", "lpar": "test-lpar", "version": "9.1.6", "instance-name": "test-instance", "unique-id": "66064bac07c2b3966a0b65df2ad4c708", "monitor-state": "ACTIVE", "activity-socket": "0.0.0.0:2000" }
```

Monitor DB2 on z/OS using CorreLog

You can use CorreLog to monitor IBM DB2 databases running on zOS/mainframe servers.

Task

- 1 Install CorreLog Agent on the zOS server. (For installation instructions, see CorreLog documentation.)
- 2 Install a dedicated DAM sensor on a Linux server.
- 3 On the **Sensor properties** page, click **Advanced**.
- 4 In the text box, add an entry on a separate line:
db2_zos.enable=1
- 5 Configure the database list file in the format described in *Create database list file*. Restart the sensor.
- 6 Add rules for this sensor as you would for any other sensor.

Monitor DB2 on iSeries (System i or AS/400) using Raz-Lee iSecurity

You can use Raz-Lee iSecurity software to monitor IBM DB2 databases running on iSeries (System i or AS/400) servers.

Communication between the Raz-Lee Agent and the dedicated sensor is over TCP, with a configurable port. A single sensor can be used to monitor several CorreLog Agents and DB2/zOS database by configuring several databases with different ports.

Task

- 1 Install Raz-Lee iSecurity. For installation instructions, see Raz-Lee documentation.
- 2 Install a sensor on a dedicated Linux server.
- 3 On the **Sensor properties** page, click **Advanced**.
- 4 In the text box, add an entry on a separate line:
as400.enable=1
- 5 Configure the database list file in the format described in *Create database list file*.

- 6 Restart the sensor.
- 7 Add rules for this sensor as you would for any other sensor.

Troubleshooting the sensor installation

If you installed a sensor but do not see it on the **Sensors** page, do not see your DBMSs listed for it, or fail to monitor them, you need to troubleshoot the sensor installation.

This section describes the preliminary actions to be taken to resolve sensor installation and configuration problems.

Troubleshooting procedures

If you encounter problems while installing the sensor, for example, if you have installed a sensor and "No sensors detected" is displayed when you log in to the McAfee Database Security console, follow the steps outlined in these sections.

Verify that the McAfee Database Security sensor process is up and running:

- On Linux/Solaris — `/etc/init.d/mfe-dbs-sensor status`
- On AIX — `/etc/rc.d/init.d/mfe-dbs-sensor status`
- On HP-UX — `/sbin/init.d/mfe-dbs-sensor status`
- On Windows — `services.msc` and look for the service "McAfeeSensor"

If the sensor service is down and does not start after you run it, check that the McAfee Database Security server has a valid license. If the sensor was connected to the server before applying the license, the sensor is down, and you must manually restart it.

If you are still unable to run the McAfee Database Security sensor, contact McAfee support after running the diagnostic tool (see *Run the Diagnostic Tool*).

Sensor installation

Troubleshooting the sensor installation

If the sensor is not on Sensors list:

- 1 Verify that the server IP address and port are set correctly in the sensor's configuration file.

Platform	File path
AIX	/etc/mfe-dbs-sensor
HPUX	/etc/rc.config.d/mfe-dbs-sensor
Linux	/etc/sysconfig/mfe-dbs-sensor
Solaris	/etc/default/mfe-dbs-sensor
Windows	McAfeeDBSConfig.exe

If they are not set correctly, update the configuration file, then restart the McAfee Database Security sensor service.

- 2 Verify that the sensor can reach the server port using ping <server ip> and telnet <server ip> <port number>.
 - If the server is not reachable, verify that there is no firewall blocking the communication (check that McAfee Database Security sensor communication port is open for TCP). If it is blocked, enable TCP communications on that port, then restart the McAfee Database Security sensor service.
 - If you are still unable to reach the McAfee Database Security server from the McAfee Database Security sensor system, contact your system administrator for support.
 - If the McAfee Database Security server IP address and port are reachable from the sensor server and you still do not see the sensor on the Sensors list, run the diagnostic tool (see *Run the Diagnostic Tool*), contact McAfee support for assistance.

If no DBMSs are displayed for your McAfee Database Security sensor:

- On Windows platforms, run the diagnostic tool (see *Run the Diagnostic Tool*), then contact McAfee support for assistance.
- On non-Windows platforms, check that your `oratab` file (under `/etc/oratab` or `/var/opt/oracle/oratab`) points to the correct `ORACLE_SID` and `ORACLE_HOME` (entries in the file are of the form: `$ORACLE_SID:$ORACLE_HOME:<N|Y>:`).
- If the entries are incorrect, fix them, then restart the McAfee Database Security sensor service. Otherwise, contact McAfee support after running the diagnostic tool (see below).
- If your `oratab` file is in a different location, you can configure McAfee Database Security by editing the startup script to add `"-r <oratab full path>/oratab"` to the start function.

Platform	Startup script
AIX	/etc/rc.d/init.d/mfe-dbs-sensor
HPUX	/sbin/init.d/mfe-dbs-sensor
Linux	/etc/init.d/mfe-dbs-sensor
Solaris	/etc/init.d/mfe-dbs-sensor

After editing the startup script, run the McAfee Database Security sensor.

If your DBMS appears on the Sensors' list, but is listed as disconnected:

- 1 Verify that the database version is Oracle version 8.1.7 or above, MS SQL Server 2000 or 2005, or Sybase 12.5 or 15.0.
- 2 If you are running Oracle on non-Windows Platforms, verify that:
 - You have group read and execute permissions on \$ORACLE_HOME, \$ORACLE_HOME/dbs and group read permissions on \$ORACLE_HOME/dbs/sp*.ora and \$ORACLE_HOME/dbs/init*.ora.
 - Your ORACLE_HOME group is either dba or oinstall. If not, add the relevant Oracle group to the 'mfedbs' OS user.
- 3 If the McAfee Database Security sensor is still unable to monitor your DBMSs, run the diagnostic tool, then contact McAfee support for assistance.

Run the Diagnostic Tool

Running the diagnostic tool creates an output file for you to provide to McAfee support when requesting assistance.

Task

- 1 Change the log level from INFO to DEBUG in the dbs sensor configuration file:

Platform	Configuration file name and location
Linux	/etc/sysconfig/dbssensor
Solaris	/etc/default/mfe-dbs-sensor
AIX	/etc/mfe-dbs-sensor
HPUX	/etc/rc.config.d/mfe-dbs-sensor
Windows	mcafeeDBSconfig.exe

- 2 Run the McAfee Database Security sensor for 10 minutes.
- 3 Run the diagnostic tool:

Platform	Command
Linux	/sbin/service mfe-dbs-sensor create_analytic_package
Solaris	/etc/init.d/mfe-dbs-sensor create_analytic_package
AIX	etc/rc.d/init.d/mfe-dbs-sensor create_analytic_package
HPUX	/sbin/init.d/mfe-dbs-sensor create_analytic_package
Windows	Analytics.exe

The analytic package output file name is displayed when the process is complete. Send the file by email to the McAfee support team.

4

Configuring Operations in the Web Console

After installing the McAfee Database Security server and McAfee Database Security sensors, you need to approve the sensors in the McAfee Database Security Web Console.

Contents

- ▶ [Access the McAfee Database Security Web Console](#)
- ▶ [Approve the sensors](#)
- ▶ [MySQL/MariaDB database monitoring](#)

Access the McAfee Database Security Web Console

The McAfee Database Security Web Console can be accessed using these Web browsers:

- Mozilla Firefox 1.5 or above
- Microsoft Internet Explorer 6.0 or above
- Google Chrome (all versions)

A minimum of 128 MB RAM is recommended

Note

For a detailed description of the McAfee Database Security Web Console and its functionality, see the McAfee Database Security Product Guide.

Task

- 1 In your Web browser, enter the URL of the McAfee Database Security server based on the information configured in the installation in the format: `https://<servername>:<port number>`.

Note

The port number is 8443 unless it was changed during the server installation.

- 2 Enter the administrator user name and password as configured during the installation, then click **Login**.

The McAfee Database Security Console is displayed. If a sensor has already been installed, you are prompted to approve the sensor, as described in *Approve the sensors*.

If you have not yet installed a sensor, you are prompted to do so now. For instructions, see or click the on-screen link for detailed instructions.

If you have installed a sensor and “No sensors detected” is still displayed, click **Troubleshooting guide** to view troubleshooting information.

Approve the sensors

McAfee Database Security sensors are responsible for monitoring access to the databases and sending transaction data to the McAfee Database Security server. After installation, a sensor must be **approved** in the **Sensors** list before it can begin active monitoring of the databases.

The **Sensors** page lists the installed McAfee Database Security sensors.

If the sensor has been approved, the name of the user that approved the sensor appears in the **Approved By** field.

If the sensor has not been approved, the **APPROVE ...** button appears, indicating that you need to approve the new sensor.

Task

- 1 On the **Sensors** page, click **APPROVE ...** in the **Approved By** column.

If a new sensor reports that it is monitoring a database already recognized by the McAfee Database Security system, you are prompted to select the databases you want to monitor. For details, see *Sensor installation*. If the sensor ID already exists in the system, the **Approve Sensor** dialog is displayed.

- 2 From the **Available actions** drop-down list, select how you want to handle this sensor:

- **New** — Indicates this is a new sensor. If you select **New**, you need to change the sensor ID to a unique one.
- **Merge** — Indicates this is the same sensor, for example, following reinstallation, and both instances should be treated as one sensor.
- **Delete** — Indicates that this sensor was added in error and should be removed from the configuration.

- 3 Click **OK**.

If no databases have been defined for this sensor, the name of the logged on user appears in the **Approved By** column.

If a new sensor reports that it is monitoring a database already recognized by the McAfee Database Security system, you are prompted to select the databases you want to monitor.

MySQL/MariaDB database monitoring

You can configure Database Security to monitor your MySQL/MariaDB databases.

You must install the audit plug-in before you can configure the database monitoring. For details, see *Install the MySQL/MariaDB audit plug-in on a Linux platform*.

Tasks

- ▶ [Start MySQL database monitoring](#)
- ▶ [Configure alternative connection properties](#)

Start MySQL database monitoring

To enable a sensor to monitor a MySQL database, you need to start the monitoring process on the **Sensors** page.

To start monitoring of a database:

- 1 On the **Sensors** page, select the sensor on the **DBMS Details** tab.
The databases monitored by the sensor are listed in the lower pane.
- 2 Locate the database, then click the corresponding **Start Monitoring** button.

Configure alternative connection properties

The sensor used to monitor the MySQL database needs to connect to the server using the local socket. We recommend that you configure alternative connection properties on the **DBMS configuration** page.

To configure the sensor to connect using a local socket:

- 1 On the **DBMS configuration** page, select **Enable Alternative DBMS Connections**.
- 2 Enter the socket details as the connection string, then click **Save**.

Use the audit plug-in without alternative connection

If the sensor is used to monitor MySQL/MariaDB databases without an alternative connection, these functions do not work:

- Terminate on the rule actions
- ddl/dcl delay (where applicable)

To configure the sensor to monitor MySQL/MariaDB without an alternative connection:

- 1 Add the following line to my.cnf file:
`audit_json_socket=1`
- 2 Execute the command:
`set global audit_json_socket=1;`

5

Installation prerequisites and default installation locations

This section includes these topics:

Contents

- ▶ [Monitored database installations](#)
- ▶ [Prerequisites and default locations for McAfee Database Security server installations](#)

Monitored database installations

This section lists the prerequisites and default installation locations for monitored databases.

File system requirements

- Installation directory space required – 400M (150M for minimal installation and additional space for sensor updates).
- Logs' directory space required – default configuration requires 30M per monitored database.

Default installation directories

These are the default installation directories by platform.

Platform	Installation Directory	Logs Directory	Configuration File	Binary Name	Startup script name
AIX	/opt/mfedbs.sensor	/var/adm/mfe-dbs-sensor	/etc/mfe-dbs-sensor	dbssensor	/etc/rc.d/init.d/mfe-dbs-sensor
HPUX	/opt/mfedbs.sensor	/var/adm/mfe-dbs-sensor	/etc/rc.config.d/mfe-dbs-sensor	dbssensor	/etc/rc.config.d/mfe-dbs-sensor
Linux	/usr/local/mfedbs.sensor	/var/log/mcafee	/etc/sysconfig/mfe-dbs-sensor	dbssensor	/etc/init.d/mfe-dbs-sensor
Solaris	/opt/MFEDBSsensor	/var/adm/mfe-dbs-sensor	/etc/default/mfe-dbs-sensor	dbssensor	/etc/init.d/mfe-dbs-sensor
Windows	C:\Program Files\McAfee \ McAfee-DBS-Sensor	C:\Program Files\McAfee \ McAfee-DBS-Sensor \logs	C:\Program Files\McAfee \ McAfee-DBS-Sensor \ McAfeeDBSConfig.exe	McAfee-DBS-Sensor.exe	Service name – "McAfee-DBS-Sensor"

Installation prerequisites and default installation locations

Monitored database installations

Operating system dependencies

Successful installation requires that specific packages be installed on the target operating system.

Platform	Dependencies
AIX	IBM XL C/C++ Enterprise Edition for AIX, V9.0 Runtime Environment and Utilities: http://www-1.ibm.com/support/docview.wss?rs=2239&q1=vacpp.cmp.rte&uid=swg24015997&loc=en_US&cs=utf-8&cc=us&lang=all - xIC.aix50 - xIC.msg.Ja_JP - xIC.msg.en_US - xIC.msg.ja_JP - xIC.rte - xlsmp.aix52.rte - xlsmp.msg.EN_US.rte - xlsmp.msg.JA_JP.rte - xlsmp.msg.Ja_JP.rte - xlsmp.msg.ZH_CN.rte - xlsmp.msg.Zh_CN.rte - xlsmp.msg.en_US.rte - xlsmp.msg.ja_JP.rte - xlsmp.msg.zh_CN.rte - xlsmp.rte Notes: - xIC.aix50.rte* is backward compatible with xIC.rte - Localized resource files are not required for English-only environments
HPUX pa risc 11.11 and higher	HPUX pa risc 11.11 and higher: NFS.NFS-64SLIB OS-Core.CORE-64SLIB OS-Core.CORE-SHLIBS Streams.STREAMS-64SLIB
HPUX ia64 11.23 and higher	HPUX ia64 11.23 and higher: NFS.NFS-64SLIB OS-Core.CORE2-64SLIB OS-Core.CORE2-SHLIBS Streams.STREAMS-64SLIB
Linux	libstdc++33 (this library is almost always pre-installed)
Solaris	N/A
Windows	N/A

Additional database installation requirements

- When using an external OS authentication on the database servers (for example, NIS), a user named mfedbs, a member of the DBA (or equivalent) group, must be added to the external authentication server before installation.
- If the groups used to manage an Oracle instance are not standard (dba, oinstall), you must add the newly created "mfedbs" user to the relevant groups (for example, usermod -G group1, group2).

Prerequisites and default locations for McAfee Database Security server installations

These are the prerequisites for the server installation:

- Dedicated server, running Windows XP/Server 2003 or later
- 1-GB RAM (2 GB preferable), at least 2-GB free disk space

These are the default installation directories.

Platform	Installation Directory	Logs Directory	Configuration File
Windows	C:\Program Files\mcafee \mcafee database Security	C:\Program Files\mcafee\mcafee database security\logs	C:\Program Files\mcafee\mcafee database security\conf\ server-custom.properties

6

Upgrading McAfee Database Security

When new McAfee Database Security sensors are available it is highly recommended to upgrade the McAfee Database Security system. This requires updating the McAfee Database Security server before upgrading the sensors.

Note

Always use sensors with a release number equal to or lower than the server's release number. (For example, McAfee Database Security Sensor version 4.5 cannot be used with McAfee Database Security server version 4.1.) Servers are backward compatible (for example, sensor version 4.1 can be used with server version 4.5).

Contents

- ▶ [Upgrade the McAfee Database Security server](#)
- ▶ [Upgrade McAfee Database Security sensors](#)

Upgrade the McAfee Database Security server

While the upgrade process is simple and thoroughly tested, it is always recommended to back up the McAfee Database Security data before performing upgrades. For information about backup and restoration, refer to the *McAfee Database Security Product Guide*.

Note

When upgrading a clustered management server, we highly recommend backing up the backend database before you start the upgrade. Then, stop all nodes, and upgrading and restarting them one by one. In this manner, when you upgrade and start the last node, all nodes are up and running the latest version.

Task

- 1 Download the latest server installer for your operating system from the McAfee support portal. You do not need to download sensor installations (this is done by the server at a later stage).
- 2 Run the server installer to install a server in the location where the current server is installed. During the upgrade process, all data and configurations are saved and remains available in the new server.

Upgrade McAfee Database Security sensors

After upgrading the server, you can find out whether new sensor updates are available in the **Updates/Software Updates** tab on the McAfee Database Security server.

Note

The server must be connected to the Internet to receive information about new available updates. If the server is not connected to the Internet or you do not want to receive updates automatically, download the latest sensor installers from the support portal and proceed to manual update.


The sensors are listed on the **Updates/Software Updates** tab, including information regarding the most recent available update for each sensor. To receive the latest information, click **Check for new McAfee Database Security sensors**.

Before you begin

Make sure that the sensor you want to update is connected.

Task

- 1 On the **Updates/Software Updates** tab, select the sensors that you would like to update, then click **Remote update**.

All sensor update files are downloaded from the McAfee portal and the sensors are updated. The status of the sensor changes from "New" to "Pending", then to "Uploading," "Installing" and finally to "Up-to-date." At any stage of the update process, you can click the  button to abort the update.

Note

Depending on several factors (including network bandwidth), the process can take several minutes. If a sensor is not connected, the update job might wait up to an hour before attempting the update again. If a sensor is connected and the update does not succeed in two hours, we recommend you perform a manual update.

- 2 If you choose to manually update the sensor, log in to the sensor, then follow the sensor installation instructions provided in this document. Installing the sensor without uninstalling the previous sensor keeps the current configuration (such as server IP address or listening port).