CONFIDENTIAL

McAfee Database Security Installation Guide

McAfee Integrity Monitor for Databases
McAfee Database Activity Monitoring
McAfee Vulnerability Manager for Databases

End User License Agreement

NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS CONTRACT AND DO NOT INSTALL THE SOFTWARE.

1 Definitions**.**

a. "Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such contents as are hosted by McAfee or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) McAfee or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates including any virus or vulnerability updates (collectively "Updates"), and Software, if any, licensed to you by McAfee or an Authorized Partner as part of a maintenance contract or service subscription.

b. "Use" or "Using" means to access, install, download, copy or otherwise benefit from using the Software.

c. "Permitted Number" means one (1) unless otherwise indicated under a valid license (e.g., volume license) granted by McAfee.

d. "Computer" means a device that accepts information in digital or similar form and manipulates it for a specific result based upon a sequence of instructions.

e. "McAfee" means (a) McAfee, Inc., a Delaware corporation, with offices located at 3965 Freedom Circle, Santa Clara, California 95054, USA if the Software is purchased in the United States, Mexico, Central America, South America, or the Caribbean; (b) McAfee Ireland Limited, with offices located at 11 Eastgate Business Park, Little Island, Cork, Ireland if the Software is purchased in Canada, Europe, the Middle East, Africa, Asia, or the Pacific Rim; and (c) McAfee Co., Ltd. with offices located at Shibuya Mark City West Building 12-1, Dogenzaka 1-Chrome, Shibuya-ku, Tokyo 150-0043, Japan if the Software is purchased in Japan.

2. License Grant. Subject to the payment of the applicable license fees (where applicable), and subject to the terms and conditions of this Agreement, McAfee hereby grants to you a non-exclusive, non-transferable license to Use the Software subject to any restrictions or usage terms specified on the applicable price list, purchase agreement, and product packaging included as part of the Documentation. Some third party materials included in the Software may be subject to other terms and conditions, which are typically found in a "Read Me" file or "About" file in the Software.

3. Term. This Agreement is effective for the term set forth in the purchase order issued by you and which is accepted by McAfee or, alternatively, as set forth in the product order form issued by McAfee (the "Term"). If you issue a purchase order to an Authorized Partner and the terms and conditions as set forth in the license grant letter issued by McAfee or included in the Documentation conflicts with the terms and conditions included in the purchase order, then the terms and conditions specified in the grant letter or Documentation shall control. Except for Evaluation Software, Beta Software or freeware which is subject to Section 7 below, if no Term is included in the above described materials, then the Term shall be for one (1) year from the date of purchase unless earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must cease use of the Software and destroy all copies of the Software and the Documentation.

4. Updates. This license is limited to the version of the Software delivered by McAfee and does not include Updates, unless a separate maintenance contract is purchased or, alternatively, you have purchased a service subscription that entitles you to Updates as described in the Documentation. After the specified maintenance period or service subscription period has expired, you have no further rights to receive any Updates without purchase of a new license to the Software.

5. Ownership Rights. The Software is protected by United States' and other copyright laws, international treaty provisions and other applicable laws in the country in which it is being used. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. Any copy of the Software and Documentation authorized to be made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

6. Multiple Environment Software/Multiple Language Software/Dual Media Software/Multiple Copies/Bundles/ Updates. If the Software supports multiple platforms or languages, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you receive the Software bundled with other software, the total number of your Computers on which all versions of the Software is installed may not exceed the Permitted Number. If the Software is an Update to a previous version of the Software, you must possess a valid license to such previous version in order to Use the Update. You may continue to Use the previous version of the Software on your Computer after you receive the Update to assist you in the transition to the Update, provided that the Update and the previous version are installed on the same Computer; the previous version or copies thereof are not transferred to another Computer unless all copies of the Update are also transferred to such Computer, and you acknowledge that any obligation McAfee may have to support the previous version of the Software ends upon availability of the Update.

7. Evaluation Product Additional Terms. If the product you have received with this license has been identified as "Evaluation" Software, "Beta" Software or freeware, then the provisions of this section apply. To the extent that any provision in this section is in conflict with any other term or condition in this Agreement, this section shall supercede such other term(s) and condition(s) with respect to the Evaluation Software, Beta Software, or freeware, but only to the extent necessary to resolve the conflict. You acknowledge that the Evaluation Software, Beta Software or freeware may contain bugs, errors and other problems that could cause system or other failures and data loss. Consequently, Evaluation Software, Beta Software, or freeware is provided to you "AS-IS", and McAfee disclaims any warranty or liability obligations to you of any kind. WHERE LEGAL LIABILITY CANNOT BE EXCLUDED, BUT MAY BE LIMITED, MCAFEE'S LIABILITY AND THAT OF ITS SUPPLIERS AND AUTHORIZED PARTNERS SHALL BE LIMITED TO THE SUM OF FIFTY DOLLARS (U.S. $50) IN TOTAL. You acknowledge that McAfee has not promised or guaranteed to you that freeware or Beta Software will be announced or made available to anyone in the future that McAfee has no express or implied obligation to you to announce or introduce the Beta Software, and that McAfee may not introduce a product similar to or compatible with the Beta Software. Accordingly, you acknowledge that any research or development that you perform regarding the Beta Software or any product associated with the Beta Software is done entirely at your own risk. During the term of this Agreement, if requested by McAfee, you will provide feedback to McAfee regarding testing and use of the Beta Software, including error or bug reports; you agree to grant McAfee a perpetual, non-exclusive, royalty-free, worldwide license to use, copy, distribute, make derivative works and incorporate the feedback into any McAfee product at McAfee's sole discretion. If you have been provided the Beta Software pursuant to a separate written agreement, your use of the Beta Software is also governed by such agreement. Upon receipt of a later unreleased version of the Beta Software or release by McAfee of a publicly released commercial version of the Beta Software, whether as a stand-alone product or as part of a larger product, you agree to return or destroy all earlier Beta Software received from McAfee and to abide by the terms of the End User License Agreement for any such later versions of the Beta Software. Your Use of the Evaluation or Beta Software is limited to 30 days and use of freeware is available for only so long as McAfee makes the freeware available unless otherwise agreed to in writing by McAfee. McAfee is under no obligation to continue providing freeware or to update such freeware.

8. Restrictions. You may not sell, lease, license, rent, loan, resell or otherwise transfer, with or without consideration, the Software. If you enter into a contract with a third party in which the third party manages your information technology resources ("Managing Party"), you may transfer all your rights to Use the Software to such Managing Party, provided that (a) the Managing Party only Uses the Software for your internal operations and not for the benefit of another third party; (b) the Managing Party agrees to comply with the terms and conditions of this Agreement, and (c) you provide McAfee with written notice that a Managing Party will be Using the Software on your behalf. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement. You may not reverse engineer, decompile, or disassemble the Software, except to the extent the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon, the Software in whole or in part. You may not copy the Software or Documentation except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by McAfee.

9. Warranty and Disclaimer.

a. Limited Warranty. McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., CD ROM), if any, on which the Software is contained and provided to you will be free from defects in materials and workmanship.

b. Customer Remedies. McAfee's and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee's option, either (i) return of the purchase price you paid for the license, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to McAfee at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent McAfee is subject to restrictions under United States export control laws and regulations.

c. Warranty Disclaimer. Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS" AND MCAFEE MAKES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW. MCAFEE, ITS SUPPLIERS AND AUTHORIZED PATNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR FITNESS

FOR A PARTICULAR PURPOSE. YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, MCAFEE MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS.

10. Limitation of Liability. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL MCAFEE OR ITS AUTHORIZED PARTNERS OR SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR LOSS OF PROFITS, LOSS OF GOODWILL OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR GROSS NEGLIGENCE OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY OTHER DAMAGE OR LOSS. IN NO EVENT SHALL MCAFEE OR ITS AUTHORIZED PARTNERS OR SUPPLIERS BE LIABLE FOR ANY DAMAGE IN EXCESS OF THE PRICE PAID FOR THE SOFTWARE, IF ANY, EVEN IF MCAFEE OR ITS AUTHORIZED PARTNERS OR SUPPLIERS SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. This limitation shall not apply to liability for death or personal injury to the extent that applicable law prohibits such limitation. Furthermore, some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this limitation and exclusion may not apply to you. Nothing contained in this Agreement limits McAfee's liability to you for McAfee's negligence or for the tort of fraud. McAfee is acting on behalf of its suppliers and Authorized Partners for the purpose of disclaiming, excluding and/or limiting obligations, warranties and liability as provided in this Agreement, but in no other respects and for no other purpose. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

11. Notice to United States Government End Users. The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

12. Export Controls. You acknowledge that the Software is subject to the export control laws and regulations of the United State of America ("US"), and any amendments thereof. You shall not export or re-export the Software, directly or indirectly, to (i) any countries that are subject to US export restrictions (currently including, but not necessarily limited to, Cuba, Iran, Libya, North Korea, Sudan, and Syria); (ii) any end user known, or having reason to be known, will utilize them in the design, development or production of nuclear, chemical or biological weapons; or (iii) any end user who has been prohibited from participating in the US export transactions by any federal agency of the US government. You further acknowledge that Software may include technical data subject to export and re-export restrictions imposed by US law.

13. High Risk Activities. The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). MCAFEE EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

14. Governing Law. This Agreement will be governed by and construed in accordance with the substantive laws in force: (a) in the State of New York, if you purchased the Software in the United States, Mexico, Central America, South America, or the Caribbean; (b) in the Republic of Ireland, if you purchased the Software in Canada, Europe, Middle East, Africa, Asia, or the region commonly referred to as the Pacific Rim; and (c) in Japan if you purchased the Software in Japan. If you purchased the Software in any other country, then the substantive laws of the Republic of Ireland shall apply, unless another local law is required to be applied. This Agreement will not be governed by the conflict of laws rules of any jurisdiction or the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. The United States District Court for the Southern District of New York, and the Courts of New York County, New York, when New York law applies, the courts of the Republic of Ireland, when the law of Ireland applies, and the courts of Japan when Japanese law applies, shall each have non-exclusive jurisdiction over all disputes relating to this Agreement.

15. Free Software. This product includes or may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL, which is distributed to someone in an executable binary format that the source code also be made available to those users. For any such software, the source code is made available in a designated directory created by installation of the Software or designated internet page. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.

16. Privacy. By entering into this Agreement, you agree that the McAfee privacy policy, as it exists at any relevant time, shall be applicable to you. The most current privacy policy can be found on the McAfee web site (www.McAfee.com). By entering into this Agreement, you agree to the transfer of your personal information to McAfee's offices in the United States and other countries outside of your own.

17. Collection of Certain System Information. McAfee employs certain applications and tools through its website and within the McAfee Software, to retrieve information about your computer system to assist us in the provision and support of Software that you have chosen to subscribe to or use. This information is essential to enable us to provide you with quality service and up to the minute threat protection; and for these reasons, there is no opt-out available for this information collection.

18. Audit. McAfee may, at its expense and upon reasonable notice to customer during standard business hours audit customer with respect to its compliance with the terms of this Agreement. Customer understands and acknowledges that McAfee utilizes a number of methods to verify and support software use by its customers. These methods may include technological features of the McAfee software that prevent unauthorized use and provide software deployment verification, which will be automatically reported to McAfee. In the event that McAfee requests a report for confirmation, customer will provide a system generated report verifying customer's software deployment, such request to occur no more than four (4) times per year. In the event that McAfee requires a physical audit, such audit shall be preceded by thirty (30) days written notice and shall occur no more than once per year unless otherwise required for compliance with the Sarbanes-Oxley Act.

19. Auto-Boot /Post Boot Mode. McAfee shall have no liability to you for any damages resulting from the use of the Software in the "auto-boot" or "post-boot" mode. You are advised that such tools are designed for product deployment purposes only, and any other use does not provide adequate data security. Any such contrary use shall be at your sole risk. Moreover, in the event of a data breach resulting from such contrary use, you shall not publicize McAfee's name in connection with such breach, nor make any statements that unfairly disparage the reputation of McAfee products.

20. Miscellaneous. This Agreement sets forth all rights for the user of the Software and is the entire Agreement between the parties. This Agreement supersedes any other communications, representations or advertising relating to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect.

21. McAfee Customer Contact. If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call (408) 992-8599 or (866) 622-3911, FAX to (972) 963-7001, or write: McAfee, Inc., Attention: Customer Service, 5000 Headquarters Drive, Plano, TX 75024, or e-mail to http://www.mcafeehelp.com. Alternatively, you may contact your local McAfee entity at the number listed at http://www.McAfee.com.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
USA

Document Version: MFE_DBS_1.0
Product Version: 4.0.0
Publication Date: July 2010

Table of Contents

1 Introducing McAfee Database Security

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.

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 addition, users of McAfee Vulnerability Manager can test the security level of their databases.

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
- Advanced vulnerability assessment and security scanning
- Integration with ePolicy Orchestrator

1.1 Available Product Versions

- **McAfee Integrity Monitor**: This version provides monitoring and management of database activity for change management purposes, and basic reporting functionality. (This version does not include vulnerability assessment and vPatch functionality.) The Integrity Monitor can be upgraded to McAfee Database Activity Monitoring or Vulnerability Manager, or both.
- **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, as well as an optional security update service. (This version does not include data activity monitoring and vPatch functionality.)

Note: Product features depend on the product version used. When a function is unavailable in the version you are using, the UI will inform you that you need a different license to enable the feature.

1.2 Deployment

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

The McAfee Database Security solution comprises three components:

- **McAfee Database Security Server**: A J2EE server that manages all system components and integrates with McAfee ePO.
- **McAfee Database Security Web Console**: A rich Web-based GUI dashboard that connects to the Security Server and enables the administrator to review alerts, and define rules and policies.
- **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 DBMS(s) in real-time. 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 via the McAfee Database Security Web Console, the Server logs the transaction, issues an alert, and/or prevents access to the DBMS. The sensor is not required for users of Vulnerability Manager.

1.3 Installation Workflow

The McAfee Database Security installation includes the following procedures:

- Install the McAfee Database Security Server (refer to 2 Installing the McAfee Database Security Server)
- Install the Sensor (unless you intend to use Vulnerability Manager only).

If you are installing the Integrity Monitor version, you need to perform the following additional steps:

- Configure Integrity Rules (Integrity Monitor only)
- Add VA DBMS (Integrity Monitor)

If you intend to use Vulnerability Manager only:

- Add VA DBMS/s
- Finally, integrate the Database Security Server with McAfee ePO (refer to *Integrating McAfee Database Security within ePolicy Orchestrator).*

2 Installing the McAfee Integrity Monitor Version

This section describes how to install and configure the McAfee Integrity Monitor version of McAfee Database Security.

Note: This version does not include McAfee Database Activity Monitoring and Vulnerability Management functionality.

This section includes the following procedures:

- 2.1 Installing the McAfee Database Security Server
- 2.2 Configuring McAfee Database Security for Integrity Monitoring

2.1 Installing the McAfee Database Security Server

The McAfee Database Security Server is a J2EE server that manages all system components and communicates with ePO.

The McAfee Database Security Server can be installed on a machine running the Windows 2003/2008 Server or Windows XP/Vista operating system. For other operating systems (Linux or Solaris), contact technical support.

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

Before attempting to install the McAfee Database Security Server, verify that the machine on which the server is to be installed meets the following minimum requirements:

- 1 GB free RAM
- 2 GB free disk space

To install the McAfee Database Security Server:

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**. The Choose Product Type window is displayed.
3. Select **McAfee Integrity Monitoring** and click **Next**. The License Agreement window is displayed.
4. Read the license agreement carefully, and then click **I agree** to indicate your agreement and continue with the installation. The Choose Install Location window is displayed.
5. Enter or browse to the location in which you want to install the application and click **Next**. The Administrator Configuration window is displayed.
6. Enter the administrator name and password. (It is recommended that you create a strong password, containing 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**. The Configuration window is displayed.

8 Configure the server listening ports as follows:

- In the **HTTP/1.1 Connector Port** and **HTTPS/1.1 Connector Port** fields, enter the desired management port numbers or leave the default settings unchanged. (It is recommended 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, enter the number of the port on the server that will be used by the sensor to communicate with the server.

9 Click **Install**.

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

10 Select the relevant backend database type and click **Next**.

Notes:

An internal database can be used for an evaluation installation only.

If you select **Oracle/MSSQL External Database**, see the Working with External Databases section in the *McAfee Database Security User's Guide* before proceeding.

11 Click **Next**. The Completing the Setup Wizard window is displayed.

12 Verify that the **Run McAfee Database Security Server service** checkbox is selected and click **Finish**. The server is successfully installed on your machine and you are prompted to log into the McAfee Database Security console.

Notes:

If you are installing the McAfee Database Security Server on a Windows XP platform, the installation process might not be able to set the correct permissions. After the installation, verify that only the administrator has read permissions on the McAfee Database Security Server internal database located at: < **McAfee Database Security Server installation directory>\webapps\ROOT\WEB-INF\hsqldb_data**.

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

2.2 Configuring McAfee Database Security for Integrity Monitoring

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

Although McAfee Integrity Monitor requires the configuration of both Database Activity Monitoring and Vulnerability Assessment, it is important that you configure the Database Activity Monitoring first.

To configure the Integrity Monitor version:

1. Log in to the McAfee Database Security console using the username and password specified in the server installation process.
2. In the Choose your configuration page, click the **Configure sensors** link. 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 4 Installing the Sensor.
4. Approve the sensor, as described in 5.2 Approving the Sensors.
5. When the sensor installation is complete and the sensor has been approved, the Integrity Rules page is displayed in the McAfee Database Security console. Configure the Integrity rules as described in 5.3 Configuring Integrity Rules.
6. Configure the DBMS(s) that are to be used for Vulnerability Assessment, as described in 5.4 Configuring VA DBMSs. (This is required to create reports on current DBMS users, user and role privileges and more.)
7. After completing all stages. you should integrate the Security Server with ePO. Refer to *Integrating McAfee Database Security within ePolicy Orchestrator.*

3 Installing McAfee Database Security

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

This section includes the following procedures:

- 3.1 Installing the McAfee Database Security Server
- 3.2 Configuring McAfee Database Security Manager

3.1 Installing the McAfee Database Security Server

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 machine running the Windows 2003 Server and up or Windows XP/Vista operating system.

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

Before attempting to install the McAfee Database Security Server, verify that the machine on which the server is to be installed meets the following minimum requirements:

- 1 GB free RAM
- 2 GB free disk space

To install the McAfee Database Security Server:

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**. The Choose Product Type window is displayed.
3. Select **McAfee Database Security** and click **Next**. The License Agreement window is displayed.
4. Read the license agreement carefully, and then click **I agree** to indicate your agreement and continue with the installation. The Choose Install Location window is displayed.
5. Enter or browse to the location in which you want to install the application and click **Next**. The Administrator Configuration window is displayed.
6. Enter the administrator name and password. (It is recommended that you create a strong password, containing 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**. The Configuration window is displayed.

8 Configure the server listening ports as follows:

- In the **HTTP/1.1 Connector Port** and **HTTPS/1.1 Connector Port** fields, enter the desired management port numbers or leave the default settings unchanged. (It is recommended 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, enter the number of the port on the server that will be used by the sensor to communicate with the server.

9 Click **Install**.

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

10 Select the relevant backend database type and click **Next**.

Notes:

An internal database can be used for an evaluation installation only.

If you select **Oracle/MSSQL External Database**, see the Working with External Databases section in the McAfee Database Security User's Guide before proceeding.

11 Click **Next**. The Completing the Setup Wizard window is displayed.

12 Verify that the **Run McAfee Database Security Server service** checkbox is selected and click **Finish**. The server is successfully installed on your machine and you are prompted to log into the McAfee Database Security console.

Notes:

If you are installing McAfee Database Security Server on a Windows XP platform, the installation process might not be able to set the correct permissions. After the installation, verify that only the administrator has read permissions on the McAfee Database Security Server internal database located at: **< McAfee Database Security Server installation directory>\webapps\ROOT\WEB-INF\hsqldb_data**.

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

3.2 Configuring McAfee Database Security Manager

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

To configure McAfee Database Security:

1 Log in to the McAfee Database Security console using the username and password specified in the server installation process.

2 In the Choose your configuration page, click the **Configure sensors** link. 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 4 Installing the Sensor.

4 Approve the sensor, as described in 5.2 Approving the Sensors.

5 After completing all stages, you should integrate the Security Server with ePO. Refer to *Integrating McAfee Database Security within ePolicy Orchestrator.*

4 Installing the Sensor

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

Before attempting to install the McAfee Database Security Sensor, verify that the database host server on which the McAfee Database Security Sensor is to be installed meets the requirements specified in section 6 Installation Prerequisites and Default Installation Locations.

Note that installing the sensor creates a new OS user on Unix/Linux platforms named “mfedbs”, a member of the dba, oinstall groups (if the groups exist). If the groups do not exist, refer to 6. Installation Prerequisites and Default Installation Locations.

For additional system and database requirements, refer to 6.1 Prerequisites and Default Locations for Monitored Database Installations.

The installation procedure varies according to the type of machine, as described in the following sections:

- 4.1 Installing the McAfee Sensor on a Redhat Linux or SUSE Machine
- 4.2 Installing the McAfee Database Security Sensor on a Sun Solaris Machine
- 4.3 Installing the McAfee Database Security Sensor on an AIX Machine
- 4.4 Installing the McAfee Database Security Sensor on an HPUX Machine
- 4.5 Installing the McAfee Database Security Sensor on a Windows Machine

4.1 Installing the McAfee Sensor on a Redhat Linux or SUSE Machine

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

To install the sensor on a Redhat Linux or SUSE machine:

1 Download the **rpm.bin** file for the sensor from the Download page of 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**.

3 Copy the file to the database machine.

4 Log in as the root user.

5 Run the following command:

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

Follow the on-screen instructions:

Optional parameters:

Usage: <installation file path>/mfe-dbs-sensor-<version#>-<build#>.<architecture>.rpm.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.

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

6 Follow the on-screen instructions. Once you accept the end user license agreement, the install script creates and installs an RPM file named **mfe-dbs-sensor-<version #>.rpm**.

During the installation you will need to enter the McAfee Database Security Server's IP address and listening port to ensure the communication between the sensor and server.

7 Run the following command to start the sensor service:
/sbin/service mfe-dbs-sensor start

Note: On older distributions, run the command **/etc/init.d/mfe-dbs-sensor start**.

To uninstall the sensor:

- Log in as root and run the following command:
rpm -e mfe-dbs-sensor

4.2 Installing the McAfee Database Security Sensor on a Sun Solaris Machine

The McAfee Database Security Sensor is installed on a Sun Solaris machine using a PKG file.

To install the sensor on a Sun Solaris machine:

1 Download the sensor from the Download page of 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 machine.

3 Log in as root and run the following 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: sh <installation file path>/mfe-dbs-sensor-<version#>-<build#>.<architecture>.pkg.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.

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

5 During the installation you will be prompted to enter the McAfee Database Security Server's IP address and listening port.

6 Run the following command to start the service:
/etc/init.d/mfe-dbs-sensor start

To uninstall the sensor:

- Log in as root and run the following command:
pkgrm mfe-dbs-sensor

4.3 Installing the McAfee Database Security Sensor on an AIX Machine

The McAfee Database Security Sensor is installed on an AIX machine using a BFF package.

To install the sensor on an AIX machine:

1 Download the bin file from the Download page of 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#>.bff.bin**

2 Copy the file to the database machine.

3 Log in as root and run the following command to install the sensor:

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

4 Follow the on screen instructions.

Optional parameters:

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

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

5 During the install you will be prompted to enter the McAfee Database Security server IP address and listening port.

6 Run the following command to start the service:
/etc/rc.d/init.d/mfe-dbs-sensor start

To uninstall the sensor:

- Log in as root and run the following command:
installp -u mfe-dbs-sensor

4.4 Installing the McAfee Database Security Sensor on an HPUX Machine

The McAfee Database Security Sensor is installed on an HPUX machine using a DEPOT file.

To install the sensor on an HPUX machine:

1 Download the HPUX for the sensor from the Download page of 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 machine.

3 Log in as root and run the following 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.

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

5 During the installation you will be prompted to enter the McAfee Database Security Server's IP address and listening port.

6 Run the following command to start the service:
/sbin/init.d/mfe-dbs-sensor start

To uninstall the sensor:

- Log in as root and run the following command:
swremove mfe-dbs-sensor

4.5 Installing the McAfee Database Security Sensor on a Windows Machine

The McAfee Database Security Sensor is installed on a Windows machine using a Setup Wizard.

To install the sensor on a Windows machine:

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

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

2 Run the installation file. The Welcome window of the McAfee Database Security Sensor Setup Wizard is displayed.

3 Click **Next**. The License Agreement is displayed.

4 Read the license agreement and select **I agree** to indicate your acceptance of its terms. The Choose Install Location window is displayed.

5 Browse and select the location in which you want to install the sensor (or leave the default setting), and click **Next**. The Server Connection Settings window is displayed.

6 Enter the Server IP address and Server listening ("connector") port details in the designated fields, and click **Install**. The Installing window is displayed briefly.

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

7 Click **Finish**. The installation is complete.

To uninstall the sensor:

- From the **Start** menu, select **Programs | McAfee Database Security Sensor | Uninstall**. When the confirmation message is displayed, click **Yes**. The Uninstalling window is displayed briefly. When the uninstall process is complete, a popup message is displayed indicating that the sensor has been uninstalled.

4.6 Troubleshooting the Sensor Installation

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

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

4.6.1 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 into the McAfee Database Security console, follow the steps outlined in the sections below:

Check if the McAfee Database Security Sensor process is up and running:

- On Linux/Solaris, run: /etc/init.d/mfe-dbs-sensor status
- On AIX, run: /etc/rc.d/init.d/mfe-dbs-sensor status
- On HPUX, run: /sbin/init.d/mfe-dbs-sensor status
- On Windows: run **services.msc** and look for the service "McAfeeSensor"

If the Sensor service is down and does not come up after you run it, check that the McAfee Database Security Server has a valid license. Note that if the sensor was connected to the server before applying the license, it will be down and you need to manually restart it.

If you are still unable to run the McAfee Database Security Sensor, contact McAfee support after running the diagnostic tool (see 4.6.2 Running the Diagnostic Tool).

If the McAfee Database Security Sensor is not on the McAfee Database Security Server Sensors’ list:

1. Verify that the server IP and port are set correctly in the Sensor's configuration file (located in Linux: /etc/sysconfig/mfe-dbs-sensor, Solaris: /etc/default/mfe-dbs-sensor, AIX: /etc/mfe-dbs-sensor, HPUX: /etc/rc.config.d/mfe-dbs-sensor and on Windows run McAfeeDBSConfig.exe).

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

2. Verify that the sensor is able to reach the server port, using ping <server ip> and telnet <server ip> <port number>.

   - If it 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 and restart the McAfee Database Security Sensor service.
   - If you are still unable to reach the McAfee Database Security Server machine from the McAfee Database Security Sensor machine, contact your system administrator for support.

  - If the McAfee Database Security Server IP address and port are reachable from the McAfee Database Security Sensor machine and you still do not see the Sensor on the Sensors list on the McAfee Database Security Server, run the diagnostic tool (see 4.6.2 Running the Diagnostic Tool) and then contact McAfee support for assistance.

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

- On Windows platforms, run the diagnostic tool (see 4.6.2 Running the Diagnostic Tool) and 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 and 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 accordingly (on Linux/Solaris: /etc/init.d/mfe-dbs-sensor, on AIX: /etc/rc.d/init.d/mfe-dbs-sensor, on HPUX: /sbin/init.d/mfe-dbs-sensor) by adding "-r <oratab full path>/oratab" to the start function.
  - 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 Oracle is version 8.1.7 and above or MS SQL Server 2000 or 2005, Sybase 12.5 or 15.0.
   When 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, please add the relevant Oracle group to the 'mfedbs' OS user
2. If the McAfee Database Security Sensor is still unable to monitor your DBMSs, run the diagnostic tool (see 4.6.2 Running the Diagnostic Tool) and then contact McAfee support for assistance.

4.6.2 Running the Diagnostic Tool

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

1. Change the log level from INFO to DEBUG in the dbssensor configuration file as follows:
   - On Linux, run: **/etc/sysconfig/dbssensor**
   - On Solaris, run: **/etc/default/mfe-dbs-sensor**
   - On AIX, run: **/etc/mfe-dbs-sensor**
   - On HPUX, run: **/etc/rc.config.d/mfe-dbs-sensor**
   - On Windows, run **mcafeeDBSconfig.exe**

   Follow the instructions and change the log level to Debug.

2 Run the McAfee Database Security Sensor for 10 minutes.

3 Run the diagnostic tool:

- On Linux, run: **/sbin/service mfe-dbs-sensor create_analytic_package**
- On Solaris, run: **/etc/init.d/mfe-dbs-sensor create_analytic_package**
- On AIX, run: **/etc/rc.d/init.d/mfe-dbs-sensor create_analytic_package**
- On HPUX, run: **/sbin/init.d/mfe-dbs-sensor create_analytic_package**
- On Windows, run: **Analytics.exe**

The analytic package output file name is displayed when the process is complete. Send the file via e-mail to the McAfee support team.

5 Configuring Operations in the Web Console

After installing the McAfee Database Security Server and McAfee Database Security Sensors, you still need to approve the sensor(s) in the McAfee Database Security Web Console.

This section includes the following topics:

- 5.1 Accessing the McAfee Database Security Web Console
- 5.2 Approving the Sensors
- 5.3 Configuring Integrity Rules
- 5.4 Configuring VA DBMSs
- 5.5 Approving the Database(s)

5.1 Accessing the McAfee Database Security Web Console

The McAfee Database Security Web Console can be accessed using either of the following 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, refer to the McAfee Database Security User's Guide.

To access the McAfee Database Security Console:

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.

   The Welcome page is displayed.

2. Enter the administrator username and password as configured during the installation, and 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 5.2. Approving the Sensors.

   Notes:

   If you have not yet installed a sensor, you are prompted to do so at this time. Refer to 4. Installing the Sensor or click the relevant on-screen link for detailed instructions.

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

5.2 Approving the Sensors

McAfee Database Security Sensors are responsible for monitoring access to the database(s) and sending transaction data to the McAfee Database Security Server. After installation, a sensor needs to be approved in the Sensors list before it can begin active monitoring of the database(s).

The Sensors page lists the installed McAfee Database Security Sensor(s).

In the Sensors page, 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.

To approve a sensor (no issue detected scenario):

- In the Sensors page, if the APPROVE... button appears in the **Approved By** column, click the icon to approve the sensor.

  If a new sensor reports that it is monitoring a database that is already recognized by the McAfee Database Security system, the Approve Database page is displayed prompting you to select the databases to be monitored. For details, see 5.5 Approving the Database(s).

To approve a sensor (when a duplicate sensor is discovered):

1. In the Sensors page, if the sensor ID already exists in the system, the Approve Sensor dialog is displayed.
2. From the **Available actions** dropdown 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 a single 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 icon in the **Approved By** column is replaced by the name of the logged on user.

   If a new sensor reports that it is monitoring a database that is already recognized by the McAfee Database Security system, the Approve Database page is displayed prompting you to select the databases to be monitored. For details, see 5.5 Approving the Database(s).

5.3 Configuring Integrity Rules

The McAfee Integrity Monitor is provided with predefined Integrity rules. You can enable and disable specific rules, and edit the actions that are taken when a rule violation is detected.

When the sensor installation is complete and the sensor has been approved, the Integrity rules page is displayed in the McAfee Database Security console.

Note: This section is applicable only when McAfee Integrity Monitoring is selected in the McAfee Database Security Setup wizard.

5.3.1 Enabling/Disabling Integrity Rules

The current status of a rule in the Rules list is indicated by the icon in the leftmost column:

- ✅: The rule is enabled.
- ⊟: The rule is disabled.

To enable a rule:

- In the Rules list, click ⊟ in the row for the rule that is to be enabled. The rule is enabled and the ✅ icon is displayed.

To disable a rule:

- In the Rules list, click ✅ in the row for the rule that is to be disabled. The rule is disabled and the ⊟ icon is displayed.

5.3.2 Viewing the Integrity Rule Properties

You can view the details of a specific rule in Rule properties page.

To view a rule's properties:

- In the Rules list, click the **Properties** icon 📝 in the row for the rule. The Rule Properties page is displayed.

5.3.3 Configuring the Action for an Integrity Rule

In addition to enabling or disabling an Integrity rule, you can define the alert level and the action to be taken when the conditions of a specific rule are met (send alert to console, send email, terminate session and so on). For details, see Configuring the Action for a vPatch Rule in the McAfee Database Security User's Guide. (The available actions for an Integrity rule are the same as for vPatch rules.)

5.3.4 Creating Integrity rule exceptions

In some case you will find that rules create alerts that your policy does not require. You can create exception so that a rule will not apply to a specific database, to a specific user, an application and so on.

Examples:

a. To prevent a rule from running on a database called "hr_staging" add the following exception: dbms_name = 'hr_staging'

b. To prevent a rule from triggering an alert when the user is dan and the application's name is sqlplus.exe add the following exception: user = 'dan' and application = 'sqlplus.exe'

5.4 Configuring VA DBMSs for Integrity Monitoring Users

Integrity Monitoring uses the VA module for creating reports on database users, their privileges and more. Multiple DBMSs can be configured for vulnerability assessment. VA DBMSs are not automatically added to the configuration, even if they are already monitored by a sensor.

You can manually add a VA DBMS or you can perform a network scan to create a VA DBMS for a database instance in the scan results.

The procedure below describes how to manually add a VA DBMS. For details on creating a VA DBMS from scan results, see the McAfee Database Security User's Guide.

Note: This section is applicable only when McAfee Integrity Monitoring is selected in the McAfee Database Security Setup wizard.

To add a VA DBMS:

1 In the DBMSs page, click **Add VA DBMS**. The Add VA DBMS page is displayed.

1 From the **DBMS type** dropdown list, select the database type (for example, Oracle or MS SQL).

2 In the **Host** field, enter the name of the host server or IP address and click **Check Host** to verify the validity of the name/IP.

3 Configure the following host parameters:

- Select **Port** and enter the port number to be used for connecting to the database. Then click **Check Port** to check its validity.
- Select **Instance Name** and enter the name of the database instance on the server. Then click **Check Instance** to check its validity.

4 In the **User Name** and **Password** fields, enter the user name and password to be used to connect to the DBMS. Scripts that create a user with the correct and minimal privileges for scanning are available in the screen.

5 Click **Check Connection** to check the connectivity between the VA server and the database.

6 (Optional) Click **Advanced** to configure additional VA parameters (used for troubleshooting purposes only):

- **Connection String**: The database connection string.
- **Connection Properties**: Properties typically used by tech support personnel for troubleshooting/alternative connection purposes.
- **Enable alternative DBMS connection (advanced users only, for DAM only)**: When selected, alternative connections can be made using the following parameters:

  User Name: The user name to be used to connect to the DBMS.

  Password: The password to be used to connect to the DBMS.

  Connection String: The connection string to be used to connect to the DBMS. This parameter is applicable for Oracle DBMSs only.
- **McAfee Database Security Cache Size**: The size of the cache that can be used by the DBMS. This parameter is applicable for MS SQL DBMSs only (do not change the size unless instructed to do so by tech support).
- **DBMS Groups**: The DBMS groups to which this DBMS belongs.

7 Click **Save**. The DBMS is added to the DBMSs list.

Notes: To clear all filter selections, click **Clear** and then **Apply**.

5.5 Approving the Database(s)

If a new sensor reports that it is monitoring a database that is already recognized by the McAfee Database Security system, the approve Database page is displayed when you attempt to approve the sensor.

To approve the database(s):

1. In the Approve DBMS page, select the databases to be monitored by the sensor.

   If more than one database has the same name, select one of the following from the adjacent dropdown list:

   - **New**: Indicates this is a new database that needs to be monitored separately from the existing database.
   - **Merge**: Indicates this database is the same database and the entries should be merged.
2. Click **Save** to complete the approval process. The Congratulations page is displayed.

6 Installation Prerequisites and Default Installation Locations

This section includes the following topics:

- 6.1 Default Locations for Monitored Database Installations
- 6.2 Prerequisites and Default Locations for McAfee Database Security Server Installations
- 6.3 Additional Installation Requirements

6.1 Prerequisites and Default Locations for Monitored Database Installations

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

6.1.1 Supported DBMSs and Operating Systems for Database Monitoring

The following DBMSs and Operating Systems are supported (contact McAfee support if your platform is not supported):

OS	OS Version	DBMS
Windows (32/64bit/Itanium)	Windows 2000 and up	SQL 2005, SQL, SQL 2000, SQL 2008, Oracle 8i and up Sybase ASE 12.5, 15.0
AIX	5.2 and up	Oracle 8i and up Sybase ASE 12.5,15.0
HPUX (Itanium/PA-RISC)	11.11 and up	Oracle 8i and up Sybase ASE 12.5,15.0
Linux (Itanium/32/64 bit)	RH 2.4 and up SUSE 9 and up	Oracle 8i and up Sybase ASE 12.5,15.0
Solaris (Intel or Sparc, 32/64 bit)	8,9,10	Oracle 8i and up Sybase ASE 12.5,15.0

6.1.2 Supported VA DBMSs

- Oracle 9g, 10g, 11g on all OS platforms
- MS SQL 2000, 2005, 2008 on all OS platforms
- MySQL 3.23 and up on all OS platforms
- DB2 LUW 8.1, 8.2, 9.1, 9.5, 9.7

6.1.3 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.

6.1.4 Default Installation Directories

The following table lists default installation directories per 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”

6.1.5 Dependencies per Oracle Platform

The following table lists the dependencies per Oracle platform. Please ensure that the packages listed are installed on the database server.

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 - xlC.aix50 - xlC.msg.Ja_JP - xlC.msg.en_US - xlC.msg.ja_JP - xlC.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
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	N/A
Solaris	N/A
Windows	N/A

6.1.6 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 prior to 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 (e.g. usermod –G group1, group2).

6.2 Prerequisites and Default Locations for McAfee Database Security Server Installations

The following are the prerequisites for the server installation:

- Dedicated server, running Windows XP/Server 2003 and up
- 1 GB RAM (2 GB preferable), at least 2 GB free disk space
- Default installation directories per platform, as follows:

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

6.3 Additional Installation Requirements

The following additional requirements must be 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)

7 Upgrading McAfee Database Security

This section includes the following topics:

- 7.1 Upgrading the McAfee Database Security Server
- 7.2 Upgrading McAfee Database Security Sensors

Whenever new McAfee Database Security sensors are available it is highly recommended to upgrade the McAfee Database Security system. To do this you will first need to update the McAfee Database Security Server and only then upgrade the sensors.

While the upgrade process is very simple and thoroughly tested, it is always recommended to back up the McAfee Database Security data before performing upgrades. For information about back up and restoration, download the document “Backup_Guide” from McAfee’s support portal.

Note: Always use sensors whose release number is equal to or lower than the server’s release number (e.g. McAfee Database Security Sensor version 4.5 cannot be used with McAfee Database Security Server version 4.1). Servers are always backward compatible (Sensor version 4.1 can be used with Server version 4.5).

7.1 Upgrading the McAfee Database Security Server

Download the latest server installer for your operating system from the McAfee support portal. You do not need to download sensor installations (this will be done by the server at a later stage).

After downloading install the new server in the same location where the current server is installed. During the upgrade process all data and configurations will be saved and will be available in the new server.

7.2 Upgrading McAfee Database Security Sensors

After upgrading the server, you can find out whether new sensor updates are available in the **Updates/Software Updates** tab in 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 wish to receive updates automatically, download the latest sensor installer(s) from the support portal and proceed to manual update.

All of your sensors are listed in the **Updates/Software Updates** tab, including information regarding the newest available update for each sensor. To receive the latest information, click **Check for new McAfee Database Security sensors**.

Select the sensors that you would like to update and click **Remote update**. Before updating a sensor, make sure that the sensor is connected.

All sensor update files will be downloaded from the McAfee portal and the sensors will be updated. Accordingly, the status of chosen sensors will change 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 ☒ (cancel update) button to abort the update.

Note: Depending on several factors (including the network bandwidth), the process may take several minutes. If a sensor is not connected the update job may wait up to an hour before attempting the update again. If a sensor is connected and the update does not succeed within 2 hours, it is recommended to perform a manual update.

If you choose to manually update the sensor, simply log in to the sensors system, and follow the relevant sensor installation instructions provided in this document. Installing the sensor without uninstalling the previous sensor will keep the current configuration (server IP address, listening port, and so on).