COPYRIGHT
Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS
Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and 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**

- About this guide ................................................................. 9
- Audience .................................................................................. 9
- Conventions ............................................................................ 9
- Find product documentation ................................................... 10

1 **Introduction**

- Key features ............................................................................ 11
- Available product versions ..................................................... 12

2 **Deployment**

- Solution components ............................................................ 13
- McAfee Database Security server and sensor management .......... 13
  - Manage the Database Security Server process ......................... 14
  - Tune McAfee Database Security Server performance ................. 14

3 **McAfee Database Security web console**

- Access the web console .......................................................... 17
- McAfee Database Security web console components .................. 17
- System-wide functionality ....................................................... 18
  - Sort data ............................................................................. 18
  - Filtering data ....................................................................... 19
  - Change your password ........................................................ 21
  - View license information ..................................................... 21
  - Upgrade license information ................................................. 22
  - Log out ............................................................................... 22

4 **Alerts**

- Alerts list ................................................................................ 23
- Filter the Alerts list ................................................................. 24
- View alert details ..................................................................... 25
- Handling alerts ....................................................................... 27
  - Resolve an alert ................................................................... 27
  - Resolve multiple alerts ....................................................... 28
  - Create a rule based on an alert ............................................. 28
  - Create trust for a session ..................................................... 29
  - Create a rule exception based on an alert .............................. 29
  - Terminate a session ............................................................. 30
  - Generate alert reports ........................................................ 30
  - Archive alerts ...................................................................... 30
- Managing resolve types ......................................................... 31
  - Create a resolve type .......................................................... 31
  - Edit a resolve type name ..................................................... 31
  - Delete a resolve type ........................................................... 31

5 **VA results**

- VA results list ......................................................................... 33
- Filter the VA results list .......................................................... 33

---

**McAfee Database Security 4.6.x**

**Product Guide**

---
Handling VA results ................................................................. 35
Resolve a VA result ..................................................................... 35
Resolve multiple VA results ....................................................... 35
Archive VA results ..................................................................... 36

6 McAfee Database Security Dashboard ........................................ 37
Dashboard components ............................................................. 37
Viewing dashboard data ............................................................. 38
Recalculate chart data ............................................................... 38
Filter the dashboard alerts ......................................................... 38
Set the number of most active rules ......................................... 38

7 Rules ....................................................................................... 39
Rules and monitoring policy ....................................................... 39
Viewing rules ............................................................................. 40
Rules list .................................................................................... 40
Enabling and disabling rules ..................................................... 41
Enable a rule ............................................................................. 41
Disable a rule ........................................................................... 42
Managing vPatch rules ............................................................... 42
View the properties of a vPatch rule ........................................ 42
Configure the action for a vPatch rule ..................................... 43
Configure the action for a DBMS ............................................. 44
Update the security level of the vPatch rules ......................... 46
Installing or removing vPatch rules ......................................... 46
Managing custom rules ............................................................. 47
Create a custom rule ............................................................... 48
Clone a rule ............................................................................ 52
Change the order of custom rules ............................................ 52
Edit a custom rule ................................................................... 53
Remove a custom rule ........................................................... 53
Importing and exporting rule settings ...................................... 54
Export rule settings ................................................................. 54
Import rule settings ................................................................. 54
Rule syntax .............................................................................. 54
Identifiers .............................................................................. 55
Operators .............................................................................. 57
Rule examples ........................................................................ 58
Managing rule objects ............................................................ 59
Create a static/active directory rule object ............................... 59
View or edit rule object properties .......................................... 60
Delete a rule object ............................................................... 60
DVM-based rule objects .......................................................... 60
Script configuration ............................................................... 62
Configure a signed script ......................................................... 62
View or edit a signed script ..................................................... 63
Application mapping ............................................................... 63
Create an alert rule ................................................................. 64
Create a mapping exception rule ............................................ 64
Working with tags ................................................................... 65
Assign tags to rules ............................................................... 65
Assign rules to DBMSs based on tags ..................................... 65
View tags per DBMS/DBMS group ......................................... 66
Importing and exporting rules ................................................ 67
Export rules ........................................................................... 67
View DML monitoring results ................................................................. 104
Enable or disable DML triggers ............................................................ 104
Enable or disable redo buffer monitoring ............................................. 104
Configure failed logins ........................................................................ 105
Configure the character set .................................................................. 105
Enable application mapping .................................................................. 105
View sensors by DBMS .......................................................................... 106
Monitor a clustered database ................................................................. 106
Working with network scans ................................................................. 106
View network scan results .................................................................. 107
Filter the network scan results .............................................................. 107
Create a network scan ......................................................................... 107
Create a VA DBMS from scan results .................................................. 109
Clone a network scan .......................................................................... 109
Stop a network scan ............................................................................ 110
Rerun a network scan .......................................................................... 110
Delete a network scan ......................................................................... 110
Managing DBMS groups ....................................................................... 110
Create a DBMS group ......................................................................... 111
View/edit a DBMS group ..................................................................... 111
Delete a DBMS group .......................................................................... 111
Apply DBMS actions ........................................................................... 112

13 Roles .................................................................................................. 113
Predefined roles .................................................................................... 113
Roles list ................................................................................................ 114
View role details ................................................................................... 114
Create a new role ................................................................................ 115
Edit the permissions of an existing role .............................................. 116
Remove a role ....................................................................................... 116

14 Users .................................................................................................. 117
Users list ................................................................................................ 117
Managing users .................................................................................... 118
Add a user ............................................................................................. 118
View user details .................................................................................. 119
Change a user’s permissions ................................................................. 119
Change a user’s password .................................................................... 120
Remove a user ....................................................................................... 120
Export users .......................................................................................... 120
Import users .......................................................................................... 121
Configure password policy .................................................................... 121

15 System ................................................................................................. 122
Configuring system interfaces .............................................................. 122
Configure the outgoing e-mail account ................................................. 122
Configure LDAP .................................................................................... 123
Configure SNMP ................................................................................... 124
Configure the Syslog ............................................................................ 125
Configure the Windows event log ......................................................... 127
Configure log to file .............................................................................. 128
Configure VPN-1 blocking .................................................................... 128
Configure the XML API .......................................................................... 129
Configure the Analytics Module ........................................................... 129
Alert archiving ....................................................................................... 130
Configure automatic alert archiving ................................................................. 130
Configure manual alert archiving .................................................................... 131
Reload a whole archive ..................................................................................... 131
Rearrange alerts ............................................................................................... 132
Remove an alert archive ................................................................................... 132
Quarantining users ............................................................................................ 132
Configure the quarantine parameters ............................................................... 133
Remove a user from quarantine ....................................................................... 133
Viewing clusters .............................................................................................. 133
Viewing action history ..................................................................................... 134
Set the time period for saving actions history ................................................ 134
View actions history details ............................................................................. 134
Configuring and downloading server logs ....................................................... 135
Configure the server logs ................................................................................ 135
Download the server logs ............................................................................... 135
Configure automatic resolution of IP addresses ............................................ 135
Viewing system messages ............................................................................... 136
View system message details ......................................................................... 136
Mark system messages as read or unread ......................................................... 137
Delete a system message ............................................................................... 137
Configure system messages .......................................................................... 137
View backend DBMS details .......................................................................... 138
Updates ............................................................................................................. 138
Configure security update settings .................................................................. 139
Manually check for/install vpatch security updates ....................................... 139
Manually check for/install VA security updates ............................................ 140
Manually check for and install server software updates .................................. 140
Manually check for/install sensor software updates ....................................... 140
Install offline updates ..................................................................................... 140
View the update history ................................................................................... 141
Reports ............................................................................................................. 141
Generating system reports ............................................................................ 141
Working with dynamic reports ..................................................................... 142
Configure the report settings ....................................................................... 147
XML API .......................................................................................................... 147
Sensor service ................................................................................................. 148
Alert service .................................................................................................... 148
Working with external databases .................................................................... 149
Migrating the internal database to an external database ................................ 150
Change the configured password for the external database ....................... 152
Create your own database (advanced configuration) ..................................... 154
Working with the McAfee Database Security Server in Cluster mode ............ 154
Configure your McAfee Database Security Servers to work in Cluster mode 154
Troubleshooting ............................................................................................. 156
Backup and recovery ....................................................................................... 157
Back up the server configuration files ............................................................ 157
Back up the server backend databases ........................................................... 157
Back up the archive files ................................................................................ 158
Recovery .......................................................................................................... 158
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.
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](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

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.
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.

**Note**

For a description of the installation process, see the *McAfee Database Security Installation Guide*.

### McAfee Database Security server and sensor management

#### Tasks

- *Manage the Database Security Server process*
- *Tune McAfee Database Security Server performance*
- *Manage the sensor process*
- *Configure the sensor*
Manage the Database Security Server process
The McAfee Database Security Server process is managed as a Windows service.

Task
1. On Windows, run services.msc and locate the service McAfee Database Security.
2. Select one of these options:
   - **Start** — Starts the McAfee Database Security Server process.
   - **Stop** — Stops the McAfee Database Security Server process.
   - **Restart** — Restarts the McAfee Database Security Server process.
   - **Status** — Checks the status of the McAfee Database Security Server process (running or stopped).

Tune McAfee Database Security Server performance
If you experience performance issues with your McAfee Database Security Server running on a Windows platform, it is recommended that you set your JVM to run in Server mode.

Task
1. Install the Sun Java JDK 1.6.
2. Run McAfeeDBSw.exe, which is located in the McAfee Database Security Server installation bin directory (the default location is: C:\Program Files\Mcafee\McAfee Database Security\bin).
   - The Properties page is displayed.
3. On the **Java** tab, configure the executable to use the jvm.dll located in the server directory in the JRE of the JDK.
   - For example, C:\Program Files\Java\jdk1.6.0\jre\bin\server\jvm.dll
4. Click **Apply**, then restart the McAfee Database Security Server.
5. If you still experience performance problems, contact McAfee support.

Manage the sensor process
The sensor management process varies according to platform.

Task
1. Run the sensor management file for the platform:
   - On Linux/Solaris — /etc/init.d/mfe-dbs-sensor start/stop/restart/status
   - On AIX — /etc/rc.d/init.d/mfe-dbs-sensor start/stop/restart/status
   - On HPUX — /sbin/init.d/mfe-dbs-sensor start/stop/restart/status
   - On Windows — services.msc and locate the service McAfee-DBSSensor
2. Select one of the available options:
   - **Start** — Starts the McAfee Database Security Sensor process.
   - **Stop** — Stops the McAfee Database Security Sensor process.
**Deployment**

McAfee Database Security server and sensor management

- **Restart** — Restarts the McAfee Database Security Sensor process.
- **Status** — Checks the status of the McAfee Database Security Sensor process (running or stopped).

**Configure the sensor**

You can control the McAfee Database Security Sensor by modifying its configuration file.

**Task**

1. Edit the sensor configuration file:
   - On Linux — `/etc/sysconfig/mfe-dbs-sensor`
   - On Solaris — `/etc/default/mfe-dbs-sensor`
   - On AIX — `/etc/mfe-dbs-sensor`
   - On HPUX — `/etc/rc.config.d/mfe-dbs-sensor`
   - On Windows — McAfeeDBSConfig.exe

2. Follow the on-screen instructions to modify these parameters:
   - McAfee Database Security Server host and IP address.
   - McAfee Database Security Sensor log file location, log level, and maximum size and number of log files.
   - McAfee Database Security Sensor update directory. This is the directory used for the Sensor software updates. Each software update occupies about 50 MB. If you are low on disk space at the default location, you can edit this setting and select a different location.
McAfee Database Security web console

The McAfee Database Security Web Console enables you to manage various aspects of the McAfee Database Security functionality, including viewing alerts, approving sensors, defining rules, policies, role and users, and configuring security updates.

Contents
- Access the web console
- McAfee Database Security web console components
- System-wide functionality

Access the web console

The web console can be accessed using these Web browsers:

- Mozilla Firefox 1.5 or above
- Microsoft Internet Explorer 7.0 or above

A minimum of 128-MB RAM is recommended.

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: \( \text{https://<servername>:<port number>} \).

   Note
   The default port number is 8443.

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

McAfee Database Security web console components

The McAfee Database Security web console comprises these pages:

- **Alerts** — Lists the data activity monitoring alerts generated by the McAfee Database Security Server. For details, see Alerts.

- **VA Results** — Lists the results of McAfee Database Security Vulnerability Assessment scans. For details, see VA results list.

- **Dashboard** — Displays a range of statistical data regarding the status of alerts, DBMS monitoring, security updates, and rules. For details, see McAfee Database Security Dashboard.
System-wide functionality

This section addresses specific system-wide functionalities.

Tasks

- Sort data
- Change your password
- View license information
- Log out

Sort data

To facilitate the viewing of data in the McAfee Database Security Web Console, you can set the criteria by which each of the various lists is sorted. You can sort a list according to multiple criteria by setting the hierarchy of sort criteria (such as primary or secondary).
Note
You can sort a list by a single criterion at any time by clicking the head of the column according to which you want to sort the data. Click again to reverse the order (ascending/descending).

Task
1 Click **Sort Options** above the table.

   The current sorting criteria are listed in the **Sort By** pane, in the order in which they take precedence. The sort order is indicated by an (a) for ascending or (d) for descending.

   This example shows the **Sort By** page for the Alerts list. The primary sort criteria is the level of the alert in descending order (high severity first); the secondary sort criteria is the timestamp, also in descending order (most recent first).

   The available columns are listed in the **Table Columns** pane.

2 To sort by a specific data column, select the column name in the **Table Columns** pane. Then click (A-Z) to apply the sort criteria in ascending order or click (Z-A) to apply the sort criteria in descending order. (To reverse the directional setting of a sort criterion, select the column name in the **Sort By** pane, then click (A-Z) and then (Z-A) or (Z-A) as required.)

3 To change the position of the sort criteria, select the column name in the **Sort By** pane, then click (↑) or (↓) to move the column name up or down.

4 To remove a column name from the sort criteria, select the column name in the **Sort By** pane, then click (×).

5 Click **OK** to apply the sort criteria.

Filtering data
You can set the filter criteria that determine the items that are listed on various pages. You can then save the filter criteria as customized filters, eliminating the need to redefine the filter criteria each time you view the respective page.

Tasks
- **Define a filter**
- **Save a filter**
- **Apply a filter**
- **View the filter properties**
- **Delete a filter**

Define a filter
You can filter lists to display data that matches specific criteria.

Although the process for defining a filter varies by page, the basic instructions are the same throughout the system.

Note
Page-specific instructions are provided later in this document for pages that include more complex options.
Task
1. Expand the Edit Filters area above the list.
2. Set one or more filter criteria by entering/selecting the relevant values (for example, name or action).
   You can use one or more of these symbols to define the matching criteria:
   - = Match
   - ! Not similar to
   - != Not the same as/equal to
   - \ Ignore escape characters
   *Note* The ! and = symbols cannot be used in the Statement field.
3. Click Apply.
   The list is filtered to display only those entries that match the filter criteria.
   *Note* To deselect all filter selections, click Clear.

Save a filter
You can create and save multiple filters and easily alternate between the saved filters as the need arises. This eliminates the need to redefine the filter criteria each time you view a page.

Task
1. Expand the Edit Filters area at the top of the page and define the filter criteria, then click Save.
2. Enter the name and a brief description of the filter.
3. Click Save again.
   The filter name is added to the Filters list.

Apply a filter
You can apply a saved filter the next time you view the page.

Task
1. Select the filter from the Filters drop-down list.
   The filter criteria in the Set Filter values area are refreshed to reflect the values of the customized view.
2. Click Apply.
   *Note* By default, the most recently applied filter is applied each time you access a page.
View the filter properties
You can view the criteria that define a saved filter.

Task
1. Select the filter from the Filters drop-down list, then click Edit.
   The filter details are displayed for the selected filter.
2. Change the filter criteria, then click Save.

Delete a filter
You can delete a saved filter.

Task
1. Select the filter from the Filters drop-down list, then click Delete Filter.
2. When prompted for confirmation, click OK.

The filter is deleted and is no longer available from the Filters drop-down list.

Change your password
For security purposes, it is recommended that you change your password from time to time or according to your corporate policy.

Task
1. Click Change Password at the top of any page.
2. In the Old Password field, enter your current password.
3. In the New Password and Confirm Password fields, enter your new password.
   Note: The password must comprise at least four characters. (It is highly recommended to use longer passwords and refrain from setting passwords that can be easily guessed by others.)
4. Click OK.
   Note: McAfee Database Activity Monitoring and Vulnerability Manager versions enable you to use an external LDAP server (such as Active Directory) to manage the system users. If you are using an external LDAP server, you do not have to manage your passwords in McAfee Database Security. For details, see Configure LDAP.

View license information
You can view the status of your license, as well as third-party license details and the End User License Agreement (EULA).

Task
1. Click License at the top of any page.
2. To view third-party license information, click View third-party licenses.
3. To view the EULA, click EULA (end-user license agreement).
Upgrade license information
You can import a license data file to upgrade your license.

Task
4  Click License at the top of any page, then click Upgrade License From a File.
5  Click Choose File, then select the license file.
6  Click Upload.

Log out
When you are not actively using the McAfee Database Security Web Console, it is recommended that you log out of the system. In addition, for security purposes, the system automatically logs you out if it does not detect activity for several minutes.

Task
- Click Logout at the top of any page.
Alerts can be handled in various ways in keeping with company policy and constraints. You can resolve an alert or you can immediately close a potentially dangerous DBMS session in response to an alert. In addition, you can create a rule based on the scenario that triggered the alert (particularly useful in preventing future false positives) or establish trust for a specific current session.

## Contents
- Alerts list
- Filter the Alerts list
- View alert details
- Handling alerts
- Managing resolve types

### Alerts list

The Alerts page lists the generated alerts, including these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Level  | The level of the alert, as indicated by these icons:  
  - A blue icon indicates a low-level alert.  
  - An orange icon indicates a medium level alert.  
  - A red icon indicates a high-level alert.  
  - A brown icon with an "n" indicates a notice.  
  - A blue icon with an "i" indicates an information result. |
| DBMS   | The name of the DBMS for which the alert was generated. |
| Time   | The date and time when the alert was generated. |
| State  | The result state compares the result to the last scan. Result can be New, Old, or No Change. Test result types can be Yes/No or Result Set. Old means that there was no result in the scan (the issue was most probably resolved). |
| Resolution | The state of the alert (such as Unresolved, Resolved, False Alarm, Session Terminated). |
| Statement | The requested operation (original SQL statement) that triggered the alert. |
| Rules  | The names of the rules that generated the alert. |
Alerts
Filter the Alerts list

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>The actions that can be performed on this rule:</td>
</tr>
<tr>
<td></td>
<td>Create a rule</td>
</tr>
<tr>
<td></td>
<td>Resolve alert</td>
</tr>
<tr>
<td></td>
<td>Trust Session</td>
</tr>
<tr>
<td></td>
<td>Terminate Session</td>
</tr>
<tr>
<td></td>
<td>Excessive Behavior</td>
</tr>
<tr>
<td>Excessive</td>
<td>If a single alert is generated for multiple instances of the same rule</td>
</tr>
<tr>
<td>behavior</td>
<td>violation, the icon is displayed. The alert details displayed are for the</td>
</tr>
<tr>
<td></td>
<td>last transaction to violate the rule.</td>
</tr>
</tbody>
</table>

Filter the Alerts list

You can filter the Alerts list according to various alert properties.

In addition, you can save filter criteria as customized filters, eliminating the need to redefine the filter criteria each time you view the Alerts list.

By default, the most recently applied filter is applied to the Alerts list each time you access the Alerts page.

**Note**

For details about saving, applying, and deleting saved filters, see Filtering data.

**Task**

1. On the Alerts page, expand the Edit Filters area above the Alerts list.
2. Set one or more filter criteria by entering/selecting the relevant values (for example, DBMS, Resolution, or Level).

**Note**

Any free text field filters also seek a match for the String entered as a substring of the field’s value. For example, if you enter “General SQL” in the Rule Name field, all alerts triggered by all the General SQL Injection rules are shown.

3. In the Statement, Client ID, OS User, Module, User, Host Name, and Application fields, enter one or more of these symbols to define the matching criteria:

   = Match
   ! Not similar to
   != Not the same as/equal to
   \ Ignore escape characters

   For example, if you enter =scott in the User field only those alerts for the user "scott" are displayed (and not scott1 or jscott). If you enter \=scott, all alerts containing the string “scott” are displayed (scott, scott1 and jscott).
Alerts

View alert details

Note

The ! and = symbols cannot be used in the Statement field.

4 From the Display alerts per page drop-down list, select the number of alerts to display on each page.

5 (Optional) To sort the results according to specific criteria, click Sort Options, then set the sort criteria.

6 Click Apply.

The list of alerts is filtered to display only those alerts that match the filter criteria.

Note

To deselect all filter selections, click Clear. Click Apply again to retrieve the unfiltered list.

View alert details

You can drill down into the details of a specific alert.

1 On the Alerts page, click the icon next to the alert.

The alert row expands to display more details. The specific details displayed vary according to the type of database that is monitored.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The DBMS user</td>
</tr>
<tr>
<td>OS User</td>
<td>The operating system user.</td>
</tr>
<tr>
<td>Rules</td>
<td>The rules that generated the alert. Clicking the rule name displays the Rule details page for the rule.</td>
</tr>
<tr>
<td>Duplicate alerts amount</td>
<td>An alert is counted as duplicate if it was submitted from the same session within 1.5 seconds of the previous one or if it is one of the last three alerts submitted. This field indicates the number of aggregated duplicate alerts.</td>
</tr>
<tr>
<td>Statement</td>
<td>The SQL statement that triggered the alert.</td>
</tr>
<tr>
<td>DBMS</td>
<td>The name of the DBMS for which the alert was generated.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that created the SQL statement that triggered the alert.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the user (if available).</td>
</tr>
<tr>
<td>Hostname</td>
<td>The user host name (if available).</td>
</tr>
<tr>
<td>ID</td>
<td>Alert ID (automatically generated by the system).</td>
</tr>
</tbody>
</table>
To view more advanced details for the selected alert, click **Detailed View**.

These alert details are displayed in the **Alert Details** page in read-only format.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor</td>
<td>The name of the sensor that generated the alert.</td>
</tr>
<tr>
<td>Session ID</td>
<td>The session ID provided by the DBMS.</td>
</tr>
<tr>
<td>Serial#</td>
<td>Relevant for Oracle only. The serial number generated by Oracle for this instance of the Session. This ID, when taken together with the Session ID, provides a unique session identifier.</td>
</tr>
<tr>
<td>User</td>
<td>The DBMS user.</td>
</tr>
<tr>
<td>OS User</td>
<td>The operating system user.</td>
</tr>
<tr>
<td>Action</td>
<td>The application action.</td>
</tr>
<tr>
<td>CMD Type</td>
<td>The SQL command type.</td>
</tr>
<tr>
<td>Log on time</td>
<td>Relevant for MSSQL only. The time when the user logged on to the application. This field, when taken together with the Session ID, provides a unique session identifier.</td>
</tr>
<tr>
<td>DBMS</td>
<td>The name of the DBMS for which the alert was generated.</td>
</tr>
<tr>
<td>DB Container</td>
<td>The database container (only for Oracle 12c Pluggable Databases).</td>
</tr>
<tr>
<td>Application</td>
<td>The application that created the SQL statement that triggered the alert.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the user (if available).</td>
</tr>
<tr>
<td>Hostname</td>
<td>The user host name (if available).</td>
</tr>
<tr>
<td>Terminal</td>
<td>The user terminal (if available).</td>
</tr>
<tr>
<td>Module</td>
<td>The module that generated the alert (if available).</td>
</tr>
<tr>
<td>Client ID</td>
<td>The Client ID of the application user that triggered the alert (if available).</td>
</tr>
<tr>
<td>Context Info</td>
<td>In MSSQL only. It usually contains the user information. (It is used instead of the Application, Module and Client ID fields that are used in Oracle.)</td>
</tr>
<tr>
<td>Statement</td>
<td>The SQL statement that triggered the alert.</td>
</tr>
<tr>
<td>Rules</td>
<td>The rules that generated the alert. Clicking the rule name displays the Rule details page for the rule.</td>
</tr>
<tr>
<td>Accessed Objects</td>
<td>The objects in the DBMS that were accessed as a result of the operation.</td>
</tr>
<tr>
<td>Inflow SQL</td>
<td>The SQL statement components that originated the action (for example, declare).</td>
</tr>
<tr>
<td>Inflow Objects</td>
<td>The original PL/SQL program units in the DBMS that originated the SQL command.</td>
</tr>
<tr>
<td>Resolution</td>
<td>The type of alert resolution.</td>
</tr>
<tr>
<td>Resolved by</td>
<td>The user that resolved the alert.</td>
</tr>
</tbody>
</table>
Alerts

Handling alerts

Alerts are triggered based on the rules defined and applied to SQL statements sent to the DBMS. As part of the monitoring process, you can view the alert information and take appropriate actions.

**Tasks**
- **Resolve an alert**
- **Resolve multiple alerts**
- **Create a rule based on an alert**
- **Create trust for a session**
- **Create a rule exception based on an alert**
- **Terminate a session**
- **Generate alert reports**
- **Archive alerts**

**Resolve an alert**

When an alert is first triggered, the alert is displayed in the Alerts list with a default status of Unresolved. You can review the details of the alert and, depending on its specific properties, change its resolution state to either **Resolved** or **False Alarm**.

You can also change the state of a resolved alert back to unresolved.

**Note**

For easier monitoring, you can filter the Alerts list to show only Unresolved alerts. For details, see *Filter the Alerts list*.

**Task**

1. On the **Alerts** page, click the icon next to the alert to be resolved.
   
The alert expands to show more details.

2. Review the alert details, then click **Resolve**.

3. On the **Resolve Alert** page, select the applicable resolution option.

   **Note**

   McAfee Database Security is provided with preconfigured resolve types. McAfee Database Activity Monitoring users can define more resolve types to meet their specific needs. For details, see *Managing resolve types*.

4. Enter a brief summary of the reason for resolving the alert.

5. Click **Resolve**.

The alert details are updated to reflect the new resolution status.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve date</td>
<td>The date and time when the alert was resolved.</td>
</tr>
<tr>
<td>Reason</td>
<td>The reason for the alert’s resolution (if available).</td>
</tr>
</tbody>
</table>
Resolve multiple alerts
You can change the resolution state of multiple alerts in one operation.

Note
For easier monitoring, you can filter the Alerts list to show only Unresolved alerts. For details, see Filter the Alerts list.

Task
1 On the Alerts page, select the alerts to be resolved in one of these ways:
   - Select the checkboxes for the specific alerts in the Alerts list.
   - Filter the alerts, then click the All link above the table header to select all alerts in the Alerts list.
   - Click the Page link above the table header to select all alerts in the page of the Alerts list that is currently displayed.

2 Click Resolve.

3 On the Resolve Multiple Alerts page, select the applicable resolve option from the drop-down list, then enter a brief summary of the reason for resolving the alerts.

4 Click Resolve.

The selected alerts are updated to reflect the new resolution status.

Create a rule based on an alert
You can create a rule based on an alert in the Alerts list. This is particularly helpful when you need to create an exception, for example, to prevent the repeated occurrence of false positives. The resulting rule is based on the criteria that triggered the alert, eliminating the need to define a custom rule from scratch. The rule can then be edited and positioned in the Custom Rules list as required.

Task
1 On the Alerts page, click the icon next to the alert that is to serve as the basis of a rule.

2 Review the alert details, then click Create Rule.

   The Custom Rules | Create Rule page is displayed, with an automatically generated condition based on the details of the originating alert. By default, this is an Allow rule.

3 Edit the rule details to refine its properties, then select the DBMSs where the rule should be installed. (For a detailed description of the rule components and how they are defined, see Create a custom rule.)

4 Click Save.

   The rule is created and added at the top of the Custom Rules list.

5 Move the rule to the appropriate location in the Custom Rules list by clicking the directional arrows. (For details, see Change the order of custom rules.)

   Note
   Exceptions are typically placed immediately above the rule that triggered the alert.
6 Click Save.

Rule Created appears as the resolution status of the alert in the Alerts list.

Create trust for a session

If you want to ignore the alerts for a specific session, you can create trust based on an alert for that session, for example, if you detect a long session that is repeatedly generating false alarms. The trust is created for the current session only.

As previously mentioned, a session is identified by the system according to the DBMS session ID and an internal ID. This prevents wrongly identifying more than one session as a single session (because DBMSs sometimes reuse session IDs). If the behavior that triggered the alerts is repeated in a new session, alerts are triggered and displayed accordingly.

**Note**

Trust should only be created after you have examined the alert details and determined that the session does not pose a security threat.

**Task**

1 On the Alerts page, click the icon next to the alert that is to serve as the basis for creating trust.

2 Review the alert details, then click the Trust Session icon 🎉.

3 On the Trust Session for Alert page, enter a brief summary of the reason for trusting the session.

4 Click Trust.

The behavior that triggered the alert is ignored during the current session. Trusted appears as the resolution status of the alert in the Alerts list.

Create a rule exception based on an alert

You can create an exception to a vPatch or custom rule based on an alert, for example, to prevent the repeated occurrence of false positives.

**Task**

1 On the Alerts page, click the sign next to the alert that is to serve as the basis of the exception.

2 Review the alert details, then click the Add Exception icon 🎉.

   A condition is automatically generated condition based on the details of the originating alert in the Exception field.

3 Edit the rule details to refine its properties (for example, to allow a specific IP address). (For a detailed description of the rule components, see Viewing rules.)

4 Click Save.

**Note**

If the alert was triggered by several rules, you are prompted to select the rule for which you want to create an exception.
Alerts
Handling alerts

**Terminate a session**

You can terminate a session for a user on the DBMS based on an alert in the Alerts list.

**Task**

1. On the Alerts page, click the ![ icon next to the alert.

2. Review the alert details, then click **Terminate Session** icon 🗓.

3. On the Terminate Session for Alert page, enter a brief summary of the reason for terminating the session.

4. Click **Terminate Session**.

The session that triggered the alert is terminated immediately. **Session Terminated** appears as the resolution status of the alert in the Alerts list.

**Generate alert reports**

McAfee Integrity Monitor and McAfee Database Activity Monitoring are provided with a simple mechanism for creating reports from alerts in PDF format. For more advanced alert reports available in the McAfee Database Activity Monitoring version only, see **Reports**.

You can generate a report that contains detailed information about each of the alerts currently displayed in the Alerts list.

The alerts contained in the report are subject to the filter that is applied to the Alerts list. For example, to generate a report that contains only those alerts that have resolution state of **False Alarm**, filter the list accordingly before trying to print the report.

### Before you begin

A PDF reader must be installed on the host computer to generate and view the PDF document.

**Task**

- On the Alerts page, after applying the appropriate filter criteria, click **Generate Report**. The report is displayed as a PDF file, which contains separate detailed entries for each of the alerts displayed in the Alerts list.

**Archive alerts**

McAfee Integrity Monitor and McAfee Database Activity Monitoring are provided with a mechanism for archiving alerts. Archived alerts are compressed and then stored in an archive file. Archived alerts do not appear in the Alerts list unless the archive file is reloaded.

**Task**

- On the Alerts page, after applying the appropriate filter criteria, click **Archive Alerts**.

The alerts are sent to the archive configured in the system/archive section.
Managing resolve types

Assigning a meaningful resolve type when you resolve an alert makes it easier to monitor the system for recurring problems.

McAfee Database Security has six preconfigured, system resolve types – Unresolved, Resolved, False Alarm, Sensor Deleted, Session Terminated and Created rule. System resolve types can’t be edited or deleted.

You can create more resolve types and assign them when you resolve alerts in the Alerts page.

Tasks

- Create a resolve type
- Edit a resolve type name
- Delete a resolve type

Create a resolve type

Based on your own experience, you can create custom resolve types to facilitate the monitoring of alerts generated in response to specific conditions or events.

Task

1. On the Rules page, select the Resolve Types tab, then click New Type.
2. In the Name field, enter a name for the resolve type.
3. Click Save.

The resolve type is added to the Resolve Types list.

Edit a resolve type name

You can edit the name of a custom resolve type at any time.

Task

1. On the Rules page, select the Resolve Types tab, then click the Properties icon in the row for the resolve type. The Resolve Type Properties page is displayed.
2. Edit the resolve type name, then click Save.

Delete a resolve type

You can delete a user-defined resolve type that is no longer needed.

Note

You cannot delete a system resolve type.

Task

- On the Rules page, select the Resolve Types tab, then click in the row for the resolve type to be deleted.

The resolve type is removed from the Resolve Types list. Alerts previously resolved using this resolve type are not affected, but the deleted resolve type is no longer available for selection.
After running a VA scan, McAfee Database Security Vulnerability Manager provides detailed information about the scan findings.

Contents

- VA results list
- Filter the VA results list
- Handling VA results

## VA results list

The **VA Results** page lists the vulnerability scan results, including these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
<td>The level of the scan result, as indicated by these icons:</td>
</tr>
<tr>
<td></td>
<td>- A blue icon indicates a low-level result.</td>
</tr>
<tr>
<td></td>
<td>- An orange icon indicates a medium level result.</td>
</tr>
<tr>
<td></td>
<td>- A red icon indicates a high-level result.</td>
</tr>
<tr>
<td></td>
<td>- A brown icon with an &quot;n&quot; indicates a notice.</td>
</tr>
<tr>
<td></td>
<td>- A blue icon with an &quot;i&quot; indicates an information result.</td>
</tr>
<tr>
<td><strong>DBMS</strong></td>
<td>The name of the DBMS for which the result was returned.</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>The date and time of the scan result.</td>
</tr>
<tr>
<td><strong>Resolution</strong></td>
<td>The state of the scan result (such as Unresolved, Resolved, False positive).</td>
</tr>
<tr>
<td><strong>Test</strong></td>
<td>The names of the tests that returned the results.</td>
</tr>
<tr>
<td><strong>Actions</strong></td>
<td>The actions that can be performed on this rule (for example, Resolve result).</td>
</tr>
</tbody>
</table>

From the **VA Results** page, you can:

- Filter the **Results** list according to various result properties, as described in *Filter the VA results list*.
- Set the criteria by which the list is sorted, as described in *Sort data*. 

---

McAfee Database Security 4.6.x

Product Guide

33
Filter the VA results list

To facilitate the viewing of VA results, you can filter the VA Results list according to various result properties.

In addition, you can save filter criteria as customized filters, eliminating the need to redefine the filter criteria each time you view the VA Results list.

By default, the most recently applied filter is applied each time you access the VA Results page.

**Task**

1. Expand the Edit Filters area above the VA Results list.

2. Set one or more filter criteria by entering/selecting the relevant values (for example, **DBMS**, **Resolution**, or **Level**). Any free text field filters also look for a match for the string entered as a substring of the field's value.

3. In the Statement, **Client ID**, **OS User**, **Module**, **User**, **Host Name**, and **Application** fields, you can use one or more of these symbols to define the matching criteria:
   - **=** Match
   - **!** Not similar to
   - **!=** Not the same as/equal to
   - \\
     Ignore escape characters

   For example, if you enter `=scott` in the User field, only results for the user "scott" are displayed (and not scott1 or jscott). If you enter `\=scott`, all results with the string "scott" are displayed (scott, scott1 and jscott).

   **Note** The ! and = symbols cannot be used in the Statement field.

4. From the **Display results per page** drop-down list, select the number of results to display on each page.

5. (Optional) To sort the results according to specific criteria, click **Sort Options**, then set the sort criteria.

6. Click **Apply**.

The list of VA results is filtered to display only those results that match the filter criteria.

**Note** To clear all filter selections, click **Clear**. Click **Apply** again to retrieve the unfiltered list.
Handling VA results

VA Results are triggered based on tests defined as part in the VA scans. You can resolve and archive the VA results.

Tasks
- Resolve a VA result
- Resolve multiple VA results
- Archive VA results

Resolve a VA result

When a VA result is first returned, it is displayed in the VA Results list with a default status of Unresolved. You can later change its resolution state to either Resolved or False Positive.

You can also change the state of a resolved result back to unresolved.

Note
For easier monitoring, you can filter the list to show only unresolved results. For details, see Filter the VA results list.

Task
1. On the VA Results page, click the sign next to the result to display more result details.
2. Review the result details, then click Resolve.
3. On the Resolve VA Result page, select the applicable resolution option from the drop-down list.

Note
McAfee Database Security is provided with preconfigured resolve types. Vulnerability Manager users can define more resolve types to meet their specific needs. For details, see Create a resolve type.

4. Enter a brief summary of the reason for resolving the VA result.
5. Click Resolve.

The result details are updated to reflect the new resolution status.

Resolve multiple VA results

You change the resolution state of multiple results.

Note
For easier monitoring, you can filter the VA Results list to show only unresolved results. For details, see Filter the VA results list.

Task
1. On the VA Results page, select the alerts to be resolved in one of these ways:
   - Select the checkboxes for the specific alerts in the VA Results list.
   - Filter the alerts, then click the All link above the table header to select all alerts in the VA Results list.
VA results
Handling VA results

- Click the Page link above the table header to select all results in the currently displayed page of the VA Results list.

2 Click Resolve to display the Resolve Multiple Results page.

3 Select the applicable resolution option from the drop-down list.

   **Note**

   McAfee Database Security is provided with preconfigured resolve types. Vulnerability Manager users can define more resolve types to meet their specific needs. For details, see *Create a resolve type*.

4 Enter a brief summary of the reason for resolving the results, then click Resolve.

   The selected results are updated to reflect the new resolution status.

## Archive VA results

McAfee Database Security Vulnerability Manager is provided with a mechanism for archiving VA results. Archived results are compressed and stored in archive file. Archived results do not appear in the VA Results list unless the archive file is reloaded.

**Task**

1 On the VA Results page, after applying the appropriate filter criteria, select the checkboxes for the results you want to archive.

2 Click Archive.

   The selected results are sent to the Database Security archive.
The McAfee Database Security Dashboard displays a wide range of statistical data regarding the status of alerts, DBMS monitoring, security updates, and rules.

### Contents
- Dashboard components
- Viewing dashboard data

## Dashboard components

The Dashboard displays these types of statistical data for the selected time frame.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unresolved Alerts</td>
<td>The distribution of unresolved alerts in all monitored DBMSs according to severity (High, Medium, Low).</td>
</tr>
<tr>
<td>Alerts per DBMSs</td>
<td>The distribution of alerts per DBMS according to severity (High, Medium, Low) in the selected system or the five user-selected DBMSs. You can change the displayed DBMSs, but the dashboard limits the display to five databases.</td>
</tr>
<tr>
<td>Sensors Status</td>
<td>The distribution of sensors according to status – Down, Pending, or Up. (Pending sensors are sensors that have not been approved by the administrator.)</td>
</tr>
<tr>
<td>DBMS Status</td>
<td>The distribution of DBMSs according to their monitoring status – Monitored, Partly Monitored, or Unmonitored. (Partly monitored DBMSs are clustered DBMSs where only some members are currently monitored.) The display is accurate in database clusters unless sensors are installed on all cluster members.</td>
</tr>
<tr>
<td>Alerts Summary</td>
<td>The distribution of alerts (all types) according to severity (High, Medium, Low) across the selected time period.</td>
</tr>
<tr>
<td>Quarantine List</td>
<td>The elements currently in quarantine, including the start time, the DBMS, and the rule that triggered the quarantine.</td>
</tr>
<tr>
<td>Installed Security Updates</td>
<td>The installed security updates, including version number, date installed, and the person responsible for their installation.</td>
</tr>
<tr>
<td>Available Security Updates</td>
<td>The available security updates, including version number, when published, and a brief description (if available).</td>
</tr>
<tr>
<td>Most Active vPatch</td>
<td>The most active vPatch rules in the system, including the rule name, the DBMS where the rule is installed, and the number of alerts (based on the time selected at the top of the screen).</td>
</tr>
</tbody>
</table>
### McAfee Database Security Dashboard

#### Viewing dashboard data

You can set the interval of the data to be displayed in the **Dashboard** by selecting the relevant time period at the top of the page. You can also filter and recalculate chart data.

**Tasks**

- **Recalculate chart data**
- **Filter the dashboard alerts**
- **Set the number of most active rules**

#### Recalculate chart data

You can refresh the chart data to reflect the most recently available statistics at any time by clicking **Recalculate chart data** at the top of the **Dashboard** page.

#### Filter the dashboard alerts

To facilitate the analysis of alerts data, you can filter the **Dashboard** to display data for up to five specific DBMSs.

**Task**

1. On the **Alerts per DBMSs** header, click **Choose DBMSs**.
2. Select the DBMSs for which you want to view alert statistics. You can select up to five DBMSs.

**Note**

To revert to the default settings, click **Use Default**.

3. Click **Select** to apply your selection and return to the **Dashboard**.

#### Set the number of most active rules

You can set the number of rules included in the Most Active vPatch Rules and Most Active Custom Rules lists.

**Task**

1. On the **Most Active vPatch Rules** header or **Most Active Custom Rules** header, click **Edit**.

   The **Number of rules selection** dialog box is displayed for the selected type of rule.

2. From the **Number of vPatch/custom rules** drop-down list, select the number of rules to include in the respective most active rules list.

3. Click **Save**.
Rules

McAfee Database Security provides enhanced DBMS security based on both predefined vPatch rules and custom rules.

Contents
- Rules and monitoring policy
- Viewing rules
- Enabling and disabling rules
- Managing vPatch rules
- Managing custom rules
- Importing and exporting rule settings
- Rule syntax
- Managing rule objects
- Script configuration
- Application mapping
- Working with tags
- Importing and exporting rules
- Rule revisions

McAfee Database Security also enables McAfee Database Activity Monitoring users to apply compliance rules. For details about managing compliance rules, see Compliance.

Rules and monitoring policy

DBMSs are manipulated by SQL statements and queries on an ongoing basis. The monitoring policy for a DBMS comprises the various rules enabled and applied on that DBMS. Rules define what types of statements are allowed to run on the DBMS, which types are forbidden, and which types should be monitored. Incoming statements are compared to the rules enabled for the DBMS and action is taken based on the first rule that is matched. If a statement does not match any of the existing rules, the statement is allowed.

McAfee Database Security provides enhanced DBMS security based on vPatch rules and custom rules. vPatch rules are included in the installation of the McAfee Database Activity Monitoring version and help prevent attacks against known vulnerabilities. In addition, you can define custom rules to define the level of monitoring and alerts, and further protect your DBMSs against potential threats. For example, custom rules can be used to limit access to specific tables in the DBMS, or to limit access to the DBMS by specific users or at specific times of day.

Rules are defined and/or enabled per one or more DBMSs. Rules for each DBMS are managed in the various tabs of the DBMS Properties page. vPatch rules are listed on the vPatch Rules tab of the DBMS properties page. Custom rules are listed on the Custom Rules tab of the DBMS properties page. Incoming statements are checked against the vPatch Rules list before they are checked against the Custom Rules list.
vPatch rules address known attacks and therefore should not be overruled by custom rules. Nonetheless, you can disable all vPatch rules or specific rules if the need arises, for example, for false positives where exceptions are unable to resolve the issue.

Viewing rules

Rules – both custom and vPatch – are viewed and managed on the Rules page.

The Rules page comprises these tabs:

- **vPatch Rules** — Lists the predefined vPatch rules and indicates whether they are enabled for the DBMSs. For details, see Managing vPatch rules.

- **Custom Rules** — Lists the custom rules defined for the DBMSs. For details, see Managing custom rules.

- **Application Mapping** — Lists data collected on the applications that access each monitored DBMS. Application mapping can significantly reduce the time required to create custom rules. For details, see Application mapping.

- **Tags-DBMSs** — Lists the existing tags, and shows the extent to which the rules that include each specific tag are applied to the DBMSs. For details, see Working with tags.

- **Rule Revisions** — Enables you to view the state of rules at any specific point in time and the revisions made to rules over time. For details, see Rule revisions.

- **Rule Objects** — Enables you to define rule objects, which can then be used as components in other rules. For details, see Managing rule objects.

- **Settings** — Enables you to configure notifications regarding rule changes and application mapping. For details, see Configure rule modification and application mapping notifications.

**Note**

Compliance rules are managed on the Compliance page. For details, see Compliance.

Rules list

vPatch and custom rules appear on separate tabs on the Rules page.

**Task**

On the Rules page, select the Custom Rules tab to view the rules for all DBMSs or select the vPatch Rules tab to view the vPatch rules.

The Rules list includes these parameters for each rule on the selected tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled/Disabled</td>
<td>An icon indicating the status of the rule, enabled ✅ or disabled 🚫.</td>
</tr>
<tr>
<td>No.</td>
<td>The ID number of the rule.</td>
</tr>
</tbody>
</table>
### Rules

Enabling and disabling rules

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>Rule</td>
<td>The comparator statements that serve as the criteria for matching the rule. For details, see Rule syntax.</td>
</tr>
<tr>
<td>Installed on</td>
<td>The DBMSs where the rule is currently installed.</td>
</tr>
<tr>
<td>Rule Actions</td>
<td>The actions to take when the rule criteria are met.</td>
</tr>
<tr>
<td>Actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>🏷 Properties — Displays the rule details.</td>
</tr>
<tr>
<td></td>
<td>☑️ Clone — Duplicates a rule.</td>
</tr>
<tr>
<td></td>
<td>✗ Remove — Deletes the rule.</td>
</tr>
<tr>
<td>Level</td>
<td>The level of the rule:</td>
</tr>
<tr>
<td></td>
<td>• A red icon indicates a forbidden violation.</td>
</tr>
<tr>
<td></td>
<td>• An orange icon indicates a medium level violation.</td>
</tr>
<tr>
<td></td>
<td>• A blue icon indicates a low-level violation.</td>
</tr>
<tr>
<td></td>
<td>• A brown icon with an &quot;n&quot; indicates a notice level rule.</td>
</tr>
<tr>
<td></td>
<td>• A blue icon with an &quot;i&quot; indicates an information level rule.</td>
</tr>
</tbody>
</table>

Note

You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see Filtering data.

---

### Enabling and disabling rules

You can enable/disable vPatch rules and Custom rules at any time.

The 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.

#### Tasks

- Enable a rule
- Disable a rule

#### Enable a rule

A rule must be enabled before it can be processed by the sensor.

**Task**

- In the Rules list, click ✅ in the row for the rule you want to enable.

The rule is enabled and the ✅ icon is displayed.
Managing vPatch rules

vPatch rules are listed on the vPatch tab of the page. vPatch rules cannot be deleted, however they can be disabled, installed on or removed from DBMSs and DBMS groups.

Note

A red exclamation point is displayed in the left margin to indicate that a vPatch rule has not been installed on any DBMS or DBMS group.

Tasks

- View the properties of a vPatch rule
- Configure the action for a vPatch rule
- Configure the action for a DBMS
- Update the security level of the vPatch rules
- Installing or removing vPatch rules

View the properties of a vPatch rule

You can view the details of a vPatch rule, including the DBMSs and DBMS Groups where the rule is installed.

Task

- On the Rules page, select the vPatch Rules tab, then click the Properties icon in the row for the rule.
These properties of the vPatch rule are displayed on the **Rule Properties** page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ID</td>
<td>The ID number of the rule.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the rule.</td>
</tr>
<tr>
<td>Exception</td>
<td>Any exception added by the user (normally to prevent false positives).</td>
</tr>
<tr>
<td>Action</td>
<td>The specific action to be taken when the conditions of the vPatch rule are</td>
</tr>
<tr>
<td></td>
<td>met.</td>
</tr>
<tr>
<td>DBMSs</td>
<td>The DBMSs where the rule is installed.</td>
</tr>
<tr>
<td>Tags</td>
<td>The tags assigned to this rule.</td>
</tr>
<tr>
<td>Enable Rule</td>
<td>The specific action to be taken per DBMS when the conditions of a specific</td>
</tr>
<tr>
<td></td>
<td>vPatch rule are met.</td>
</tr>
</tbody>
</table>

**Configure the action for a vPatch rule**

In addition to enabling or disabling a vPatch rule, you can define the alert level and the action to be taken when the conditions of a specific vPatch rule are met.

**Note**

You cannot change additional properties of a vPatch rule.

**Task**

1. On the **Rules** page, select the **vPatch Rules** tab, then click the **Properties** icon in the row for the rule.

2. In the **Action** area of the **Rule Properties** page, set the action as follows:

   - To configure email notification in addition to the alert in the log, select **Email**, then select the priority to assign to the email message (Low, Medium, or High). You can also define the email addresses. By default, the administrator’s email address is selected. The email settings must be configured on the **System** page to route email alerts correctly.

   **Note**

   If SNMP is not enabled in the System SNMP properties, this option is disabled.

   - To send an alert as an SNMP trap if the rule is matched, select **SNMP Trap**.

   **Note**

   If SNMP is not enabled in the System properties, this option is disabled.

   - To send a message using Twitter if the rule is matched, select **Twitter**.

   **Note**

   If Twitter is not enabled in the System properties, this option is disabled.
Rules
Managing vPatch rules

- To terminate a session if the rule is matched, select **Terminate**.

  **Note**
  This option should be used sparingly because terminating sessions can disrupt legitimate business transactions. Depending on environmental variables (such as command type and table size), session termination might not stop the current SQL command. Stronger termination capability is provided for DCL and DDL commands that use a before trigger (see **DDL triggers**).

If you select **Terminate**, the **Quarantine** option is displayed. To quarantine a user, select **Quarantine**, then enter the number of minutes the user is prevented from reconnecting. For the purposes of quarantine, "user" can mean the database user, OSUser, host name, IP address and more, or a combination of these parameters. The user definition for quarantine purposes is defined in the **Security/Quarantine Settings** section.

- To run an action script if the rule is matched, select **Script**, then set the script to run on the host DBMS. You can use all parameters that McAfee Database Security monitors within the script, by using '$' as a prefix. For example, if you want to use the "user" parameter in a script, enter $user.
  
  For example:
  "revoke dba from $user" as part of a script revokes the DBA permissions of the database user who executed the SQL command.

  **Note**
  This option is intended for advanced users only.

3. To enable this rule, select **Enable Rule**.

4. Click **Save**.

**Configure the action for a DBMS**

You can set the specific action to be taken per DBMS when the conditions of a specific vPatch rule are met.

Alerts are enabled per rule; You can define only how the alert is handled for the selected DBMS.

  **Note**
  Actions that are not enabled in the system properties are not available for selection.

**Task**

1. On the **Rules** page, select the **vPatch Rules** tab, then click the **Properties** icon in the row for the rule.
   
   The **Rule Properties** page is displayed.

2. In the **DBMSs and Groups** area, click **Change Actions** in the row for the DBMS for which you want to define a specific action. The vPatch Rule Action Per DBMS page is displayed.

3. To send an alert, select **Send Alert**, then select the relevant actions:
   
   - **Send alert to Console** — Generates an alert on the alert screen, according to the selected alert priority (Low, Medium, or High).
   - **SNMP Trap** — Sends an alert as an SNMP trap when the rule is matched.
   - **Syslog** — Sends an alert to the Syslog when the rule is matched.
Rules
Managing vPatch rules

- **Windows event log** — Sends an alert to the Windows event log when the rule is matched.
- **Log to file** — Sends the alert to a log file.
- **Archive** — Sends the alert only to the archive (without displaying it in the console or any other location). This option is suitable for auditing information that does not require monitoring on a day-to-day basis.
- **Send alert to email** — Sends the alert to the specified email addresses.

4 To terminate a session if the rule is matched, select **Terminate**.

**Note**
This option should be used sparingly because terminating sessions can disrupt legitimate business transactions. Depending on environmental variables (such as command type and table size), session termination might not stop the current SQL command. Stronger termination capability is provided for DCL and DDL commands that use a before trigger (see **DDL triggers**).

If you select **Terminate**, the **Quarantine** option is displayed. To quarantine a user, select **Quarantine**, then enter the number of minutes the user is prevented from reconnecting. For the purposes of quarantine, “user” can mean the database user, OSuser, host name, IP address and more, or a combination of these parameters. The user definition for quarantine purposes is defined in the **Security/Quarantine Settings** section.

5 To run the defined action script if the rule is matched, click select **Script**. You can use all parameters that McAfee Database Security monitors in the script, by using ‘$’ as a prefix. For example, if you want to use the “user” parameter in a script, enter $user.

For example: “revoke dba from $user” as part of a script revokes the DBA permissions of the database user who executed the SQL command.

**Note**
This option is intended for advanced users only.

6 (Optional) Configure limitations on the frequency of alerts as follows:

- From the **Limit alerts per second** drop-down list, select the maximum number of alerts to generate per second.
- From the **Limit alerts per session** drop-down list, select the maximum number of alerts to generate per session or select **Unlimited**.

**Note**
The session is uniquely identified by the Session ID and the Serial fields in Oracle, and by the Serial ID and the Logon time in MSSQL.

7 (Optional) To prevent the display of sensitive data in alerts, select **Mask Sensitive Data** and enter a regular expression in the **Regular Expressions** text box using standard regular expression syntax. To check the validity of the regular expression, click **Test**. In the Test Regular Expression dialog box, enter a value to be masked, then click **Test**.

**Note**
For more information about standard regular syntax, see: [http://java.sun.com/javase/6/docs/api/java/util/regex/Pattern.html](http://java.sun.com/javase/6/docs/api/java/util/regex/Pattern.html).

8 Click **Save**.
Rules
Managing vPatch rules

Update the security level of the vPatch rules
You can select the security levels you want to apply to virtual patches. This determines which vPatch rules are in effect in your databases. For example, you can decide whether to receive alerts from low confidence rules or alerts about attacks relevant to Oracle 8i only, even when Oracle 10g is the target. This feature enables you to control the tradeoff between security level and performance. By default "High Security" is selected. High security was designed as the optimal high security/high performance combination.

You can view the current security level at the top of the vPatch Rules page.

Task
1 On the Rules page, select the vPatch Rules tab, then click the security level.
2 Select the security level you want to apply, then click Save.

Tip When you select a security level, its description is displayed.

Installing or removing vPatch rules
By default, vPatch rules are automatically installed on all DBMSs during the installation process. Nonetheless, you can manually remove vPatch rules from and install vPatch rules on some or all DBMSs.

Tasks
- Install all or multiple vPatch rules on DBMSs and DBMS groups
- Install a vPatch rule on DBMSs and DBMS groups
- Remove vPatch rules from DBMSs and DBMS groups

Install all or multiple vPatch rules on DBMSs and DBMS groups
You can install all or a filtered group of vPatch rules on specific DBMSs or DBMS groups.

Task
1 On the Rules page, select the vPatch Rules tab, then filter the vPatch Rules list to display all rules or only the rules that you want to install on the DBMSs.
2 Click Install Rules on DBMSs. The Install on DBMSs and DBMS Groups page is displayed.
3 Select the DBMSs or DBMS Groups where you want to attach the rules from the DBMSs and DBMS Groups list or select All DBMSs to install the vPatch rules on all DBMSs.

Note To remove a DBMS selection, deselect the corresponding checkbox.
4 Click Save.

All rules currently displayed in the vPatch Rules list are attached to the DBMSs. (Rules that are not displayed per filter criteria are not attached.)

Install a vPatch rule on DBMSs and DBMS groups
You can install a vPatch rule on specific DBMSs or DBMS groups.
**Task**

1. On the **Rules** page, select the **vPatch Rules** tab, then click the **Properties** icon in the row for the rule that you want to install.

2. On the **Rule Properties** page, click **Install On** next to **DBMSs and Groups**.

3. Select the DBMSs or DBMS Groups to which you want to attach the rule from the DBMSs and DBMS Groups list or select **All DBMSs** to install the vPatch rules on all DBMSs.

   **Note**

   To remove a DBMS selection, deselect the corresponding checkbox.

4. Click **Save**.

   The rule is attached to the DBMS.

---

### Remove vPatch rules from DBMSs and DBMS groups

You can remove all or a filtered group of vPatch rules from specific DBMSs or DBMS groups.

**Task**

1. On the **Rules** page, select the **vPatch Rules** tab, then filter the **vPatch Rules** list to display all rules or only the rules that you want to remove from the DBMSs.

2. Click **Remove Rules from DBMSs**.

3. Select the DBMSs or DBMS Groups from which you want to remove the rules or select **All DBMSs** to remove the vPatch rules from all DBMSs.

4. Click **Remove**.

   All rules currently displayed in the **vPatch Rules** list are removed from the DBMSs. (Rules that are not displayed per filter criteria are not attached.)

---

## Managing custom rules

Based on your organization's ongoing monitoring of potential risks, custom rules can be defined to provide protection against activity that is considered suspicious per your IT policy and to help you protect specific DBMSs according to their functionality. For example, you might want to monitor access to sensitive tables in an HR DBMS, such as tables with employee compensation information, or you might want to protect against the usage of specific SQL query tools on production databases. Before trying to create custom rules, it is recommended that you familiarize yourself with the Application Mapping functionality, which can save considerable time in creating custom rules.

**Contents**

- *Create a custom rule*
- *Clone a rule*
- *Change the order of custom rules*
- *Edit a custom rule*
- *Remove a custom rule*
Create a custom rule

You can create and enable custom rules that determine how statements received by the DBMS are handled. Rules can be used to allow statements that match ("whitelist"), or they can be used to generate alerts regarding statements that do not match the policy ("blacklist"). A rule can also be used to automatically terminate potentially dangerous sessions.

Each rule consists of one or more comparator statements. The relationship between multiple comparator statements is based on Boolean logic, using AND, OR, or NOT.

You can define exceptions to a rule by creating an Allow rule for the exception case and placing it before the rule in the Rules list. You can also create an exception in the rule itself.

New rules can be defined using the Rule Creation wizard or on the New Rule page.

Tasks
- Create a rule with the Rule Creation wizard
- Create a rule in the New Rule page

Create a rule with the Rule Creation wizard

The Rule Creation wizard breaks down the rule definition process into individual steps, making it easy to create custom rules to meet the specific needs of your enterprise. If you are new to the rule creation process, it is recommended that you take advantage of the wizard’s guided process when creating your first rules.

Task
1. On the Rules page, select the Custom Rules tab, then click Create New Rule with Wizard.
2. In the Name field, enter a name for the rule. It is recommended that the name selected clearly reflect the nature of the rule (for example, "Sensitive HR tables" or "PCI-DSS password protection"). Then click Next to display the Rule Trigger page.
3. In the If fields, define the first rule comparator statement as follows:
   - In the first field, type the first letter of the identifier name, then select the required identifier from the drop-down list.
   - In the second field, select the required operator from the drop-down list.
   - In the third field, enter the literal component to be matched. If the literal component is a string, the text must be enclosed in single quotation marks.

   Note
   1. For a detailed description of rule comparator statements and their syntax, see Rule syntax.
   2. Alternatively, you can enter the comparator statement directly into the text box below the If fields, entering a space to access the respective drop-down lists.
   3. To turn off the auto-completion feature, select Disable auto completer.

4. Click Add.

   The comparator statement appears in the textbox. If the rule includes more than one comparator statement, enter the relevant Boolean operator (AND, OR, or NOT) in the fourth field, then define the next comparator statement. Repeat for additional comparator statements as required.
5 Click Next to display the Rule Action page.

6 To send an alert if the rule is matched, select Send Alert to, then select the relevant actions:
   - **Send alert to Console** — Generates an alert on the alert screen, according to the selected alert priority (Low, Medium or High).
   - **SNMP Trap** — Sends an alert as an SNMP trap when the rule is matched.
   - **Twitter** — Sends a Twitter message (tweet) when the rule is matched.
   - **Syslog** — Sends an alert to the Syslog when the rule is matched.
   - **Windows event log** — Sends an alert to the Windows event log when the rule is matched.
   - **Log to file** — Sends the alert to a log file.
   - **Archive** — Sends the alert only to the archive (without displaying it in the console or any other location). This option is suitable for auditing information that does not require monitoring on a day-to-day basis.
   - **Send alert to email** — Sends the alert to the specified email addresses.

7 To terminate a session if the rule is matched, select Terminate.

   - **Note**
     This option should be used sparingly because terminating sessions can disrupt legitimate business transactions. We recommend using the terminate option only if these conditions are met:
     - You are certain that the rule will not create false positives (it is recommended to use the rule first in alert only mode to make sure that legitimate traffic is not affected).
     - The risk involved with the rule condition is very high.
     - Terminating a session causes only minimal disruption to other transactions.

If you select Terminate, the Quarantine option is displayed. To quarantine a user, select Quarantine, then enter the number of minutes during which the user is prevented from reconnecting.

   - **Note**
     Quarantine is done based on the quarantine settings in the System tab. Make sure that you edit the quarantine settings before you enable quarantine on any of your rules. (The quarantine settings are configurable on the System page under Quarantine | Settings).

8 To enable the VPN-1/FireWall-1 to block the connection, select Create VPN-1 SAM rule, then configure these parameters:
Managing custom rules

- From the **Action** drop-down list, select the type of VPN blocking action to be taken.

- In the **Gateway** field, enter the name of the gateway, then set the number of minutes to block the connection.

9 To allow the statement to be processed if the rule is matched, select **Allow**. (This enables you to create an exception to a rule that appears later in the policy.)

10 To stop the matching process if a rule is matched, select **Stop Verifying Additional Rules**. This is the default setting when the **Rule Action** is set to **Allow**. If this option is not selected, the matching process continues.

11 (Optional) Expand the **Advanced** section to configure these parameters:

- **Script** — Specify the script to run when a statement matches the rule (SQL*Plus script in Oracle and T-SQL run by OSQL in Microsoft SQL Server).

- **Limit alerts per second** — Set the maximum number of alerts to generate per second or select **Unlimited** (the default value).

- **Limit alerts per session**: Set the maximum number of alerts to generate per session or select **Unlimited** (the default value).

- To trigger an alert only if a minimum number of rows are returned from the database, enter the number of rows in the **Set Minimum Rows** field. (This option is available only when network monitoring is enabled.)

**Note** If this parameter is set and the minimum number of rows is exceeded, the alert includes a “minimum rows exceeded” notification.

- To prevent the display of sensitive data in alerts, select **Mask Sensitive Data** and enter a regular expression in the text box using standard regular expression syntax.

**Note** For more information about standard regular syntax, see: [http://java.sun.com/javase/6/docs/api/java/util/regex/Pattern.html](http://java.sun.com/javase/6/docs/api/java/util/regex/Pattern.html).

- To check the validity of the regular expression, click **Test**. In the Test Regular Expression dialog box, enter a value to be masked, then click **Test**.

- To apply an action only in response to repetitive or excessive behavior, select **Apply action when rule triggers**. Then, in the adjacent fields, specify the minimum number of alerts within the number of seconds, minutes or hours, required to trigger the actions. When this option is configured, one alert is generated for multiple instances of the same rule violation.

In the Alerts list, the 🟥 icon indicates those alerts triggered by excessive behavior. The alert details are displayed for the last transaction to violate the rule.

12 To select the DBMSs where the rule is applied:

- Click **Install On** to display the **Install on DBMSs and DBMS Groups** page.

- Select one or more relevant DBMSs and/or DBMS Groups, then click **Save** to return to the rule definition page.

The selected DBMSs and DBMS Groups are listed in the **DBMSs** and **DBMS Groups** fields respectively.

13 To assign a tag to the rule, enter the tag name in the **Tags** field or enter a space in the field to select the tag from the drop-down list.
14 (Optional) By default, all users can edit the properties of a custom rule. To limit the ability to edit the properties of this rule to specific users or users assigned a specific role, enter the user names or role names in the Role Restriction field.

15 Click Next.

16 In the Comments field, enter a free text description/comment, then click Next.

17 To enable the rule, select Enable Rule.

    Note
    You can enable/disable the rule at any time by selecting/clearing the Enable Rule checkbox.

18 Click Finish to validate and save the rule.

Create a rule in the New Rule page
You can create custom rules in the New Rule page, defining all rule properties in a single window.

    Note
    If you are new to the rule creation process, it is recommended that you take advantage of the wizard’s guided process when creating your first rules.

Task
1 On the Rules page, select the Custom Rules tab, then click Create New Rule.

2 In the Name field, enter a name for the rule. It is recommended that the name selected clearly reflect the nature of the rule (for example, "Sensitive HR tables" or "PCI-DSS password protection").

3 In the If area, define the first rule comparator statement, as described in step 3 of Create a rule with the Rule Creation wizard, then click Add.

    Note
    For a detailed description of rule comparator statements and their syntax, see Rule syntax.

    If the rule is to include more than one comparator statement, enter the relevant Boolean operator (AND, OR, or NOT), then define the next comparator statement. Repeat for additional comparator statements as required.

    Note
    • You can define rule objects, which can then be used as components in other rules. For example, a rule object might be used in the definition of a rule intended to allow a specific range of IP addresses. For details, see Managing rule objects.
    • If there is a problem with the rule syntax, validation fails and a message is displayed. For example, if you fail to enclose a text string in single quotation marks, a message is displayed regarding an unexpected token.

4 To create an exception to this rule, click Add Exception. Then, in the Exception text box, enter a comparator statement that defines the conditions which when matched are treated as an exception to this rule. Repeat to define additional exceptions as required.

    Note
    1 For a detailed description of rule comparator statements and their syntax, see Rule syntax.
5  In the **Then** area, select the actions to be taken when a statement matches the rule, as described in step 6 of *Create a rule with the Rule Creation wizard*.

6  To select the DBMSs where the rule is applied:
   - Click **Install On** to display the **Install on DBMSs and DBMS Groups** page.
   - Select one or more relevant DBMSs and/or DBMS Groups, then click **Save** to return to the rule definition page.

   The selected DBMSs and DBMS Groups are listed in the **DBMSs** and **DBMS Groups** fields respectively.

7  To assign a tag to the rule, enter the tag name in the **Tags** field or enter a space in the field to select the tag from the drop-down list.

8  In the **Comment** field, enter a free text description/comment. It is recommended that you indicate the reason for creating the rule.

9  To enable the rule, select **Enable Rule**.

   **Note**

   You can enable or disable the rule at any time by selecting/clearing the **Enable Rule** checkbox.

10  To prevent the triggering of alerts by signed scripts, select the **Ignore Signed Scripts** checkbox.

11  Click **Finish** to validate and save the rule.

### Clone a rule

You can create a rule by cloning an existing rule. This eliminates the need to define all rule properties from scratch when creating rules that share many common properties.

**Task**

1  In the **Custom Rules** list, click ![Clone](#) in the row for the rule you want to clone.

   The **New Rule** page is displayed, with the properties of the original rule configured by default.

2  Change the rule name and change specific rule properties as required. (For a detailed description of the rule parameters, see *Create a rule in the New Rule page*.)

### Change the order of custom rules

The order of the rules in the Custom Rules list is important. The first rule that is matched is the rule that is applied to the statement. If a statement does not match any of the existing rules, the statement is allowed.

The McAfee Database Security system enables you to create a policy according to your preferences and security requirements in various ways.

Fundamentally, there are two approaches to defining policy:

- **Whitelist approach** — Resembles the approach of firewalls, whereby you determine the allowed actions first and then alert on all other actions (assuming that all other actions are suspect).
- **Blacklist approach** — Resembles the approach of IDS/IPS systems, whereby everything is allowed except actions that are considered suspect.

McAfee Database Security users normally create a policy that integrates elements of both approaches, for example, using a Blacklist approach for all known attacks, while using a Whitelist approach for the use of development SQL tools.

**Note**

Incoming statements are checked against the vPatch Rules list before they are checked against the Custom Rules list.

**Task**

- Select the rule in the Rules list and then drag the position indicator on the slider to a new location. For example, to move the rule to the top of the list, drag the indicator to the top of the slider.

**Edit a custom rule**

You can edit the properties of a rule in the Custom Rules tab of the DBMS Properties window.

**Task**

1. In the Custom Rules list, click the name of the rule that you want to edit. The rule properties are expanded to display the options that comprise the rule definition.

2. Edit the rule comparator statements, actions, and other parameters, as required. For details, see Create a custom rule.

3. Click Save.

**Remove a custom rule**

You can remove a rule from the Custom Rules list.

**Note**

You cannot remove a rule from the vPatch Rules list.

**Tip**

Only remove a rule if you are sure that you will not need it in the future. If you might need it again, you can temporarily disable it.

**Task**

1. In the Custom Rules list, click in the row for the rule you want to remove.

2. When prompted for confirmation, click OK.

The rule is removed from the list.
Rules
Importing and exporting rule settings

Importing and exporting rule settings
You can import and export vPatch and custom rule settings, including exceptions.

Tasks
- Export rule settings
- Import rule settings

Export rule settings
When you export a custom rule, the entire rule is copied (not just the settings).

Task
1. In the vPatch or Custom Rules tab, click Export Rule.
2. In the File Download dialog box, click Save, then select the location where you want to save the file.
3. Click Save again.
   The file is saved in the specified location.

Import rule settings
When you import a custom rule, the entire rule is copied (not just the settings).

Task
1. On the vPatch or Custom Rules tab, click Import Rule.
2. Select the file you want to import, then click Import.
   The rules are imported.

   Note
   If identical rule objects exist in the system, the Duplicate Rule Object dialog box is displayed. Select the checkboxes for the rules that you want to overwrite, then click Continue. The selected rules are overwritten.

Rule syntax
Each rule consists of one or more comparator statements, which comprise Identifiers, Operators and Literals.

The relationship between multiple comparator statements is based on Boolean logic, using AND, OR, or NOT. Comparator statements can be grouped using parentheses.

If parentheses are not used, the order of precedence is:
- NOT
- AND
- OR

This section includes these topics:
• Identifiers
• Operators
• Rule examples

**Identifiers**
There are three basic types of identifiers.

<table>
<thead>
<tr>
<th>Identifier type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String-based</td>
<td>Types that are matched against strings.</td>
</tr>
<tr>
<td>Number-based</td>
<td>Types that can be translated into a number representation. Numbers can be in a specific range. Number-based types can be enforced to equal only a fixed set of constants.</td>
</tr>
<tr>
<td>Enumerated</td>
<td>Types that represent a fixed set of constants that cannot be translated into a number representation.</td>
</tr>
</tbody>
</table>

McAfee Database Security supports these identifiers.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>string</td>
<td>The application action.</td>
</tr>
<tr>
<td>application</td>
<td>string</td>
<td>The application used to connect to the DBMS.</td>
</tr>
<tr>
<td>client_appl_name</td>
<td>string</td>
<td>Sybase client application name. (Sybase only)</td>
</tr>
<tr>
<td>client_host_name</td>
<td>string</td>
<td>The Sybase client host name. (Sybase only)</td>
</tr>
<tr>
<td>client_name</td>
<td>string</td>
<td>The Sybase client name. (Sybase only)</td>
</tr>
<tr>
<td>clientid</td>
<td>string</td>
<td>The application set clientid accessing the DBMS. (Oracle only)</td>
</tr>
<tr>
<td>cmdtype</td>
<td>string</td>
<td>An action the statement is trying to perform.</td>
</tr>
<tr>
<td>context_info</td>
<td>string</td>
<td>Microsoft SQL context information. (Microsoft SQL only)</td>
</tr>
<tr>
<td>date</td>
<td>number</td>
<td>The date the statement is executed. The date must be in the form MM/DD/YY (US date format), for example 1/25/07.</td>
</tr>
<tr>
<td>day</td>
<td>number</td>
<td>The day of the month when the statement is executed. An integer in the range of 1–31.</td>
</tr>
<tr>
<td>db_container</td>
<td>string</td>
<td>The database container. This provides specific database context information when using the Pluggable Database functionality. (Oracle 12c only)</td>
</tr>
<tr>
<td>error code</td>
<td>number</td>
<td>The error code returned by the DBMS (for example, when the user tries to access a table that does not exist).</td>
</tr>
<tr>
<td>exec_user</td>
<td>string</td>
<td>If a user logs in to an application and then changes to another user, the exec_user is the new user.</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>The domain name of the connecting application.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hour</td>
<td>number</td>
<td>The hour in which the statement is executed. The hour must be in the form HH[ — MM] where HH is in the range of 0–23 and MM in the range of 0–59. The minutes setting is optional.</td>
</tr>
<tr>
<td>inflow</td>
<td>string</td>
<td>The inflow PL/SQL object that originated the current executing statement. Same format as object.</td>
</tr>
<tr>
<td>inflowsql</td>
<td>string</td>
<td>The SQL statement part that originated the current executing command.</td>
</tr>
<tr>
<td>instance</td>
<td>string</td>
<td>The instance where the execution takes place. In Oracle, this value is the SID of the database instance. In Sybase, this value is the instance name. In MS SQL, it is the full instance name including the host (for example — MYHOST\SQLSERVER).</td>
</tr>
<tr>
<td>ip</td>
<td>number</td>
<td>The IP address the statement is executed from. IP addresses must be in the form of — XXX.XXX.XXX.XXX (single IP address) or XXX.XXX.XXX.XXX/YYY.YYY.YYY (IP with subnet). Each IP address is validated by the McAfee Database Security system to prevent errors.</td>
</tr>
<tr>
<td>module</td>
<td>string</td>
<td>The application set module.</td>
</tr>
<tr>
<td>month</td>
<td>number</td>
<td>The month in which the statement is executed: JANUARY, FEBRUARY, MARCH, APRIL, MAY, JUNE, JULY, AUGUST, SEPTEMBER, OCTOBER, NOVEMBER, DECEMBER. Alternatively, the short form of month name is also supported for example: JAN.</td>
</tr>
<tr>
<td>nethost</td>
<td>string</td>
<td>The host name of the network (this might differ from the host name reported for an application). Applicable only when network monitoring is enabled.</td>
</tr>
<tr>
<td>netip</td>
<td>number</td>
<td>The IP address of the network (this might differ from the IP address reported for an application). Applicable only when network monitoring is enabled.</td>
</tr>
<tr>
<td>object</td>
<td>string</td>
<td>The DBMS object being accessed. Supports syntax of the form [owner.]objectname. DBMS objects can be tables, triggers, stored procedures, and so on. In Oracle, the format is owner.objectname; in MS SQL and Sybase it is database.owner.objectname.</td>
</tr>
<tr>
<td>osuser</td>
<td>string</td>
<td>The operating system user.</td>
</tr>
<tr>
<td>schema</td>
<td>string</td>
<td>The schema of the DBMS.</td>
</tr>
<tr>
<td>session_state</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• session_state=NEW_SESSION for monitoring session logins</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• session_state=END_SESSION for logouts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• session_state=NEW_LOGIN and session_state=END_LOGIN for monitoring change of user during transaction execution (Specifically for Microsoft SQL Server)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• session_state=CHANGE_SCHEMA for monitoring changes in schema during the session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• session_state=EXECUTE for all other statements</td>
</tr>
<tr>
<td>statement</td>
<td>string</td>
<td>The raw statement sent to the server.</td>
</tr>
<tr>
<td>terminal</td>
<td>string</td>
<td>The computer where the user is logged in.</td>
</tr>
<tr>
<td>user</td>
<td>string</td>
<td>The DBMS user that is accessing the DBMS. See also exec_user.</td>
</tr>
</tbody>
</table>
### Rules

#### Rule syntax

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version_mssql</td>
<td>number</td>
<td>The Microsoft SQL version. For example, version_mssql = 9.0.4053 for the relevant version of MS SQL 2005 (rarely used).</td>
</tr>
<tr>
<td>version_oracle</td>
<td>number</td>
<td>The full 5-digit oracle version. For example, 10.1.0.3.0 (rarely used).</td>
</tr>
<tr>
<td>version_sybase</td>
<td>number</td>
<td>The Sybase particular version. For example, version_sybase = 12.5 or later (rarely used).</td>
</tr>
<tr>
<td>weekday</td>
<td>value</td>
<td>The day of the week when the statement is executed: SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY. Alternatively, the short form is also supported for example: TUE.</td>
</tr>
</tbody>
</table>

**Note**

All rules are case insensitive. An identifier can be specified in lowercase letters, uppercase letters, or a combination of both. For example: user, User, USER, uSEr are all legal for the user identifier. In addition, constant values are case insensitive so SUNDAY and SunDAy are equivalent.

### Operators

McAfee Database Security supports these operators.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equals (all types)</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than (number types only)</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than (number types only)</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to (number types only)</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to (number types only)</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Not equal to (all types)</td>
</tr>
<tr>
<td>(not)? like</td>
<td>Compare to a string supporting the '%', character as symbol to any string (string types only)</td>
</tr>
<tr>
<td>(not)? between</td>
<td>Check if an identifier is between two values (number types only)</td>
</tr>
<tr>
<td>(not)? in</td>
<td>Check if an identifier is in a list of values (all types)</td>
</tr>
<tr>
<td>(not)? matches</td>
<td>Perform a regular expression match (string types only)</td>
</tr>
<tr>
<td>(not)? contains</td>
<td>Perform a simple and fast string match (string types only)</td>
</tr>
<tr>
<td>length</td>
<td>When inserted before an identifier, indicates a condition on the field's length. For example:</td>
</tr>
<tr>
<td></td>
<td>• &quot;length statement &gt; 1024&quot; catches statements longer than 1024 bytes.</td>
</tr>
<tr>
<td></td>
<td>• &quot;length user &lt; 10&quot; catches SQL statements where a DB user name length is shorter than 10 characters.</td>
</tr>
</tbody>
</table>
Rule examples

These examples illustrate the rule syntax.

Example 1

OSUSER = 'mycompany\john' AND APPLICATION CONTAINS 'sqlplus' AND HOST = 'johnlaptop.localdomain' AND IP = 192.168.1.7

Action: Allow

The above rule allows john to use SQL*Plus from his station (defined by host name and IP address), thereby bypassing many of the rules that come later (such as preventing SQL*Plus from being used).

Example 2

APPLICATION CONTAINS ‘sqlplus’ OR APPLICATION CONTAINS ‘toad’

Action: Log-high, e-mail-high, terminate

This rule terminates any access by the applications Toad or SQL*Plus. It also sends a high-severity alert and email message to the McAfee Database Security administrator.

Example 3

STATEMENT CONTAINS ‘emps’

Action: log-medium

This example assumes that the emps.* columns include sensitive data that require protection, and that emps.salary and emps.cc are particularly sensitive.

This rule provides an alert every time an SQL statement includes the string emps, alerting on any access attempt to columns containing the name emps (or any other SQL statement component that includes the string emps). Even when the user is not actually accessing the objects (for example, the DBMS prohibits access based on authorization rules), this rule generates alerts (in contrast to using object, see example 4 below).

Example 4

OBJECT = ‘emps.salary’ OR OBJECT = ‘emps.cc’

Action: log-high, email-high

This example assumes that the tables emps.salary and emps.cc are particularly sensitive.

This rule provides a high-level alert and an email each time the specified objects are accessed. An alert appears whether the object is accessed in a view, a stored procedure, a trigger, or another database. In this case, if the DBMS successfully restricts the user from accessing the objects, an alert is not generated because the object is not accessed.

Example 5

Statement contains ‘drop session’ Alert low
Statement contains ‘alter DBMS’ Alert low
Statement contains ‘drop table’ Alert Low
Statement contains ‘grant’ Alert low
Statement contains ‘grant dba’ Alert medium
Managing rule objects

You can define rule objects, which can then be used as components in other rules. This can be particularly helpful when working with Allow rules. For example, a rule object might be used in the definition of a rule intended to allow a specific range of IP addresses.

Rule objects are managed on the Rule Objects tab of the Rules page.

McAfee Database Security is provided with several predefined rule objects. These predefined objects are used in the predefined rules and are listed on the Rule Objects tab.

Tasks

- Create a static/active directory rule object
- View or edit rule object properties
- Delete a rule object
- DVM-based rule objects

Create a static/active directory rule object

You can define a rule object and then use that object in multiple rules.

Task

1. On the Rules page, select the Rule Objects tab, then click New Object.
2. From the Type list, select the type of identifier for the rule object.
3. In the Name field, enter a name for the rule object.
4. In the Value field, set the object value (according to the selected type).
5. In the Comment field, enter a brief comment or description.
6. If you want to define a dynamic object and enable the use of LDAP security groups for this rule object in creating rules, select Dynamic Object.

Note: The use of dynamic objects is possible only if LDAP is enabled.

7. If you want to upload a list of values from an existing file, enter the file location in the File upload field, or click browse and select the file. Then click Upload to upload the list.
8. Click Save.

The rule object is automatically added to the list of available values according to Identifier type and can be used in rule definitions.
**View or edit rule object properties**

You can view and edit the properties of an existing rule object.

**Task**

1. On the Rules page, select the Rule Objects tab, then click the Properties icon in the row for the rule object. The Rule Object Properties page is displayed.

2. Edit the rule object properties, then click Save.

**Delete a rule object**

You can delete a rule object, however it is recommended that you do so only if you are absolutely sure that it is not included in the definition of existing enabled rules.

**Note**

If you remove a rule object that is included in an existing rule definition, the rule is automatically disabled and is removed the Rule Errors list. Use caution when deleting rule objects.

**Task**

1. On the Rules page, select the Rule Objects tab, then click in the row for the rule object you want to delete.

2. When prompted for confirmation, click OK.

The rule object is removed from the Rule Objects list. Any existing rules that incorporate the rule object are automatically invalidated.

**DVM-based rule objects**

DVM rule objects are based on specific findings that include result sets. Once defined, the rule object is updated each time the test is executed. There are several types of DVM-based rule objects:

- **Specific DVM rule object** – where a rule object is distinct to a specific test on a specific database instance.

- **Global DVM rule object (distributed)** – where a rule object can be defined to contain values for all database instances where the test is executed. The rule object values for each database instance are populated by the result of the check on the instance. With this Rule Object, you can create a single rule object definition, with a single custom rule that refers to it. You can then apply the rule to multiple databases. The rule object values per instance is populated by the relevant values retrieved by the check from the instance, when last executed.

- **Global DVM rule object (Master Repository)** – where a rule object can be defined from a single result set, but contain values for different database instances. This rule object retrieves the values for each database instance from a Master Repository (table) and behaves similarly to the Global DVM Rule Objects (distributed) type. The rule object values for a specific instance are populated by values retrieved from the Master Repository query (DVM check) when last executed, based on the filtering criteria and values.
Add a specific DVM rule object

You can add a rule object to a specific test on a specific database instance.

**Task**
1. In the VA Results, locate the results you want to base the rule object on.
2. Click the Create Rule Object from Results icon, then select the object value field to include in the rule object.
3. (Optional) The Expression field can be used to augment the value format/structure when needed.
4. Click Create to display the rule object properties window.
5. Select the appropriate rule object type based on the values, then enter a name for the rule object.
6. Based on the empty list behavior, you can define whether to ignore rules that rely on the rule object when there are no values or set a static value.
7. Click Save.

Add a global DVM rule object (distributed)

You can add a rule object that contains values for all database instances where a test is run.

**Task**
1. In the VA Results, locate the results you want to base the rule object on.
2. Click the Create Rule Object from Results icon.
3. Select the object value field to include in the rule object.
4. (Optional) The Expression field can be used to augment the value format and structure when needed.
5. Select the Global DVM Rule Object (Advanced) checkbox.
6. Select the type of rule object, based on DVM results per instance, for distribution.
7. Click Create.
8. Select the appropriate rule object type based on the values and enter the rule object name.
9. (Optional) To view the values for a specific instance, enter the instance name in the Show values field (auto-complete is available for instance names), then click Show to view the list of values linked to that instance.
10. Based on the empty list behavior, you can define whether to ignore rules that rely on the rule object when there are no values or set a static value.
11. Click Save.

Add a global DVM rule object (Master Repository)

You can add a rule object from a single result set that contains values for different database instances.

**Task**
1. In the VA Results, locate the results you want to base the rule object on.
2. Click the Create Rule Object from Results icon.
3. Select the object value field to include in the rule object.

4. (Optional) The Expression field can be used to augment the value format/structure if needed.

5. Select the Global DVM Rule Object (Advanced) checkbox,

6. Select the type of rule object, based on DVM results per instance, for Master Repository.

7. Input the column name (wrapped in $ sign) you want to use as the filtering value (i.e., the value used to determine which values are sent to the different database instances.)

8. Input the criteria for evaluating the filtering expression.

9. Click Create to display the rule object properties window.

10. Select the appropriate rule object type based on the values and enter a name for the rule object.

11. (Optional) To view the values for a specific instance, enter the instance name in the Show values field (auto-complete is available for instance names), then click Show to view the list of values linked to that instance.

12. Based on the empty list behavior, you can define whether to ignore rules that rely on the Rule Object when there are no values or set a static value.

13. Click Save.

**Script configuration**

The use of a signed script enables you to run the script on one or more databases without it triggering alerts.

This functionality is intended for advanced users only.

**Note**

If the signed script does trigger an alert, the script appears in the Print view of the alert details.

**Tasks**

- Configure a signed script
- View or edit a signed script

**Configure a signed script**

You can create signed scripts for specific timeframes and/or specific databases.

**Task**

1. On the Rules page, select the Signed Scripts tab, then select Create New Script.

2. Enter the script name and a brief description in the designated fields.

3. From the Type drop-down list, select the type of script (MSSQL or Oracle).

4. Click DBMSs & Groups to select the DBMSs to run the script on.
5 Select one or more relevant DBMSs and/or DBMS Groups, then click Save to return to the Script Configuration page. The selected DBMSs and DBMS Groups are listed.

6 In the From Date and To Date fields, set the time period for the validity of the signed script.

7 To enable the script, select the Enabled checkbox.

8 Click Choose File to browse and upload the script file.

9 On the Script Configuration page, click Download. (The Download option is not available until the script is uploaded).

10 Click Save.

The signed script appears in the Signed Script list.

**View or edit a signed script**

Signed scripts are listed in the Signed Scripts tab of the Rules page. You can view the script details, enable/disable the script, and edit the date settings; however you cannot modify the script itself in anyway.

**Task**

1 On the Rules page, select the Signed Scripts tab, select the script, then click Edit.

   The Script Configuration page is displayed.

2 (Optional) In the From Date and To Date fields, set the time period for the validity of the signed script.

3 (Optional) To disable the script, deselect the Enabled checkbox.

4 Click Save.

The signed script appears in the Signed Script list.

---

**Application mapping**

Application mapping is performed per DBMS and provides information about activities taking place on the DBMS, including which applications are being run on the DBMS and by which users.

To minimize the impact on the DBMS, the system collects a sampling of information in the background. A message is sent to the user when sufficient data has been collected to be useful for analysis purposes.

**Tasks**

- Create an alert rule
- Create a mapping exception rule
Create an alert rule
When you identify an activity that should be monitored or audited, you can create a rule to monitor such actions in the future.

**Note**
The sensor needs to run for some time (normally a day or two) to collect enough information to use application mapping effectively.

**Task**
1. On the Rules page, select the Application Mapping tab, then select Audit Wizard.
2. From the Select DBMS drop-down list, select the DBMS for which you want to create an audit rule.
   Basic statistics are displayed indicating the application actions collected for the selected DBMS.
3. In the Audit by area, select Full Audit to monitor all elements on the DBMS or select one of the available elements from the drop-down down list.
   The page is refreshed according to the selected element type. For example, if Application is selected, the page is refreshed to enable you to select one or more applications.
4. Select the checkboxes for the elements where the rule is to apply. For example, if you opt to audit by application, you can select one or more applications.
5. (Optional) To create an exception to the rule, click Edit Filters in the Rule Exceptions area.
   The Rule Exceptions area is expanded to display the available exception categories in a tree-like hierarchy.
6. Select the exception category from the Exceptions tree, then select the checkboxes for the elements to be ignored. The resulting exception is displayed in the Exceptions selected text box.
7. Repeat for more exception categories as required.
8. Click Create Rule to save the rule. The rule is validated and added to the Custom Rules list.
9. If you would like to refine the rule further, in the Rule statement area, enter the rule comparator statement. For a detailed description of rule comparator statements and their syntax, see Rule syntax.

Create a mapping exception rule
After McAfee Database Security collects sampled information about the access to the DBMS, the Access Info page shows detailed information about the most commonly used “clusters” of applications, users, IP addresses, and more, which have accessed the DBMS during the sampling period, including a count for each such “cluster”.

This information can be used to create exception rules (for example, when a certain combination of IP address, application and user are audited elsewhere or are of no security/audit interest). The information gathered can also be used to create monitoring rules (for example, alert or audit each time the combination of user x, application y and IP z is detected).

You can define exceptions to your custom rules by creating an Allow rule and placing it before the relevant rules in the Custom Rules list. This option is normally used when you identify an activity that happens often and does not require monitoring. You can also create an alert rule for a specific combination. This option is used when you identify activity that should be monitored.
**Task**

1. On the Rules page, select the Application Mapping tab, then select DBMS Access Info. The DBMS Access Info page is displayed.

2. From the Select DBMS drop-down list, select the DBMS whose application mapping information you would like to review.

3. (Optional) To filter the display settings for the DBMS, enter the relevant criteria in the Filter area, then click Apply. The Display Settings table is filtered according to your selections.

4. Create the mapping rule:
   - To create an Allow rule, click the blue New icon in the row for the entry you want to allow. The Allow rule is created and added to the Custom Rules list.
   - To create an Alert rule, click the orange New icon in the row for the entry for which you want to create an alert rule. The Audit wizard page is displayed. Configure the alert details, as described in Create an alert rule.

5. Repeat for more entries in the table, as required.

---

**Working with tags**

You can use special tags to facilitate the systematic application of rules for specific purposes to specific DBMSs. Tags are applied to specific rules. The tags can then be used to apply multiple rules to a DBMS.

The use of tags is intended for advanced users of the Enterprise version and is purely optional.

Tags are created in the rule definition process. Existing tag assignments can be edited in the rule definition at any time.

**Tasks**

- Assign tags to rules
- Assign rules to DBMSs based on tags
- View tags per DBMS/DBMS group

**Assign tags to rules**

You can assign tags to existing custom rules by creating or selecting the tags in the rule definition.

**Task**

1. In the Custom Rules list, click the name of the rule that you want to edit. The rule properties are expanded to display the options that comprise the rule definition.

2. To assign a tag to the rule, enter the tag name in the Tags field or enter a space in the field to select the tag from the drop-down list.

3. Click Save.

**Assign rules to DBMSs based on tags**

You can check the extent to which the rules that include a specific tag are applied to the DBMSs. You can also systematically apply (or remove) rules that have a given tag from a DBMS.
Task

1. On the Rules page, select the Tags-DBMSs tab, then click View Tags.

   **Note**
   
   This option is enabled only if you have at least one custom rule that includes a tag.

2. Select a tag from the Tags drop-down list.

   The way that rules with the selected tag are applied to the DBMS/DBMS Groups is indicated in the Tag per DBMSs table, including these details:

   - **DBMS** — The name of the DBMS/DBMS Group.
   - **Rules Applied** — The number of rules that include this tag that are applied to the selected DBMS/DBMS Group relative to the number of rules that include this tag. For example, 25/50 indicates that out of a possible total of 50 rules, 25 of the rules have been applied to the selected DBMS/DBMS Group.
   - **Actions** — These actions can be performed from the Tags per DBMSs table on a row-by-row basis:
     - **Remove All** — Removes all rules that include the selected tag from the DBMS/DBMS Group.
     - **Apply All** — Applies all rules that include the selected tag from the DBMS/DBMS Group.

View tags per DBMS/DBMS group

The Tags-DBMSs tab shows the distribution of tags according to DBMSs and DBMS groups.

Task

1. On the Rules page, select the Tags-DBMSs tab, then click View DBMSs.

2. From the DBMS Groups and DBMSs drop-down list, select the DBMS/DBMS group.

   The Tag per DBMS Groups and DBMSs table indicates the extent to which the available tags have been applied to the selected DBMS/DBMS Group:

   - **Tag** — The name of the tag.
   - **Rules Applied** — The number of rules that include this tag that are applied to the selected DBMS/DBMS Group relative to the number of rules that include this tag. For example, 25/50 indicates that out of a possible total of 50 rules, 25 of the rules have been applied to the selected DBMS/DBMS Group.
   - **Actions** — These actions can be performed from the Tags per DBMSs table on a row-by-row basis:
     - **Remove All** — Removes all rules that include the tag from the selected DBMS/DBMS group.
     - **Apply All** — Applies all rules that include the tag from the selected DBMS/DBMS group.
Importing and exporting rules

You can import and export rules in XML file format, eliminating the need to define the same rule again for more DBMSs.

Tasks

- Export rules
- Import rules

Export rules

You can export a rule that has been defined for one DBMS to apply it to another DBMS.

Note

Compliance rules cannot be exported. All rule objects, including those created for the compliance rules, are exported.

Task

1. On the DBMS Properties page, select the Custom Rules tab, then click Export Rules.
2. Select Save to Disk, then click Save.

The displayed rules are exported to an XML file. (The location where the file is saved depends on your default settings.)

Import rules

You can import a previously defined rule and apply it to another DBMS.

Task

2. Select the saved rule file (.XML), then click Import.

The rules contained in the file are added to the Rules list.

If the imported rule objects already exist on the server, you can overwrite the existing objects with the imported objects or leave the currently installed rule objects untouched.

After importing the rules, you need to:

- Install the imported rules on the relevant DBMSs
- Enable the rules
Rule revisions

Rule revisions and history are important for several reasons. For example, if you need to roll back changes after mistakes are made in the policy or to comply with various standards and best practices. You can view the state of rules at any specific point in time and the revisions made to rules over time.

Tasks

- View the Rule Revisions list
- View rule revision details
- Compare revision details
- Configure rule modification and application mapping notifications

View the Rule Revisions list

Rule revisions are listed on the Rule Revisions tab.

Each rule revision entry reflects the existing rules at a given point in time, providing a virtual snapshot of the state of rules in the system.

Task

- On the Rules page, select the Rule Revisions tab.

The Rule Revisions tab lists these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision type</td>
<td>The type of rules or rule objects revised.</td>
</tr>
<tr>
<td>Revision date</td>
<td>The date and time of the revision.</td>
</tr>
<tr>
<td>Revision creator</td>
<td>The name of user who performed the revision.</td>
</tr>
<tr>
<td>Modified rules</td>
<td>The name of the rules modified.</td>
</tr>
<tr>
<td>Actions</td>
<td>![Folder] — Displays the details of the revision to the rule or rule objects</td>
</tr>
</tbody>
</table>

Note

You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see Filtering data.
**View rule revision details**

You can view the details of a rule revision entry in the Rule Revisions list. The rule revision data details the changes made from one implementation of revisions to the next, indicating whether changes have been made to the rules since the previous "snapshot" was recorded.

In addition, you can view the details of a previous revision and roll back to that previous revision if necessary.

**Task**

1. In the Rule Revisions list, click the Properties icon in the row for the revision.

   The Custom Rules Revision page is displayed for the selected rule revision, listing these parameters for each rule.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule properties.</td>
</tr>
<tr>
<td>Modification</td>
<td>If the rule has been changed since the previous Rule Revisions entry,</td>
</tr>
<tr>
<td></td>
<td>MODIFIED appears in this column.</td>
</tr>
<tr>
<td>Show Changes</td>
<td>Displays detailed information regarding the changes made to the rule.</td>
</tr>
</tbody>
</table>

2. To view the rule modification details, click the Show Changes icon in the row for the rule.

   Details regarding the rule modifications are displayed in read-only format.

3. To roll back the rule details to this rule revision, click the Roll back to revision link.

**Compare revision details**

You can select two revisions in the Rule Revisions list and compare their details.

**Task**

1. In the Rule Revisions list, select the checkboxes for two revisions, then click Compare.

   **Note**
   
   You can only compare revisions of the same type (for example, you cannot compare a vPatch revision with a custom rule revision).

2. To view the details of a specific revision, click the Properties icon in the row for the revision.

3. To roll back the rule details to the older rule revision, click the Roll back to revision link.

   **Note**
   
   You cannot roll back rule objects.
**Configure rule modification and application mapping notifications**

You can configure McAfee Database Security to notify you whenever a rule is modified.

If application mapping is enabled, you can also configure the system to automatically purge application mapping alerts when a configured number of alerts is exceeded.

**Task**

1. On the Rules page, select the Settings tab.
2. Select the *Send notification when rule changed* checkbox, then enter the e-mail address where the notification is to be sent in the *Send email to* field.

   **Note**  
   The email server settings must be configured on the System page to route e-mail alerts correctly.

3. In the Subject field, enter the text that is to appear in the subject line of the notification email.
4. In the Quiet Period field, enter the number of minutes during which no further notifications are sent.
5. In the When Application Mapping alerts exceed fields:
   - Set the number of alerts that triggers an automatic purge action.
   - Set the number of alerts to purge. Alerts are purged on a first-in-first-out basis, meaning that the oldest alerts are removed and the most recent alerts retained.
6. (Optional) To purge all saved mapping alerts for all DBMSs, click Purge All.

   **Note**  
   To purge all application mapping data for a specific DBMS only, click Purge in the DBMS Properties page for that DBMS.

7. Click Save.
McAfee Database Security Vulnerability Manager enables the configuration of VA scans of the databases to identify a wide range of risks and problems, such as weak passwords or missing patches.

You can configure multiple VA scans to run against one or more databases.

The **VA Scans** page comprises these tabs:

- **VA Scan Configuration** — Enables you to define, enable, disable, run and stop scans.
- **VA Scan Results Summary** — Summarizes the results of scans performed on the databases.

**Note**

This module is applicable for Vulnerability Manager users only. Other users can view the module but scan results are limited to four results per DBMS.

### Contents

- **VA Scans list**
- **Viewing the VA scan result summary**

## VA Scans list

The **VA Scan Configuration** tab of the **VA Scans** page lists results of the configured scans.

The **VA Scans** list includes these parameters for each scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Name</strong></td>
<td>The name of the scan.</td>
</tr>
<tr>
<td><strong>Run on</strong></td>
<td>The databases where the scan is configured to run.</td>
</tr>
<tr>
<td><strong>VA Scan Actions</strong></td>
<td>The action to be taken when a scan result is returned</td>
</tr>
<tr>
<td><strong>Last Run</strong></td>
<td>The date and time when the scan was last run.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The current state of the scan (for example, pending or scanning).</td>
</tr>
</tbody>
</table>
### VA scans

#### Managing VA scans

A VA scan runs one or more groups of tests on the database. VA scans can be scheduled in advance for set intervals or they can be run on demand.

### Tasks

- **Define a VA scan**
- **Enable or disable scheduled VA scans**
- **Schedule a VA scan**
- **Clone a VA scan**
- **Run a VA scan**
- **Stop a VA scan**
- **Remove a VA scan**

### Define a VA scan

A VA scan runs one or more groups of tests on the database. VA scans can be scheduled in advance at set intervals or they can be run on demand.

The available test groups are preconfigured, except for the custom test group that contains any customized tests defined in the **VA Tests** page. You can disable specific tests within a test group for a specific scan.

**Task**

1. On the **VA Scans** page, click **Create New Scan**.
2. In the **Scan Name** field, enter a name for the scan. It is recommended that the name selected clearly reflect the nature of the scan (for example, "Monthly vulnerability scan of production databases").
3. In the **Test Groups** section, click **Select Test Groups** to determine which tests are performed as part of the scan.
4. On the **Test Groups** page, select one or more test groups, then click **Done** to return to the **New VA Scan** page.

### Option | Definition
--- | ---
**Actions** | Properties — Displays the scan details.  
Clone — Duplicates a scan.  
Run VA Scan — Runs the scan.  
Stop VA Scan — Stops a currently running scan.  
Remove — Deletes the scan.

**Note**

You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see *Filtering data*. 

---

Managing VA scans

A VA scan runs one or more groups of tests on the database. VA scans can be scheduled in advance for set intervals or they can be run on demand.

### Tasks

- **Define a VA scan**
- **Enable or disable scheduled VA scans**
- **Schedule a VA scan**
- **Clone a VA scan**
- **Run a VA scan**
- **Stop a VA scan**
- **Remove a VA scan**

### Define a VA scan

A VA scan runs one or more groups of tests on the database. VA scans can be scheduled in advance at set intervals or they can be run on demand.

The available test groups are preconfigured, except for the custom test group that contains any customized tests defined in the **VA Tests** page. You can disable specific tests within a test group for a specific scan.

**Task**

1. On the **VA Scans** page, click **Create New Scan**.
2. In the **Scan Name** field, enter a name for the scan. It is recommended that the name selected clearly reflect the nature of the scan (for example, "Monthly vulnerability scan of production databases").
3. In the **Test Groups** section, click **Select Test Groups** to determine which tests are performed as part of the scan.
4. On the **Test Groups** page, select one or more test groups, then click **Done** to return to the **New VA Scan** page.
5 If you would like to view the list of all tests or disable specific tests, click Select Planned Tests to view the specific tests in the selected test groups.

6 To disable a specific test for this scan, click the ⬇️ icon. The icon toggles to ⬆️.

7 In the Actions section, select the actions to be taken when a scan result is returned:
   - McAfee Database Security Console — Generates a result on the VA Results page based on the selected result priority.
   - Syslog — Sends the result to the Syslog.
   - Windows Event Log — Sends the result to the Windows event log.
   - Log to file — Sends the result to the log file.
   - Automatically resolve to — Resolves the result and assigns it defined resolve type.
   - Email — Sends an email notification in addition to the alert in the log, with the specified importance (Low, Medium or High).

   **Note** See Managing custom rules for more information.

8 To select the DBMSs where the scan is run:
   - In the Run on section, click DBMSs & Groups.
   - Select one or more relevant DBMSs and/or DBMS Groups, then click Save to return to the rule definition page.

   The selected DBMSs and DBMS Groups are listed on the New VA Scan page.

9 To schedule the scan to run at regular intervals, select the Schedule enabled checkbox, then configure one of these scheduling intervals:
   - To run the scan more than once a day, select by hour, then indicate the time interval between scans.
   - To run the scan on a weekly basis, select by week, then select the day of the week when the scan is run.
   - To run the scan on a monthly basis, select by month, then indicate the number of months between scans.

10 (Optional) In the Description field, enter a free text/description or comment.

11 Click Save.

**Enable or disable scheduled VA scans**

You can enable or disable VA Scans at any time.

It is a good idea to disable a scan if you have started to define a scan, but have not completed it, or if you need to temporarily prevent the scan from running.

**Task**
   - In the VA Scan details, select or deselect the Schedule enabled option as required.
Schedule a VA scan
You can schedule a scan to run at regular intervals.

Task
1  In the VA Scans list, click the Properties icon in the row for the rule.
2  To schedule the scan to run at regular intervals, select the Schedule enabled checkbox and configure one of these scheduling intervals:
   ▪  To run the scan more than once a day, select by hour, then indicate the interval between scans.
   ▪  To run the scan on a weekly basis, select by week, then select the day of the week when the scan is run.
   ▪  To run the scan on a monthly basis, select by month, then indicate the number of months between scans.
3  Click Save.

The scan properties are updated to include the new scheduling information.

Clone a VA scan
You can create a new scan by cloning an existing scan. This eliminates the need to define all the scan properties from scratch when creating scans that share many common properties.

Task
1  In the VA Scans list, click in the row for the rule you want to clone.
   The New Scan page is displayed, with the properties of the original rule configured by default.
2  Change the scan name and modify specific scan properties as required. (For a detailed description of the scan parameters, see Define a VA scan.)
3  Click Save.

The scan is added to the VA Scans list.

Run a VA scan
You can manually initiate a VA scan at any time.

Task
- In the VA Scans list, click the Run icon in the row for the scan you want to run. The state of the scan is updated to Scanning while the scan runs.

Stop a VA scan
You can stop a scan that is in progress.

Task
- In the VA Scans list, click the Stop icon in the row for the scan you want to stop. The state of the scan is updated to Stopped.
Remove a VA scan
If a VA scan is no longer required, you can remove it from the VA Scans list.

Tip
If you think you might need the scan in the future, you can disable it for now and re-enable it at later date. For details, see Enable or disable scheduled VA scans.

Task
1. In the VA Scans list, click the Remove icon in the row for the scan you want to remove.
2. When prompted for confirmation, click OK.

The scan is removed from the VA Scans list.

Viewing the VA scan result summary
The VA Scan Result Summary tab of the VA Scans page summarizes the results of the VA scans.

The VA Scan Result Summary indicates the number of results of each level of severity, for each test category, for all databases included in the scan.

If multiple databases have been scanned, each database appears separately when selecting the properties icon. Expand the DBMS scan result by clicking the plus sign to view the breakdown of results according to test category. The top row for each database indicates the total number of results (all tests) for each severity for that database.
VA tests

A VA scan includes one or more tests. A test comprises specific checks to perform against the database.

In addition to using the predefined (out-of-the-box) VA tests, you can create customized VA tests to suit the needs of your organization. These custom tests can be added to the preconfigured test groups.

VA tests are normally created by advanced users only. It is recommended to create VA tests only after running VA scans several times and becoming deeply familiar with Vulnerability Manager capabilities.

Custom tests can be assigned to the custom or data discovery categories.

Contents
- VA Tests list
- Define a custom VA test
- Remove a custom VA test
- Defining test parameters by database

VA Tests list

Custom tests are listed in the VA Tests page.

The Custom Tests list includes these details for each test:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Name</td>
<td>The name of the test.</td>
</tr>
<tr>
<td>Result Type</td>
<td>The type of test results to return (for example, Yes/No or Result Set).</td>
</tr>
<tr>
<td>Test</td>
<td>(Custom tests only) The test itself (either a SQL command or an OS test script (Java script for Windows or shell script for Unix/Linux).</td>
</tr>
<tr>
<td>Test Category</td>
<td>The leading test group that the test belongs to.</td>
</tr>
<tr>
<td>Test Groups</td>
<td>The preconfigured test groups and user-created groups where tests can be added.</td>
</tr>
<tr>
<td>Level</td>
<td>The level of severity associated with the test results.</td>
</tr>
<tr>
<td>Status</td>
<td>Unlocked (can be edited, custom tests only) or Locked (cannot be edited).</td>
</tr>
<tr>
<td>Actions</td>
<td><img src="image" alt="Properties" /> — Displays the test details.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Remove" /> — Deletes the test.</td>
</tr>
</tbody>
</table>


Define a custom VA test

A VA test can be used to identify the existence of a specific condition or vulnerability, based on a Yes/No test, or they can return a set of relevant data.

**Task**

1. On the VA Tests page, click **Create New VA Test**.

2. In the **Test Name** field, enter a name for the test. It is recommended that the name selected clearly reflect the nature of the test.

3. From the **Result Type** drop-down list, select the type of test results to return: **Yes/No** or **Result Set** (including actual data).

4. In the **Test** field, enter the test parameters in SQL command format.
   
   For example, this ResultSet test would return a list of users granted the DBA role when run on an Oracle database:
   ```sql
   select * from dba_role_privs where granted_role = 'DBA'
   ```
   
   This Yes/No command would return a Yes result if dynamic SQL is detected in Oracle outside of SYS:
   ```sql
   select 'yes' from dual where exists (select 1 from dba_source where upper(text) like '%EXECUTE IMMEDIATE%' and owner <> 'SYS');
   ```

5. From the **Severity** drop-down list, select the level of severity to assign to test results.

6. From the **Test Category** drop-down list, select **Custom** or **Data Discovery**.
   
   Data Discovery is used when the rule is designed to discover particular tables/columns in the database. Choosing this category is essential so that you can later turn the results into rule objects.

7. In the **Test Groups** section, in the **All Groups** list, select one or more test groups to include in the custom test, then click **Move** to move them to the **Selected Groups** list.

   **Note**
   
   To remove a test group from the **Selected Groups** list, select it, then click **Move** to move it to the **All Groups** list.

8. In the **System Test Groups** section, in the **All System Groups** list, select one or more test groups to include in the operating system test, then click **Move** to move them to the **Selected System Groups** list.

   **Note**
   
   To remove a test group from the **Selected System Groups** list, select it, then click **Move** to move it to the **All System Groups** list.

9. (Optional) To exclude the test from running on one or more DBMSs, click **Remove test from DBMS**, then select the DBMSs to exclude.
Remove a custom VA test

If a VA Test is no longer required, you can remove it from the Custom Tests list.

**Task**

1. In the Custom Tests list, click the Remove icon in the row for the test you want to remove.
2. When prompted for confirmation, click OK.

The test is removed from the Custom Tests list.

Defining test parameters by database

If you have the necessary permissions, you can change specific test parameter values for individual databases or database groups for predefined tests. For example, you can set different password expiration intervals for different databases or database groups.

If a parameter value is defined for a database that belongs to a database group, the default value or the value assigned to the group is ignored, and the database specific value is applied.

If a database belongs to more than one group, and a parameter value is defined for one or more of the groups – but not for that specific database – the value defined for the first applicable database group listed in the Parameter Values section is applied. If a parameter value is not defined for the database or any of its database groups, the default value is applied.

**Tasks**

- Set test parameters by database
- Edit test parameter values
- Revert test parameter values
- Change the order of DBMS group parameter values

Set test parameters by database

**Task**

1. On the VA Tests page, click the Properties icon in the row for the test. The properties page is displayed for the selected test.

The check parameters are listed in the Check Parameters section. The values set for those parameters for specific databases and database groups are listed in the Parameter Values section. (This section is visible only if the test contains parameters that can be manually set. Default indicates that the value has not been changed.)
VA tests
Defining test parameters by database

The parameter values are checked in the order they appear in the Parameter Values section – first by specific DBMS, then if no value assigned for the DBMS, by DBMS group.

2 Click Add Parameter Value to DBMS or Add Parameter Value DBMS Group.

3 Enter the DBMS or DBMS Group name, then click Apply.

4 To set a parameter value, select the corresponding Override Default checkbox and enter the value in the adjacent field.

Note Only the parameters that you are allowed to change are listed in the dialog box. The description, data type (string, number, date), and default value are listed for each such parameter.

5 Repeat for more parameters as required.

6 Click Save.

When run, the test parameters are applied to the specified database according to the values set above.

Edit test parameter values
You can assign a specific value as the test parameter value. This value is applied instead of the default value.

Task
1 On the VA Tests page, click the Properties icon in the row for the test. The properties page is displayed for the selected test.

2 In the Parameters Values section, click the corresponding Edit icon. In the pop-up window, edit the test parameters, then click Save.

Revert test parameter values
You can revert a test parameter value to the default value.

Task
1 On the VA Tests page, click the Properties icon in the row for the test. The properties page is displayed for the selected test.

2 In the Parameters Values section, click the corresponding Edit icon.

3 In the pop-up window, deselect the Override Default checkbox next to the parameter name, then click Save.
Change the order of DBMS group parameter values

DBMS group parameters are checked in the order in which they appear in the Parameter Values section on the test properties page.

Task

1. In the Parameters Values section of the test properties page, click the Move icon.
2. In the pop-up window, reorder the DBMS groups, then click Save.

The parameter value used is determined based on the order in which the DBMS groups appear.
McAfee Database Activity Monitoring enables you to create security rules based on established international standards, including PCI-DSS, Sarbanes Oxley (SOX), SAS-70, GLBA and HIPAA. In addition, a Best Practices wizard is available, which can help in initiating an audit policy for regulatory compliance purposes.

Usually, it is important to enable vPatch rules on all in-scope databases (if they are not already enabled).

A compliance rule can be applied to all DBMSs or to specific DBMSs and DBMS groups.

The Compliance page lists the regulations for which compliance rules can be configured.

This section includes these topics:

- Configure compliance rule
- Save partial compliance rule settings
- Edit compliance rules

**Configure compliance rules**

Compliance rules are based on various established standards and regulations. Compliance rules are configured using the Compliance Wizard.

The specific definitions required in defining a compliance rule vary based on the type of regulation, therefore the parameters set in the configuration and the number of pages in the Compliance Wizard vary accordingly.

For the purpose of illustration only, the procedure below includes selected pages from within the PCI-DSS Compliance Wizard. Only those pages that include parameters common to all types of regulations are described herein. The parameters in additional pages should be configured based on the Wizard’s on-screen instructions.

**Note**

- Clicking Reset in any page resets the default values for that step only.
- If a red message appears after clicking Next, there is a problem with the values set for the indicated parameter. Fix the settings, then click Next again.

**Task**

1. On the Compliance page, select the type of regulation for which you want to verify compliance, then click Select.

   The Compliance page is redisplayed, indicating that the respective Compliance Wizard has not been completed and advising you of the information required to configure a compliance rule for the selected type of regulation.
2 Click **Configuration Wizard** to begin the process of configuring the compliance rule.

3 Select the DBMSs and/or DBMS Groups where you want to apply the compliance rule.

4 Click **Next** to display the **Application User Names** page of the Compliance Wizard is displayed.

5 Enter the usernames that are used by approved applications to access the DBMSs in either of these ways:
   - Enter the user names in the field provided separated by commas.
   - Import the contents of a CSV file containing the usernames by browsing to select the file and clicking **Upload**.

   **Note**
   From this point onward, you can opt to exit the Wizard and continue the configuration later from the point where you stopped. To do so, click **Proceed Later**. For details, see **Save partial compliance rule settings**.

6 Click **Next** to display additional Compliance Wizard pages and configure the necessary parameters according to the on-screen instructions on each page.

   Depending on the regulation type, the Cardholder Tables or Sensitive Data tables or another page of the Wizard is displayed.

7 Enter the database tables that contain cardholder data/sensitive data in any of the selected DBMSs in either of these ways:
   - Enter the database tables in the field provided.
   - Import the contents of a CSV file containing the database tables by browsing to select the file and clicking **Upload**.

8 Click **Next** to display additional Compliance Wizard pages and configure the necessary parameters according to the on-screen instructions on each page.

   Depending on the regulation type, the DDL Commands page of the Wizard is displayed several pages later.

   The DDL Commands are listed on the DDL page. You do not need to make any changes.

9 Click **Next** without making any changes. The next Compliance Wizard page is displayed.

10 Configure the necessary parameters according to the on-screen instructions on each page.

   Depending on the regulation type, the Complete page of the Wizard is displayed several pages later.

11 To enable the configured rule, read the instructions carefully, then select **Enable [Regulation Type] Compliance Rules**.

   **Note**
   If the above option is not selected, the rule is created but it is not enabled. Make sure that vPatch rules are enabled on all in-scope databases.
Save partial compliance rule settings

Once you have completed the initial pages of the Compliance Wizard, you can opt to exit the Wizard and continue the configuration later from the point where you stopped.

**Task**

1. In the **Compliance Wizard**, click **Proceed Later**. You are prompted to confirm that you want to close the wizard.
2. Click **OK**.
   
   A pop-up message indicates that the data has been saved and you can complete the configuration later.
3. To return to the wizard, select the regulation type and click **Configuration Wizard**.

   Although the wizard contains the values you previously configured, it is still displayed from its first page. Review your settings and continue from where you left off.

Edit compliance rules

You can edit the settings of a compliance rule.

**Task**

1. On the **Compliance** page, select the type of compliance rule regulation to be edited, then click **Select**.
2. Click **Edit Configuration**.
3. On the **Compliance Rules Configuration** dialog box, select the required action:
   
   - To reconfigure the rule properties, select **Reconfigure rules**. The Compliane Wizard is displayed, with the values you previously configured. Review and change the settings as required based on the on-screen instructions.
   - To disable the rules, select **Disable rules**. (To re-enable the rules, select **Enable rules**.)
   - When prompted for confirmation, click **OK**.
   - To remove the configuration, select **Remove configuration completely**. Exercise caution in selecting this option; this action cannot be reversed. This action totally deletes the existing configuration. The Compliance Wizard is automatically displayed, prompting you to completely redefine the regulation.
11 Sensors

McAfee Database Security Sensors are responsible for monitoring access to the DBMSs and sending transaction data to the McAfee Database Security Server. After installation, a sensor must be approved before it can begin active monitoring of a DBMS.

Contents
- Sensors list
- Approve a sensor
- Approve the DBMS
- Change the sensor action for a DBMS
- Sensor management
- Troubleshooting the sensor installation

Sensors list

The Sensors page lists the installed McAfee Database Security sensors, including these parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the sensor as configured in the installation process.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the sensor (CONNECTED, DISCONNECTED, or DELETED). By default, all deleted sensors are hidden. To view deleted sensors, you need to change the filter settings. When a DBMS is down, its status appears as DISCONNECTED. DBMS Down.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The name of the DBMS host server where the sensor is installed.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the sensor.</td>
</tr>
<tr>
<td>OS</td>
<td>The operating system of the sensor.</td>
</tr>
<tr>
<td>Approved By</td>
<td>If the sensor has been approved, the name of the user that approved the sensor appears. If the sensor has not been approved, the button appears. For details about approving a sensor, see Approve a sensor.</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays the sensor details.</td>
</tr>
<tr>
<td>Actions</td>
<td>The available actions:</td>
</tr>
<tr>
<td></td>
<td>- Stops the sensor. For details, see Stop a sensor.</td>
</tr>
<tr>
<td></td>
<td>- Deletes the sensor. For details, see Delete a sensor.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>Restarts sensor. For details, see Restart a sensor.</td>
</tr>
</tbody>
</table>

More sensor-related documentation is available from this page:

- Access the installation guide by clicking the McAfee Database Security Installation Guide link.
- Access the sensor troubleshooting guide by clicking the Troubleshooting link. For details, see Troubleshooting the sensor installation.

**Note**
You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see Filtering data.

**Tasks**
- View monitored DBMSs by sensor
- View sensor details
- Add a DBMS to a sensor

**View monitored DBMSs by sensor**
You can view a list of the DBMSs assigned to a sensor on the Sensors page.

**Task**
- On the Sensors page, select the sensor in the Sensors list.

The DBMSs monitored by the selected sensor are listed below the Sensors list, including these details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the DBMS.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of DBMS.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the DBMS.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the DBMS (Fully Monitored, Not Monitored, or Partly Monitored).</td>
</tr>
<tr>
<td>Action</td>
<td>The action that can be applied to the DBMS. For details, see Change the sensor action for a DBMS.</td>
</tr>
</tbody>
</table>

**View sensor details**
You can view the detailed properties of a sensor in the Sensor Properties page.

**Task**
1. On the Sensors page, click the Properties icon in the row for the sensor.

These sensor details are displayed on the Details tab of the Sensor Properties page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the sensor (editable).</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the DBMS host server where the sensor is installed.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the sensor.</td>
</tr>
<tr>
<td>MAC Address(es)</td>
<td>The MAC address of the host server NICs.</td>
</tr>
<tr>
<td>No. of CPU cores</td>
<td>The number of CPU cores detected on the host server.</td>
</tr>
<tr>
<td>Version</td>
<td>The sensor version.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system of the DBMS host server.</td>
</tr>
<tr>
<td>Log Level</td>
<td>The detail level of logs to be created (by default, the log level is set to INFO).</td>
</tr>
<tr>
<td>Log File Size</td>
<td>The maximum size of the log file (in MB).</td>
</tr>
<tr>
<td>Number of Log Files</td>
<td>The maximum number of log files to create.</td>
</tr>
</tbody>
</table>

2 To view the statistics for the DBMSs monitored by the selected sensor, click **Statistics Per DBMS**. These statistics are displayed on the **Statistics Per DBMS** tab:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the DBMS.</td>
</tr>
<tr>
<td>Note: If DBMSs have been configured in multiple partitions, a suffix indicates the partition number, for example, <code>&lt;databasename&gt;_p0</code>, <code>&lt;databasename&gt;_p1</code>.</td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of the DBMS host server where the sensor is installed.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the DBMS.</td>
</tr>
<tr>
<td>No. CPU</td>
<td>The number of CPUs used by the sensor to monitor this DBMS.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the DBMS (full, none, or partial).</td>
</tr>
<tr>
<td>Statements monitored last 5 minutes</td>
<td>The number of statements for this DBMS detected and monitored by the sensor in the last five minutes.</td>
</tr>
<tr>
<td>Statements monitored last 24 h.</td>
<td>The number of statements for this DBMS detected and monitored by the sensor in the last 24 hours.</td>
</tr>
</tbody>
</table>

**Add a DBMS to a sensor**

You can manually add a DBMS from the **Sensor Properties** page.

**Task**

1. On the **Sensors** page, click the **Properties** icon in the row for the sensor.

2. On the **Sensor Properties** page, select the **DBMS Details** tab.
3 Click Add a DBMS manually.

4 On the database properties page, configure these mandatory parameters:

   - Select New for a new DBMS (when adding a DB2 with multiple partitions, add the first partition. If you have already added a partition for the DBMS, select Cluster, then select the first partition that was already added).
   - Type — The type of database.
   - SID — The database instance identifier.
   - DBMS Home — The part to the database installation.
   - Architecture — The database architecture (32-bit or 64-bit).

5 Click Save.

### Approve a sensor

The sensor must be approved before it can begin active monitoring of the DBMS.

On 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 button appears.

#### Task

1 On the Sensors page, click the icon to approve the sensor.

   If a new sensor reports that it is monitoring a DBMS that is already recognized by McAfee Database Security, you are prompted to select the DBMSs to monitor. For details, see Approve the DBMS.

   If the sensor ID exists in the system, the Approve Sensor page 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 a single sensor.
   - Delete — Indicates that this sensor was added in error and should be removed from the configuration.

3 Click OK.
Approve the DBMSs

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

**Task**

1. On the Approve DBMS page, select the DBMSs to be monitored by the sensor.

   **Note**
   
   You can filter the list of DBMSs by selecting one of these options from the drop-down list above the list:
   
   - All DBMSs
   - New DBMSs
   - Existing DBMSs

2. If more than one DBMS has the same name, select one of these from the adjacent drop-down list:
   
   - New — Indicates this is a new DBMS that needs to be monitored separately from the existing DBMS.
   - Merge — Indicates this DBMS is the same DBMS and the entries should be merged.
   - Cluster — Indicates that the DBMS is included in a cluster (and your policy for the DBMS will be installed on all cluster members). If you select Cluster, the display expands to show details for the DBMS.

   You can choose whether you want to install triggers on each DBMS. It is highly recommended to use triggers (chosen by default) with Oracle DBMSs. Triggers used by McAfee Database Security are highly efficient and have minimal impact on the DBMS performance. Use triggers with MS SQL servers when you intend to use McAfee Database Security’s prevention capabilities (allowing you to stop DDL actions before they take place). You can always change your choice later by selecting DBMS properties on the DBMSs tab, or by selecting Manage DBMSs on the Sensors page.

3. Click Save to complete the approval process.

   The name of the logged on user is displayed in the Approved By column.

Change the sensor action for a DBMS

You can determine how the sensor handles a specific DBMS by setting the action for that DBMS to Start Monitoring or Stop Monitoring, as required.

**Task**

1. On the Sensors page, select the sensor.

   The DBMSs monitored by the selected sensor are listed below the Sensors list.

2. In the row for the DBMS, set one of these monitoring actions:

   - Click Start Monitoring to set the sensor to monitor a DBMS, then select the DBMSs to be monitored on the Approve DBMS page. For details, see Approve the DBMS.
   - Click Stop Monitoring to set the sensor to stop monitoring a DBMS.
Sensor management

You can start, stop, and delete sensors from the system according to the monitoring needs of your organization.

Tasks
- **Stop a sensor**
- **Restart a sensor**
- **Delete a sensor**

Stop a sensor
You can remove a sensor that is no longer used for monitoring purposes. As a result, monitoring of the corresponding DBMSs stops.

A stopped sensor is not deleted from the Sensors list.

**Task**
1. On the Sensors page, click ![Stop sensor](image) in the row for the sensor you want to stop.
2. When prompted for confirmation, click **OK**.

The sensor is stopped and no longer monitors the DBMS.

Restart a sensor
You can restart the sensor process as long as the sensor is connected. Use this function if you suspect that the sensor is malfunctioning or when asked to do so by tech support. This action is not available when a sensor is stopped or disconnected.

**Task**
1. On the Sensors page, click ![Restart sensor](image) in the row for the sensor you want to restart.
2. When prompted for confirmation, click **OK**.

The sensor is restarted and resumes its monitoring activities.

Delete a sensor
You can delete a sensor that is no longer used for monitoring purposes.

A deleted sensor is not deleted from the Web console, or from the DBMS itself, but its status is set to “DELETED”.

If you want to uninstall the sensor from the DBMS, you must access the DBMS host and uninstall the sensor (for example, using rpm –e in Linux machines, uninstall in MS Windows, and so on).

**Task**
1. On the Sensors page, click ![Delete sensor](image) in the row for the sensor you want to delete.
2. When prompted for confirmation, click **OK**.

The sensor no longer monitors the DBMS.
Troubleshooting the sensor installation

This section describes the preliminary actions for resolving 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 Web 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 HP-UX, run: `/sbin/init.d/ mfe-dbs--sensor status`
- On Windows, run: `services.msc` and look for the service " McAfee-DBS-Sensor"

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. If the sensor was connected to the server before applying the license, you need to manually restart the sensor.

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).

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

1. Verify that the server IP address and port are set correctly in the McAfee Database Security Sensor's configuration file (located in Linux): `/etc/sysconfig/mfe-dbs-sensor`; Solaris: `/etc/default/mfe-dbs-sensor`; AIX: `/etc/mfe-dbs-sensor`; HP-UX: `/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 can 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 from the McAfee Database Security Sensor server, contact your system administrator for support.
   - If the McAfee Database Security Server IP address and port are reachable from the McAfee Database Security Sensor computer and you still do not see the Sensor on the Sensors list on the McAfee Database Security Server, run the diagnostic tool (see Run the diagnostic tool), then contact McAfee support for assistance.

Note: The resolution state of alerts previously generated by the removed sensor is automatically updated to **Sensor Deleted** in the Alerts list.
If no DBMSs are displayed for your McAfee Database Security Sensor:

- On Windows platforms, run the diagnostic tool (see 0 Run the diagnostic tool) and then contact McAfee support for assistance.
- On non-Windows platforms, verify that:
  - You have group read and execute permissions on $ORACLE_HOME and $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 ‘mcafee’ OS user
  - 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 in this format: $ORACLE_SID:$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.
  - If your oratab file is in a different location, you can configure the sensor 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 the DBMS appears on the Sensors list, but is listed as disconnected:

3 Verify that Oracle is version 8.1.7 or above, or MS SQL Server 2000 or above, or Sybase ASE 12.5. If you are trying to monitor another DBMS version, verify with support that the version is already supported.

4 If the McAfee Database Security Sensor is still unable to monitor your DBMSs, run the diagnostic tool (see 0 Run the diagnostic tool), then contact McAfee support.

**Run the diagnostic tool (Analytic Package)**

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

You can change the sensor log level and remotely create an analytic package as follows:

1 On the Sensors page, click the Properties icon in the row for the sensor.
2 From the Log Level drop-down list, select DEBUG.
3 Run the McAfee Database Security Sensor for five minutes (no sensor restart is required).
4 Click Generate.
5 Restore the log level to INFO after troubleshooting is complete.

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

If you are running an earlier version or having trouble connecting to the sensor, perform these steps:

6 Change the log level from INFO to DEBUG in the sensor configuration file as follows:
Troubleshooting the sensor installation

7 Run the McAfee Database Security sensor for 10 minutes.

8 Run the diagnostic tool:

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

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

**Sensor log files**

Sensor log files use a base name (referred to later as `<BASE_NAME>`). The name on Linux and Unix is: `dbs.log` and on Windows it is: `logfile.log`.

- **Sensor main log** — Name: `<BASE_NAME>`. This log file contains general logging regarding the sensor. This includes communication flow, database detection, statistics and management of monitored DBMSs.

- **Sensor DBMS instance log** — Name: `<BASE_NAME>_<DBMS Unique Name>`. The sensor maintains a log file per monitored DBMS instance. The log file contains information for the specific monitored DBMS instance. This includes DBMS details, statistics and alerts.

- **Standard output log** — Name: `<BASE_NAME>.std`. This log file contains the standard output and standard error output of the Sensor process. The file contains a log line every time the Sensor is started and may contain sparse periodic information output. This file should not contain errors and should not grow in size. The file is not rolled over. If it grows beyond 1 MB it is recommended to review the file and, if needed, report it to McAfee support.

- **Cache Statistics log** — Name: `<BASE_NAME>.log_caches`. This log file contains statistics about internal caches used by the sensor. This file can help help in the analysis of sensor resource utilization.

**Sensor log file size**

When a log file reaches its maximum size, the log file is backed up by adding the number “1” after its file name extension and a new log file is created. The extension numbering of any existing backup files are incremented sequentially. For example, when `dbs.log` reaches its maximum size, it is renamed `dbs.log.1`; the file `dbs.log.1` is renamed to `dbs.log.2`, and so on, up to the maximum number of log files configured (the default setting is 13).

When the maximum number of files is reached, the oldest file is deleted.
Sensor log file size and maximum number of log files are configured on the Sensor properties page in the management console.

**Sensor log format**

The sensor main log and sensor DBMS instance logs use this format:

```
```

Sample log message:

```
```

The logs contain these fields:

- **DATE** — The time and date the log line was written. Time is formatted according to the local time zone of the machine where the sensor runs.
- **THREAD ID** — Operating system thread ID. The sensor is a multi-threaded process. This field can be used to monitor the activity of a single thread.
- **FILE NAME, LINE NUMBER** — Source file name and line number where the log line was called in the code. This helps McAfee support and engineering identify the code the log entry was generated from.
- **SEVERITY** — Severity of the log entry. These are the available log severity levels in order of severity:
  - **ERROR** — Represents an unexpected error or conditions that the sensor has encountered. Log lines with the ERROR severity indicate a problem that requires review.
  - **WARNING** — Represents transient conditions that might later lead to an error. These log entries can provide insight into subsequent errors. These log entries do not require review if not accompanied by ERROR entries.
  - **NOTICE** — Sensor’s default log level, useful information about the proper operation of the sensor.
  - **INFO** — Medium level of detailed information about sensor operation. This log level might be requested by McAfee Support for troubleshooting if DEBUG is generating too many log entries and logs are rolling over.
  - **DEBUG** — High level of detailed information about sensor operation. This log level is used by support and engineering teams for troubleshooting.
  - **TRACE** — Low level tracing information that might be requested by development teams. This log level is intensive and should not be set unless explicitly requested by McAfee support.
- **MESSAGE** — Log message. Can span multiple lines.

**Note**

The minimum severity level to write to the log file is configured on the Sensor properties page in the management console. The default and recommended level is NOTICE, meaning that NOTICE, WARNING and ERROR log lines are written to the log file. Changing to a log level below NOTICE can cause extensive logging and affect sensor resource utilization.
**Sensor startup logging**

When the sensor starts, it writes a special header in the log file in the following format:

```
*************************** Security Sensor Started [ <DATE> ] ****************************
```

Monitoring the sensor logs for this header can indicate when the sensor experienced a restart. Multiple sensor restarts in a short time period can indicate an issue that requires further investigation. On Unix/Linux systems, the sensor DBMS instance log also contains the start header as the instance is monitored by a child process that can be started and stopped. A process that experiences multiple restarts in a short time period can also indicate an issue that requires further investigation.

**Sensor cache statistics logging**

Starting from version 4.4.7, the sensor will log periodically (hourly) into a special file statistics about its cache usage. This file can assist to analyze resource utilization of the sensor. The file contain statistics for these sensor caches: rule cache, stored procedure cache, prepared statement cache, session per NIC, and the network session buffers. The format of each log entry beyond the standard header is:

```
<MONITORING_COMPONENT>: <SUB_COMPONENT> <STATS_INFO>
```

The log contains these fields:

- **MONITORING_COMPONENT** — Either NETWORK or MEMORY. Indicates the monitoring technology that the statistics info entry is related to.

- **SUB_COMPONENT** — One of the following depending on the stats info entry:
  - DB instance name — Format: DB[<full_db_name>].
  - A network interface name — Format: NIC[<full_nic_name>].
  - GLOBAL — A global stats info entry not related to a specific network interface or DB instance.

- **STATS_INFO** — The statistics information to be logged.

Sample log messages:

```

NETWORK: DB[myhost_SQL2012RTM_6049d7b3295c468a7b638d4ff2738352ab4c794a]: Stored Procedure Cache[maxSize[81920KB],load[0%]] Rule Cache[disable]

MEMORY : DB[myhost_SQL2012RTM_6049d7b3295c468a7b638d4ff2738352ab4c794a]: Stored Procedure Cache[maxSize[81920KB],load[22%],elements[2695],averElemSize[6881B],access[139],misCount[34],misRate[24%],hitCount[105],hitRate[75%],latest:[access[0]] Rule Cache[maxSize[52428800],used[80%],nodes[165],totalAccessCount[7261],totalHitCount[3730],totalHitRate[51%],totalMissCount[3531],totalMissRate[48%]]

NETWORK: DB[myhost_SQL2012RTM_6049d7b3295c468a7b638d4ff2738352ab4c794a]: Prepared Statement Cache[maxSize[51200KB],load[0%],elements[32],averElemSize[1460B],access[0]]
```
Searching sensor logs for errors
You can use the "] ERROR " search string to identify errors in the sensor logs.

For example, to search for errors using the Linux/Unix **grep** utility:

```bash
grep '] ERROR ' dbs.log*
```

For example, to search for errors using the Windows **find** utility:

```bash
find '] ERROR ' logfile.log*
```

Common log errors explained

Data access layer errors
Data access layer (DAL) errors are identified by a file name of the form: Dal*.cpp. For example: DalOracle.cpp, DalTeradata.cpp, DalMSSQL.cpp. They usually occur when the sensor fails to connect or execute a statement on the database. If the failure is critical, the sensor sends a message box notification (Error 9 – DAL_ERROR) to the server with details of the failure. These errors can also appear in the log in non-critical situations, such as when the database is shutting down or restarting. In such cases, it is best to examine the log and see if the situation is resolved once the database is up and running.

An error log indicating failure to delete the failed login trace during a database restart:


Log line later on successful connection:


Communication errors
Communication errors are identified by the file names: ServerConnection.cpp and ServerTransportTCPSSL.cpp. They usually occur when the sensor has a problem communicating with the server. The problem might be transient (such as a network disconnect). It is best to examine the log to see if the communication resumed following the error.

An error log entry (followed by warning message with more info) indicating failure to communicate:


Log line later upon successful connection:

DBMSs

McAfee Database Security provides protection for the DBMSs where McAfee Database Security Sensors have been installed as well as DBMSs available for Vulnerability Manager VA scans.

The monitoring policy for a DBMS comprises the various rules that are enabled and applied on that DBMS. After installing a McAfee Database Security Sensor on a DBMS host server, if more than one DBMS is installed on the host, the DBMS must be approved in the McAfee Database Security configuration before a monitoring policy can be applied to it.

The DBMSs page lists the DBMSs where McAfee Database Security Sensors have been installed, and enables you to view the properties of each DBMS.

Contents

- DBMSs list
- Viewing DBMS properties and triggers
- View sensors by DBMS
- Working with network scans
- Managing DBMS groups

Note

For a description of the configuration of the rules that make up the monitoring policy, see Error! Reference source not found..

DBMSs list

The DBMSs page lists the DBMSs currently monitored by the McAfee Database Security Sensors, including these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>An icon indicating how the database is configured, for Data Activity Monitoring (DAM) and/or Vulnerability Assessment (VA).</td>
<td></td>
</tr>
<tr>
<td>DBMS</td>
<td>The name of the DBMS.</td>
</tr>
<tr>
<td>Note: When viewing IBM DB2, if DBMSs have been configured on multiple partitions, a suffix indicates the partition number, for example, &lt;databasename&gt;_p0, &lt;databasename&gt;_p1.</td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>The name of the host where the DBMS is installed.</td>
</tr>
<tr>
<td>Type</td>
<td>The DBMS type.</td>
</tr>
<tr>
<td>Version</td>
<td>The DBMS version.</td>
</tr>
</tbody>
</table>
### DBMSs

**Add a VA DBMS**

Multiple DBMSs can be configured for vulnerability assessment. VA DBMSs are not automatically added to the configuration.

**Task**

1. On the **DBMSs** page, click **Add VA DBMS**.

2. From the **DBMS type** drop-down list, select the database type (for example, Oracle, MSSQL, MYSQL, SQL Azure, PostreSQL, or Sybase).

   Due to MySQL licensing restrictions, you need to download the MySQL JDBC driver from the MySQL website:
   
   - Extract the file: mysql-connector-java-<version>-bin.jar and copy it to \common\lib
   - Restart the Database Security server

3. In the **Host/IP** field, enter the name of the host server or IP address, then click **Test** to verify the validity of the name/IP.

4. Configure these host parameters:
   
   - Select **Port** and enter the number of the port for connecting to the database. Then click **Test** to check its validity.
   - Select **SID/Service** and enter the service name or database instance ID on the server. Then click **Test** to check its validity.

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>A brief description of the DBMS.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The current monitoring status:</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Fully Monitored</strong> — The DBMS is fully monitored, that is, all sensors monitoring the DBMS are up and running (more than one sensor monitors a single DBMS if the DBMS is clustered).</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Not Monitored</strong> — There is currently no connection with any of the sensors monitoring the DBMS.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>PARTIAL</strong> — Not all sensors that should be monitoring the DBMS are monitoring it.</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays the main DBMS screen enabling customization of policy rules, editing of the DBMS details, and more.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td><strong>Remove</strong> — Removes the sensor (and undeletes the sensor when deleted sensors are viewed using the filter).</td>
</tr>
</tbody>
</table>

**Note**

You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see *Filtering data*. 

---

100 McAfee Database Security 4.6.x Product Guide
5 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 permissions for scanning are available in the screen.

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

7 (Optional) Click **Advanced** to configure more VA parameters (used for troubleshooting purposes only):
   - **Connection String** — The 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 these 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 the DBMS can use. 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 this DBMS belongs to.

8 (Optional) To view users that were excluded from weak password tests, expand the **Exclude Users from test** section. The listed users are exempt from weak password tests based on exceptions in the VA Results page. You can manually delete a user from the list if needed.

9 (Optional) Click **OS Connection** to configure the connection for testing the operating system:
   - **OS User Name** — The user name to be used to log on to the operating system.
   - **OS Password** — The password to be used to log on to the operating system.
   - **OS Connection Type** — The type of connection used to test the operating system.
   - Click **Check OS Connection** to check the connectivity.

10 Click **Save**.

The DBMS appears in the DBMSs list.

**Viewing DBMS properties and triggers**

You can view the detailed properties of a DBMS, including its name, description, and DBMS Group assignment, and if applicable.

The DBMS properties also include the trigger settings for the DBMS. A Data Definition Language (DDL) trigger can be added to the monitored database to prevent DDL actions before they happen.
Stopping a DDL action requires relevant custom rules, for example, `cmdtype = 'drop table'` and user `<> $privileged_users`. The DDL trigger was designed to have minimal impact on the DBMS. But, with heavy DDL traffic, the delay that the DDL trigger introduces can cause unwanted latency.

In addition, a DML trigger is available for customers who want to audit before and after values when data changes occur. Unlike the DDL trigger, the DML trigger can cause severe latency and should be used sparingly.

**Tasks**

- View DBMS properties
- View DML monitoring results
- Enable or disable DML triggers
- Enable or disable redo buffer monitoring
- Configure failed logins
- Configure the character set
- Enable application mapping

**View DBMS properties**

- In the DBMS list, click the Properties icon in the row for the DBMS.

The Properties page lists these parameters for the selected DBMS.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the DBMS.</td>
</tr>
<tr>
<td>Database version</td>
<td>The database type and version.</td>
</tr>
<tr>
<td>Instance Name</td>
<td>The name of the DBMS instance.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the DBMS.</td>
</tr>
<tr>
<td>vPatch Coverage</td>
<td>- Available vPatch relevant protections.</td>
</tr>
<tr>
<td></td>
<td>- Available relevant Oracle Critical Patch Updates.</td>
</tr>
<tr>
<td>Enable VA</td>
<td>When selected, if the DBMS is monitored by a sensor, Vulnerability</td>
</tr>
<tr>
<td></td>
<td>Assessment (VA) scans are enabled for the chosen DBMS.</td>
</tr>
<tr>
<td></td>
<td>- User Name — The user name used to connect to the DBMS.</td>
</tr>
<tr>
<td></td>
<td>- Password — The password used to connect to the DBMS.</td>
</tr>
<tr>
<td></td>
<td>- Host — The name of the host where the DBMS is installed.</td>
</tr>
<tr>
<td></td>
<td>- Port — The port on the host used to connect to the DBMS.</td>
</tr>
<tr>
<td></td>
<td>- Instance Name — The name of the DBMS instance.</td>
</tr>
<tr>
<td>Advanced Connection</td>
<td>Additional VA parameters:</td>
</tr>
<tr>
<td></td>
<td>- Connection String — The connection string used to connect to the DBMS</td>
</tr>
<tr>
<td></td>
<td>used for troubleshooting purposes.</td>
</tr>
<tr>
<td></td>
<td>- Connection Properties — Used for connection troubleshooting purposes.</td>
</tr>
<tr>
<td>Exclude Users from test</td>
<td>Lists the credentials of users to be excluded from weak password tests.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable OS tests (Windows)</td>
<td>When selected, operating system level tests are enabled on the DBMS. This option is available only when the Enable VA option is selected.</td>
</tr>
<tr>
<td></td>
<td>• OS User Name — The user name used to log on to the operating system.</td>
</tr>
<tr>
<td></td>
<td>• OS Password — The password used to log on to the operating system.</td>
</tr>
<tr>
<td></td>
<td>• OS Connection Type — The type of connection used to test the operating system (for example, dcom or SSH).</td>
</tr>
<tr>
<td>Network/Memory Configuration</td>
<td>• Enable Network Monitoring — When selected, enables the monitoring of network access to the DBMS. Do not change settings unless advised to do so by technical support.</td>
</tr>
<tr>
<td></td>
<td>• Prepared Statement Cache Size — The size of the cache (in MB) that can be used to hold prepared statements in the DBMS. Do not change settings unless advised to do so by technical support.</td>
</tr>
<tr>
<td></td>
<td>• Network Listening Ports — The ports on the DBMS used for network monitoring purposes. Do not change settings unless advised to do so by technical support.</td>
</tr>
<tr>
<td></td>
<td>• Enable Memory Monitoring — When selected, enables the monitoring of memory usage by the DBMS. Do not change settings unless advised to do so by technical support.</td>
</tr>
<tr>
<td>Application Mapping</td>
<td>• Enable Application Mapping — When selected, enables the mapping of application access to the DBMS.</td>
</tr>
<tr>
<td></td>
<td>• Limit Application Mapping Alerts per Second — The maximum number of application mapping alerts that are sampled per second.</td>
</tr>
<tr>
<td></td>
<td>• Notify When Database Events Count Exceeds — The number of database events, which when exceeded, triggers notification.</td>
</tr>
<tr>
<td></td>
<td>• Purge DBMS Application Mapping Data — When selected, purges all DBMS application mapping data for the DBMS.</td>
</tr>
<tr>
<td>Failed Login</td>
<td>• Failed Login Count — The number of failed attempts to log in to one DBMS in the defined Failed Login Measure Period that triggers an alert (if triggers are enabled).</td>
</tr>
<tr>
<td></td>
<td>• Failed Login Measure Period — The time period in which, if the Failed Login Count is exceeded, an alert is generated by the vPatch rules.</td>
</tr>
<tr>
<td>DDL/DCL Monitoring</td>
<td>• Enable Triggers — When selected, the DDL and Failed login triggers are enabled on the DBMS.</td>
</tr>
<tr>
<td></td>
<td>• DDL/DCL Delay Time — The time period for which the trigger delays the execution of the DDL/DCL command to allow the rule action to run first (so it can terminate the session before the statement is executed if so required by the rule).</td>
</tr>
<tr>
<td></td>
<td>• DML Monitoring — Similar to the DDL trigger, the DML trigger delays DML actions so that they can be prevented. In addition, the DML trigger provides the before and after values of selected columns.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The DML trigger is available only for DBMSs where VA is enabled.</td>
</tr>
<tr>
<td>Alternative DBMS Connection</td>
<td>• Enable alternative DBMS connection (advanced users only) — When selected, alternative connections can be made using these parameters:</td>
</tr>
<tr>
<td></td>
<td>• User Name — The user name used to connect to the DBMS.</td>
</tr>
<tr>
<td></td>
<td>• Password — The password used to connect to the DBMS.</td>
</tr>
<tr>
<td></td>
<td>• Connection String — The connection string used to connect to the DBMS. This parameter is applicable for Oracle DBMSs only.</td>
</tr>
</tbody>
</table>
### DBMSs
Viewing DBMS properties and triggers

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Miscellaneous** | - McAfee Database Security Cache Size — The size of the cache that the DBMS can use. This parameter is applicable for SQL DBMSs only.  
- DBMS Groups — The DBMS groups to which this DBMS belongs. |
| **Charset** | The DBMS character set (not shown on MS SQL databases):  
- Detected — The detected character set.  
- Selected — The selected character set. |

### View DML monitoring results
The DML trigger delays DML actions so that they can be prevented. In addition, the DML trigger provides the before and after values of selected columns. The DML trigger introduces latency, so it is recommended to use this feature sparingly.

**Note**
The DML trigger is available only for DBMSs where VA is enabled.

**Task**
1. Add a DML trigger. When a new trigger is added, a test is automatically created (called monitor DML actions on table [table name]).
2. When prompted, select up to 10 columns for monitoring. The trigger keeps data on the original database and on the results screen according to the relevant tests.
3. Include the test in a scan. After running the scan, you can review results in the **Results** tab.

**Note**
You can search the scan results.

### Enable or disable DML triggers
You can enable or disable DML triggers.

**Task**
- On the **DBMS Properties** page, select or deselect the **Enable Triggers** option as required.

### Enable or disable redo buffer monitoring
Redo buffer monitoring enables McAfee Database Security to obtain DDL statements without installing triggers.

**Note**
Enabling redo buffer monitoring disables triggers.

**Task**
- On the **DBMS Properties** page, select or deselect the **Monitor Redo Buffer** option as required.
Configure failed logins
You can determine the number of failed logins in a set time period that is considered abnormal for the DBMS.

**Note**
Only vPatch rules use the failed login feature.

**Task**
1. In the Failed Login Count field, set the number of failed attempts to log in to a single DBMS within the defined Failed Login Measure Period that triggers an alert.
2. In the Failed Login Measure Period field, set the time period (in seconds) within which, if the Failed Login Count is exceeded, an alert is triggered by the vPatch rules.
3. Click Save.

Configure the character set
International character sets are supported. Normally, the correct character set is automatically detected.

Sometimes (such as if the DBMS is configured with one character set but another character set is being used), manual configuration of the character set is required.

**Task**
- To select the correct character set, select the DBMS Properties page and the select the required character set from the Charset drop-down list.

Enable application mapping
You can configure the mapping of application access per DBMS. Application Mapping is enabled by default for every new monitored DBMS. It is recommended to turn off the function after configuring the policy and determining that application mapping is no longer required.

**To configure application mapping:**
1. On the DBMS Properties page, select the Application Mapping checkbox.
2. In the Limit Application Mapping Alerts per Second field, set the maximum number of application mapping alerts are sampled per second.
3. In the Notify When Database Events Count Exceeds field, set the number of database events, which when exceeded, triggers notification.
4. Click Save.

**Note**
To purge all application mapping data for the DBMS, click Purge in the DBMS Properties page. (Optional) To purge all saved mapping data for all DBMSs, click Purge on the Rule Settings tab of the Rules page.
View sensors by DBMS

You can view a list of the sensors used to monitor a DBMS on the DBMSs page.

To view the sensors that monitor a DBMS:

- On the DBMSs page, select the DBMS.

The sensors that monitor the selected DBMS are listed below the DBMSs list, including the name and status of the sensor.

Monitor a clustered database

You can monitor clustered databases by installing sensors on the cluster nodes.

Task

1. Finish the installation of the first sensor, preferably the active node, and approve the sensor and the DB.
2. Install the additional sensor in the second node, approve the sensor and discover the DB.
3. Instead of approving the DB, select the Cluster option, then click Next.
4. Select the DBs that are part of this cluster, then click Next.
5. Select the cluster configuration from the drop-down list based on the type of cluster in use (Active/Active or Active/Passive).
6. Click Save.

Working with network scans

Network scans search your network for databases that have not yet been added to the DBMSs list. Discovered DBMSs can be added to VA scans. To monitor the databases, install a sensor on the database server host.

DBMS network scans are configured on the DBMS Network Scanner tab.

Tasks

- View network scan results
- Filter the network scan results
- Create a network scan
- Create a VA DBMS from scan results
- Clone a network scan
- Stop a network scan
- Rerun a network scan
- Delete a network scan
View network scan results
The DBMS Network Scanner page lists the configured network scans and their results.

**Task**
- On the DBMS page, select the DBMS Network Scanner tab.

The DBMS Network Scanner page lists these scan properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The name of the discovered server.</td>
</tr>
<tr>
<td>Scan Date</td>
<td>The date and time the scan was last run.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the scan (pending, completed, and so on).</td>
</tr>
<tr>
<td>IP Range</td>
<td>The range of network addresses to be scanned.</td>
</tr>
<tr>
<td>Port Range</td>
<td>The range of ports to be scanned.</td>
</tr>
<tr>
<td>Open Ports</td>
<td>The number of open ports detected.</td>
</tr>
<tr>
<td>Instances</td>
<td>The number of database instances detected.</td>
</tr>
</tbody>
</table>

Filter the network scan results
To facilitate the viewing of network scan results when working with multiple scans, you can filter the Network Scan Results list according to various properties.

**Task**
1. Expand the Edit filter values area above the Network Scan Results list.
2. Set one or more filter criteria by entering/selecting the relevant values (for example, status).
3. Click Apply.

The list is filtered to display only those scan results that match the filter criteria.

**Note**
To clear all filter selections, click Clear, then click Apply.

Create a network scan
You can create multiple network scans to search your network for databases that have not yet been added to the DBMSs list.

**Task**
1. On the DBMSs page, select the DBMS Network Scanner tab, then click Create Network Scan.
2. In the Network Timeout field, set the timeout for IP connectivity.
3. In the IP Ranges field, set the range of IP addresses to be scanned on the network.
4. In the Number of Scanning thread fields, set the maximum number of concurrent scans.
To check the IP connectivity before scanning the ports, select the **Check ICMP/Echo before ports** checkbox.

To schedule the network scan, click **Schedule Network** scan, then configure these parameters:

- Select the **Schedule enabled** checkbox.
- To run the scan more than once a day, select **by hour**, then indicate the interval between scans.
- To run the scan on a weekly/daily basis, select **by day**, then select the day of the week when the scan is run.
- To run the scan on a monthly basis, select **by month**, then indicate the number of months between scans.

To scan for Oracle servers, click **Advanced Scan Configuration for Oracle**, then set these parameters:

- Select the **Check Oracle** checkbox.
- To automatically add the default Oracle ports, select the **Add Oracle default ports** checkbox.
- In the **Ports to scan** field, specify the ports to be scanned on the Oracle servers.
- To try to guess the Oracle SID names, select the **Brute force Oracle names** checkbox.

To scan for MS SQL servers, click **Advanced Scan Configuration for MS SQL**, then set these parameters:

- Select the **Check MS SQL Server** checkbox.
- To automatically add the default MS SQL ports, select the **Add MS SQL default ports** checkbox.
- In the **Ports to scan** field, specify the ports to be scanned on the MS SQL servers.
- To try to guess the MS SQL instance names, select the **Brute force MS SQL names** checkbox.

To scan for Sybase servers, click **Advanced Scan Configuration for Sybase**, then set these parameters:

- Select the **Check Sybase** checkbox.
- To automatically add the default Sybase ports, select the **Add Sybase default ports** checkbox.
- In the **Ports to scan** field, specify the ports to be scanned on the Sybase servers.
- To try to guess the Sybase instance names, select the **Brute force Sybase names** checkbox.

To scan for DB2 servers, click **Advanced Scan Configuration for DB2**, then set these parameters:

- Select the **Check DB2** checkbox.
- To automatically add the default Sybase ports, select the **Add DB2 default ports** checkbox.
- In the **Ports to scan** field, specify the ports to be scanned on the DB2 servers.
- To try to guess the DB2 instance names, select the **Brute force DB2 names** checkbox.

To scan for MySQL servers, click **Advanced Scan Configuration for Mysql**, then set these parameters:

- Select the **Check Mysql** checkbox.
- To automatically add the default Sybase ports, select the **Add Mysql default ports** checkbox.
- In the **Ports to scan** field, specify the ports to be scanned on the MySQL servers.
To try to guess the MySQL instance names, select the Brute force Mysql names checkbox.

12 To scan for PostreSQL servers, click Advanced Scan Configuration for Postgresql, then set these parameters:
   - Select the Check Postgresql checkbox.
   - To automatically add the default Sybase ports, select the Add Postgresql default ports checkbox.
   - In the Ports to scan field, specify the ports to be scanned on the Postgresql servers.
   - To try to guess the PostgreSQL instance names, select the Brute force Postgresql names checkbox.

13 Click Create Network Scan.

The scan is added to the Network Scans list.

Create a VA DBMS from scan results

You can view the details of a scan in the Network Scans list and create a VA DBMS for a database instance in the scan results.

Task
1 In the Network Scans list, click the Properties icon in the row for the scan results.
   The Create VA DBMS from Scan Results page is displayed, listing the detected database instances, including IP addresses, ports, and instance names.
2 Select the database instance for which you want to create a VA DBMS.
3 In the Username and Password fields, specify the username and password to be used to connect to the databases.
4 Click Create VA DBMSs.

The DBMS is added to the DBMSs list.

Clone a network scan

You can create a scan by cloning an existing scan. This eliminates the need to define all the scan properties from scratch when creating scans that share many common properties.

Task
1 In the Network Scans list, click in the row for the scan you want to clone.
   The New Scan page is displayed, with the properties of the original rule configured by default.
2 Change the scan name and change specific scan properties as required. (For a detailed description of the scan parameters, see Create a network scan.)
3 Click Save.

The scan is added to the Network Scans list.
Stop a network scan
You can stop a scan that is in progress.

Task
1. On the **DBMSs** page, select the **DBMS Network Scanner** tab, click the **Stop** icon in the row for the network scan results.
2. When prompted for confirmation, click **OK**.

Rerun a network scan
You can rerun a scan to check for new results.

Task
- On the **DBMSs | DBMS Network Scanner** tab, click the **Run** icon in the row for the network scan results.

Delete a network scan
If a scan is no longer required, you can remove it from the **Network Scan Results** list.

Task
1. On the **DBMSs** page, select the **DBMS Network Scanner** tab, then click the **Delete** icon in the row for the network scan results.
2. When prompted for confirmation, click **OK**.

Managing DBMS groups
To facilitate the application of rules to multiple DBMSs, you can create DBMS Groups. Rules that are applied to a DBMS Group are applied to all group members.

DBMS Groups are configured in the **DBMS Groups** tab of the **DBMS** page.

The **DBMS Groups** tab lists the existing DBMS Groups, including these parameters:

- **Name** — The name of the DBMS Group.
- **Description** — A brief description of the DBMS Group.
- **Properties** — An icon, which when clicked, enables you to view the DBMS Group details.
- **Remove** — An icon, which when clicked, deletes the DBMS Group (available only for user-defined DBMS groups).

Tasks
- **Create a DBMS group**
- **Create a DBMS group**
- **View/edit a DBMS group**
- **Delete a DBMS group**
Create a DBMS group
A DBMS Group is a subset of DBMSs to which various rules can be applied. You can define multiple DBMS Groups in keeping with the needs of your enterprise.

A DBMS Group can comprise any number of DBMSs. A specific DBMS can be a member of more than one DBMS Group. Rules that are installed on a DBMS Group are applied to all group members.

**Task**
1. On the DBMS Groups tab, click New DB Group. The DBMS Properties page is displayed.
2. Enter the name of the DBMS Group in the Name field.
3. Enter a brief informative description of the group in the Description field.
4. Select the DBMSs to include in the group from the All DBMSs list, then click the arrow to move it to the Selected DBMSs list.

**Note**
To remove a DBMS from the Selected DBMSs list, select it, then click .

5. Click Save.

View/edit a DBMS group
You can view and edit the properties of a DBMS Group.

**Task**
1. On the DBMS Groups tab, click the Properties icon in the row for the rule object. The DBMS Group Properties page is displayed.
2. Edit the DBMS Group properties, then click Save.

Delete a DBMS group
You can delete a DBMS Group that is no longer needed, but it is recommended that you exercise caution in doing so.

Deleting a DBMS Group does not delete the DBMSs that were included in the group. But, if you delete a DBMS Group that is used in a rule, the rule is automatically disabled for all members of that DBMS Group. As a result, if the rule was applied only to that DBMS Group, the rule must be assigned to specific DBMSs or other DBMS Groups in the rule definition for it to have any impact.

**Task**
1. On the DBMS Groups tab, click the DBMS Group to be deleted.
2. When prompted for confirmation, click OK.

The DBMS Group is removed from the DBMS Groups list.

**Note**
If the system detects specific problems related to the proposed deletion, an additional message describes the potential consequences and prompts you to again confirm that you want to delete the DBMS Group.
Apply DBMS actions

You can apply an action to multiple DBMSs by selecting the DBMSs on the DBMSs tab, then clicking [apply actions]. The available actions include:

- Failed logins configuration
- Trigger action configuration
- Alternate connection configuration
- Charset configuration
McAfee Database Security enables you to assign different levels of permissions to different administrators by assigning each admin user to a specific role. Each role comprises a specific set of permissions, which are granted to those users assigned to the role.

McAfee Database Security is provided with predefined roles. You can assign users to predefined roles or you can create and assign new roles.

**Contents**
- Predefined roles
- Roles list
- Create a new role
- Edit the permissions of an existing role
- Remove a role

**Predefined roles**

McAfee Database Security is provided with these predefined roles:

- **Read Only** — Enables the user to view all screens and settings, but cannot make and changes to rules, resolve alerts, and so on.

- **McAfee Database Security Operator** — Enables the user to perform operations in the system, but cannot change the security policy and related objects.

- **Policy Creator** — Enables the user to create and edit rules, and configure other system components, however the policy creator is not authorized to view alerts.

- **Read Only Alerts** — Provides the user with read-only access to the Dashboard and the Alerts list.

You can edit the permissions assigned to each of these roles to suit the needs of your organization. For instructions, see *Edit the permissions of an existing role.*
Roles list

The Roles tab of the Permission page lists the roles defined for users in the system, including these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The ID number of the role.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the role.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the role.</td>
</tr>
<tr>
<td>LDAP</td>
<td>If selected, enables you to use your existing system of user groups in your active directory.</td>
</tr>
<tr>
<td>Properties</td>
<td>An icon, which when clicked, enables you to view and edit the properties of the role.</td>
</tr>
<tr>
<td>Remove</td>
<td>An icon, which when clicked, removes the role from the Roles list.</td>
</tr>
</tbody>
</table>

Note You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see Filtering data.

View role details

You can view the detailed properties of a role on the Role Details page.

Task
- In the Roles list, click the Properties icon in the row for the role.

These role details are displayed in the Role Properties page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the role.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the role.</td>
</tr>
<tr>
<td>Selected permissions</td>
<td>A list of the permissions assigned to the role.</td>
</tr>
<tr>
<td>Selected roles</td>
<td>A list of the permission sets assigned to the role.</td>
</tr>
<tr>
<td>View Alert permissions by DBMSs</td>
<td>A list of the DBMSs and DBMS groups for which, if selected, the role is authorized to view alerts.</td>
</tr>
<tr>
<td>View Alert permissions by Rules</td>
<td>A list of the rules for which, if selected, the role is authorized to view alerts.</td>
</tr>
</tbody>
</table>
Create a new role

In keeping with organization-specific needs, you can create multiple roles – each of which comprises a unique set of permissions.

A role can also be based on the permissions set of another role, eliminating the need to define each permission in the set separately. This enables you to conveniently create a specialized group of users with the combined permissions of one or more groups and/or specific permissions.

Task

1. On the Permission page, select the Roles tab, then click Create New Role.

2. In the Name field, enter a name for the role.

3. In the Description field, enter a brief description of the new role.

4. (Optional) To use an existing system of defined users, select the LDAP checkbox. The LDAP server must be configured first on the System page. For details, see Configure LDAP.

   A drop-down list is displayed, listing all LDAP roles detected in the system.

   Select an LDAP role that matches an existing security group in the Active Directory and configure the permissions this LDAP role should have in the McAfee Database Security system.

   **Notes**

   - Please allow 60 seconds between the first configuration of the LDAP server and the definition of the LDAP roles.
   - To use more than one LDAP role, create separate roles for each LDAP security group.

5. Select the required permissions for the new role from the All Permissions list, then click to move them to the Selected permissions list.

   **Note**

   To remove permissions from the Selected permissions list, select the permissions, then click .

6. To include the permission set of an existing role in the new role, select the role in the All roles list, then click to move it to the Selected roles list.

   **Note**

   To remove a role from the Selected roles list, select the role, then click .

7. In the View Alert permissions by DBMSs area, select the DBMS groups and DBMSs for which the role is authorized to view alerts.

8. In the View Alert permissions by Rules area, select the rules for which the role is authorized to view alerts.

9. Click Save.
Edit the permissions of an existing role

You can change the permission set that is defined for an existing role. The new settings are automatically applied to users assigned the edited role.

To edit a role:

1. In the Roles tab, click the Properties icon in the row for the role to be edited. The properties of the selected role are displayed on the Role Properties page.

2. Edit the role permissions as required by moving specific permissions or roles to and from the Selected permissions list and Selected roles list, respectively, as required.

3. Click Save.

Remove a role

You can remove a role that is no longer needed.

Users assigned the removed role automatically lose the corresponding permissions set. If the user is assigned additional roles or specific permissions, those permissions are not affected.

Task

1. On the Roles tab, click in the row for the role you want to remove.

2. When prompted for confirmation, click OK.

The role is removed from the list.
Access to the McAfee Database Security Web Console is restricted to authorized users (administrators).

Users are assigned roles and or specific permissions, which define the ways in which they can use the system. For details on creating and defining roles, see Roles.

**Contents**
- Users list
- Managing users
- Configure password policy

### Users list

The Users tab of the Permissions page lists authorized users in the system, including these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The name of the user.</td>
</tr>
<tr>
<td>First Name</td>
<td>The first name of the user.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The last name (surname) of the user.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the user (active or inactive).</td>
</tr>
<tr>
<td>Properties</td>
<td>Enables you to view and edit the properties of the user, including the roles and permissions assigned to it.</td>
</tr>
<tr>
<td>Remove</td>
<td>Deletes the user. The system administrator cannot be deleted or deactivated, but you can change the administrator user name.</td>
</tr>
</tbody>
</table>

**Note**

You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see Filtering data.
Managing users

If you have the administrator permissions, you can add and remove users, and edit their details.

Tasks

- Add a user
- View user details
- Change a user’s permissions
- Change a user’s password
- Remove a user
- Export users
- Import users

Add a user

You can add authorized users to the system and define the ways in which they are allowed to use system.

You can assign more than one role to a user. In addition, you can assign specific permissions to a user.

Task

1. On the Permissions page, select the Users tab, then click Create New User.
2. In the User Name field, enter a user name for the user.
3. In the First Name field, enter the user’s first name.
4. In the Last Name field, enter the user’s surname (family name).
5. From the Status drop-down list, select the status to be assigned to the user (Active or Inactive).
6. Enter the user’s password in the Password field, then enter it again in the Confirm Password field.

   Note
   The password must contain at least four characters.

7. To apply the system’s password policy on this user’s password, select Enforce password policy.

   Note
   The password policy is configured on Password Policy tab of the Permissions page. For details, see Configure password policy.

8. To force the user to change the password the first time they log in, select Change password on next login.

9. To assign the permission set of an existing role to the new user, select the required role from the All Roles list, then click to move the role to the Selected Roles list.

   The permission sets of the selected roles are assigned to the user.

   Note
   To remove a role from the Selected Roles list, select the role, then click .
If one or more specific permissions are to be assigned to the user, select the required permissions from the All Permissions list, then click to move them to the Selected permissions list.

**Note**
To remove permissions from the Selected permissions list, select the permissions, then click .

In the Alert permissions area, select the DBMS groups and DBMSs for which the user is authorized to view alerts.

**View user details**
You can view the detailed properties of a user on the User Details page.

**To view the user details:**
- On the Users tab, click the Properties icon in the row for the user.

These details are displayed on the User Details page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The name of the user.</td>
</tr>
<tr>
<td>First Name</td>
<td>The first name of the user.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The last name (surname) of the user.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the user.</td>
</tr>
<tr>
<td>Selected permissions</td>
<td>The individual permissions assigned to the user.</td>
</tr>
<tr>
<td>Selected roles</td>
<td>The permission sets assigned to the user.</td>
</tr>
<tr>
<td>View Alert permissions</td>
<td>A list of the DBMSs and DBMS groups for which, if selected, the user is authorized to view alerts.</td>
</tr>
<tr>
<td>Default Login Page</td>
<td>The first page the user sees after logging in to the server.</td>
</tr>
</tbody>
</table>

**Change a user’s permissions**
You can change the permissions assigned an existing user by changing the roles or specific permissions assigned to the user.

**Task**
1. On the Permissions page, select the Users tab, then click the Properties icon in the row for the user to be edited.
2. Edit the user’s permissions as required by moving specific permissions or roles to and from the Selected permissions list and Selected roles list, respectively, as required.
3. Click Save.
Change a user’s password
You can change the password of an existing user, for example, if the user has forgotten the password.

**Task**

1. On the Permissions page, select the Users tab, then click the Properties icon in the row for the user to be edited.
2. On the User Details page, click Change Password.
3. Enter a new password in the New Password field, then enter it again in the Confirm Password field.

   **Note**
   The password must contain at least four characters.

4. Click OK. The password is changed.

Remove a user
You can remove a user from the Users list, thereby revoking all user’s permissions. A user that has been removed can no longer access the application or any of its functionalities.

**Task**

1. On the Permissions page, select the Users tab, then click in the row for the user you want to remove.
2. When prompted for confirmation, click OK.

   The user is removed from the list and is no longer authorized to access the application.

Export users
You can export the list of the McAfee Database Security users/administrators into an XML file, for example, to import them into another McAfee Database Security Server or as a backup before a system upgrade.

**Note**
This option is intended for advanced McAfee Database Security users only. It is available only to authorized users.

**Task**

1. On the Permissions page, select the Users tab, then Export Users.
2. You are prompted to indicate whether you want to open or save the file.
3. Click OK.

   The displayed users are exported to an XML file. (The location where the file is saved depends on your default settings.)
Import users
You can import a previously defined list of users.

Task
1. On the Permissions page, select the Users tab, then click Import Users.
2. Select the previously saved file (.XML), then click Import.

The users contained in the file are added to the Users list.

Configure password policy
You can configure the password requirements that apply to the user passwords.

The default password policy requires that a user password include at least one uppercase letter, at least one lowercase letter, and at least one digit or special character.

Note
The default password policy is defined in the server-custom.properties file.

Task
1. On the Permissions page, select the Password Policy tab.
2. To enforce the use of special characters in user passwords, select Yes from the Enforce special characters drop-down list.
3. From the Password minimum length drop-down list, select the minimum number of characters to be included in a password.
4. To force users to change their passwords at regular intervals, from the Enforce password change every drop-down list, set how often users must change their passwords. From the New password minimum lifetime drop-down list, select the minimum time after which users are prompted to change their passwords.
5. To prevent users from resetting their passwords to previously used passwords, select the time period during which users cannot reuse a past password from the Prevent password repetition drop-down
6. To prevent brute force attacks, select Yes from the Prevent brute force attack drop-down list to temporarily block login attempts from an IP address following repeated failed attempts to log in from the same IP address.
7. To lockout a user after multiple failed login attempts, select the number of failed logins after which the user is locked out of the system from the Lockout after failed logins drop-down list. Then, from the adjacent drop-down list, set the duration of the lockout period (for example, 1 day).
8. Click Save.
The System page provides several system functions, including interface configuration, custom rule groups, resolve types, and a history of actions taken by users in the graphical user interface.

Contents
- Configuring system interfaces
- Alert archiving
- Quarantining users
- Viewing clusters
- Viewing action history
- Configuring and downloading server logs
- Viewing system messages
- View backend DBMS details

Configuring system interfaces
You can configure the system interfaces, including email, LDAP, logs, VPN blocking, and more.

Tasks
- Configure the outgoing e-mail account
- Configure LDAP
- Configure SNMP
- Configure the Syslog
- Configure the Windows event log
- Configure log to file
- Configure VPN-1 blocking
- Configure the XML API
- Configure the Analytics Module

Configure the outgoing e-mail account
The outgoing e-mail settings defined in the Email tab determine the mailbox that is used by McAfee Database Security to send notifications, alerts, and traps.

Task
1. On the System page, select the Interfaces tab, then select Email.

2. Configure these email parameters:
   - From — The name of the sender to appear in outgoing email messages.
   - From address — The email address to be used for outgoing messages.
Configuring system interfaces

- **Mail Server** — The IP address or name of the host server.
- **Port** — The port used for email communications.
- **Max emails for period** — The maximum number of outgoing email messages allowed for the interval set as in the **Period of time** field.
- **Period** — The interval in milliseconds used to measure the rate of outgoing email messages, as set in the **Max emails for period** field.
- **Subject** — Text that automatically appears in the Subject field of outgoing email messages.
- **To** — The destination of outgoing email messages (single user or semicolon delimited list).
- **Template** — The template used for generating outgoing email messages.

3. Click **Save**.

**Configure LDAP**

Configuring LDAP in McAfee Database Security enables you to use existing security groups in the Active Directory, eliminating the need to set up your users and roles from scratch.

**Task**

1. On the **System** page, select the **Interfaces** tab, then select **LDAP**.
2. Select **Use LDAP** to enable McAfee Database Security to use LDAP.
3. Configure the LDAP parameters as follows:
   - **Base** — The Base distinguished name of the LDAP directory.
   - **Domain** — The domain of the Active Directory.
   - **Root Path (Optional)** — The fully qualified name of the entry to be used as the root path instead of the LDAP directory root.
   - **URL** — The URL of the Active Directory.
   - **Username** — The name of the user authorized to access the LDAP directory.
   - **Password** — The password of the user authorized to access the LDAP directory.

4. Click **Save**.

Once you have finished configuring the LDAP settings, you can configure McAfee Database Security roles based on your LDAP Roles. For more information, see *Create a new role*.

**Configure multiple LDAP servers**

Multiple-LDAP functionality enables you to configure additional LDAP servers and retrieve rule object values from other LDAP servers. Additional LDAP servers are configured in the custom properties file, with this structure and content:

```plaintext
multi.ldap.<N>.name=<LDAP server name>
multi.ldap.<N>.rootPath=<LDAP server root path>
multi.ldap.<N>.base=<LDAP server base>
multi.ldap.<N>.domain=<LDAP server domain name>
multi.ldap.<N>.username=<Username to connect to LDAP server2>
```
System
Configuring system interfaces

multi.ldap.<N>.password=<Encrypted password3>
multi.ldap.<N>.url=<LDAP server URL>

Where N stands for a plain number in a running sequence of numbers.

After configuring the LDAP servers, the Database Security management server must be restarted.

The configured servers appear in the LDAP configuration interface (System | Interfaces | LDAP).

When you configure the LDAP server credentials, the LDAP server password is encrypted using the Migration Tool. Run migration_tool.bat (located in the bin directory), then follow the on-screen instructions.

**Note** This configuration allows using the additional LDAP servers only as rule object data sources. You can log on to the Database Server management servers with an AD user using only the primary configured LDAP server (the server configured on the interface System | Interfaces | LDAP page).

Once additional LDAP servers are configured, rule object values can be populated using those servers. To reference a group in an additional LDAP server, the fully qualifying name of the group is required (groups from the primary LDAP server can still be addressed using the short names).

Auto-complete is available for both the primary LDAP server and other configured servers.

**Configure SNMP**

You can configure McAfee Database Security to use SNMP for internal communication and to send traps to third-party applications.

**Task**

1. On the System page, select the Interfaces tab, then select SNMP.
2. To enable McAfee Database Security to use SNMP for internal communications, select Use SNMP and configure the SNMP parameters as follows:
   - Port — The port for SNMP communications.
   - Community — The SNMP communication string.
3. To view the MIB file in an external browser (as a TXT file), click Open MIB file.
   The MIB file is displayed in an external file in read-only format. (Close the file to continue with the configuration process.)
4. To use SNMP to send traps to a third-party application, select Use SNMP Trap and configure the SNMP trap parameters as follows:
   - Port — The port for SNMP communications.
   - Host — The IP address of the host where the third-party application resides.
   - Community — The SNMP communication string.
5. Click Save.
Configure the Syslog
You can configure McAfee Database Security to use the syslogs to monitor alerts.

Task
1. On the System page, select the Interfaces tab, then select Syslog.
2. Select Use Syslog.
3. Configure these parameters:
   - **Host** — The IP address of the host where the syslog resides.
   - **Port** — The port for syslog communications.
   - **Facilities** — The syslog facilities.
   - **Format** — The file type to be used for the syslog (CSV, Sentinel or Custom).
4. Click Save.

The Syslog is configured and enabled.

Configure a proprietary alert format
Database Security is provided with the CEF format configured by default.

The proprietary alert format can be configured in the properties file.

**To configure a proprietary alert format:**
1. On the server machine, go to `<install dir>/conf`.
2. Open the `server-custom.properties` file and modify it as required.
3. Save the file.
4. Restart the server.
   - If the custom format is selected on the Syslog Configuration page, the respective file configuration is displayed.

Syslog fields directory
The syslog custom configuration can be edited in the `<Database Security install dir>/conf/server-custom.properties` file.

The following files need to be copied into this file from the `<install dir>/webapps/ROOT/WEB-INF/config/application/server.properties` file. (You can view this file to see how CEF and Sentinel is configured).

**Important**
Do not modify the `server.properties` file. All changes should be made in the `server-custom.properties` file.

Verify that all changes comply with the CEF protocol:
- The header should have pipe (|) delimited fields
- The body should have space delimited 'key=value' format.

```
log.format.body.custom=externalId=$id$ rt=$executionTime.time$
csl1=$database.name:20$ csl1Label=DBMS dst=$agent.ip$ src=$sourceIP$
```
Configuring system interfaces

You can then modify `log.format.body.custom` to fit your format. The format is very flexible. Each keyword identified by `$<key word>` is replaced with its value from the alert. It is also possible to specify a max length for the field, for example:

$agent.hostname:20$

If the length is not specified, the value of `log.format.length.value.custom` is used.

The following keywords can be used to define the format:

- `$clientInfo$` — Client info field from Oracle database (string, max. 100).
- `$executionTimeMillis$` — Execution time in millis format (number, 64-bit).
- `$executionTimeStr$` — Execution time in date format: dd MMM yyyy HH:mm:ss (string, max. 32).
- `$severity$` — Severity of the alert (High, Medium, Low) (string, max. 20).
- `$agent.hostname$` — Hostname of the sensor the alert was received from (string, max. 255).
- `$operation$` — Statement executed (string, unlimited).
- `$osUser$` — OS user (string, max. 100).
- `$execUser$` — Database user (string, max. 100).
- `$realExecUser$` — Real database user (string, max. 100).
- `$serial$` — Oracle session serial (number, 64-bit).
- `$sid$` — Session ID (number, 64-bit).
- `$terminal$` — Terminal (string, max. 100).
- `$execProgram$` — Executing program (string, max. 100).
- `$sourceHost$` — Source host (string, max. 255).
- `$sourceIP$` — Source IP address (string, max. 16).
- `$databaseName$` — Database name (string, max. 255).
Configure the Windows event log
You can configure McAfee Database Security to use the Windows event log to monitor alerts.

**Note**

Windows Event Log is supported on Windows XP and up, and on Windows Server 2003 and up.

**Task**

1. On the **System** page, select the **Interfaces** tab, then select **Windows Log**.
2. Select **Use Windows Event Log**, then configure these parameters:
   - **Host** — The IP address of the host where the Windows Event Log resides.
   - **Format** — The file type used for the Windows Event Log (CSV, CEF, Sentinel or Custom).
3. Click **Save**.
Configure log to file
You can configure McAfee Database Security to save log entries in a file.

**Task**
1. On the System page, select the Interfaces tab, then select Log to File.
2. Select the Log to File option, then configure these parameters:
   - **Directory Path** — The full path to the location of the log file.
   - **Rolling Period** — The time period covered by each log (hourly or daily).
   - **Delete Older Than** — The number of days after which the log file should be deleted.
   - **Format** — The file type of the log file (CSV, CEF, Sentinel, or Custom).
3. Click Save.

Configure VPN-1 blocking
OPSEC Suspicious Activity Monitoring (SAM) enables VPN-1/FireWall-1 to block a connection when suspicious activity is identified on the network or specific host, or as the result of the matching of a rule in the system.

To implement OPSEC SAM, you need to define the SAM server and the SSCLA mode.

**Task**
1. On the System page, select the Interfaces tab, then select OPSEC SAM.
2. To define the SAM server properties:
   - Select the SAM Server Properties checkbox.
   - Enter the SAM server's IP address and port number in the designated fields.
   - Select the log to be used for storing SAM alerts from the Log drop-down list.
3. To transmit without encryption, select Clear mode (no encryption).
4. To define SSLCA mode:
   - Enter the path to the OPSEC certificate in the Certificate Path field.
   - Enter the path to the Client SIC in the Client Sic field.
   - Enter the path to the Server SIC in the Server Sic field.
5. Click Save.

**Note**
You can use the Check Point pull_cert utility to retrieve the OPSEC certificate. Enter this command in the command line tool:
```
opsec_pull_cert.exe - h <name of host where file is located> -n <checkpoint object name> - p <password for object>
```
This creates the opsec.p12 certificate file.
Configure the XML API

The XML agent enables you to import and export XML files.

For further information about the XML API, see McAfee KnowledgeBase article KB72411.

Task

1. On the System page, select the Interfaces tab, then select XML API.
2. Select XML API enabled.
3. Click Save.

The XML agent is enabled. You can now use the XML API. (For details, see XML API.)

Note

To view the DTD or XSD files, click the respective link. The file opens in an external window.

Configure the Analytics Module

The McAfee® Database Security – Analytics Module provides users with the ability to collect and analyze large amounts of data, as well as visualization capabilities and data-exploration interfaces. For details, see McAfee Database Security – Analytics Module Product Guide.

Use of the Analytics Module requires that you configure the Database Security Server to export Alerts and VA Results to the server where the Analytics Module is installed.

Task

1. On the System page, select the Interfaces tab, then select Analytics Module.
2. Select Use Analytics Module.
3. Enter the IP address/hostname and port number of the server where the Analytics Module is installed in the designated fields.

Note

When the Analytics Module is used, a default user (sngimport) is created and the user name and password fields are automatically populated. If you have manually changed the password on the Analytics Module server, you must also set that password in the Password field.

4. In the Transfer Interval field, set how often to send the data (in milliseconds). The minimum value is 30,000 milliseconds (30 seconds).

5. Select one or more types of alerts to export:
   - Export Alerts (Database Security events)
   - Export VA Results (Database Security findings)
Alert archiving

To facilitate the viewing of alerts and reduce the overall size of the alerts list, McAfee Database Security enables you to automatically or manually archive alerts.

You can also unarchive existing archives to view the alerts that they contain, or you can remove alert archives that are no longer required. Existing archives are listed in the Archives tab of the System page.

Tasks
- Configure automatic alert archiving
- Configure manual alert archiving
- Reload a whole archive
- Rearchive alerts
- Remove an alert archive

Configure automatic alert archiving

You can configure McAfee Database Security to automatically archive alerts in a specific location and at preset intervals.

Task
1. On the System page, select the Archives tab, then select Settings.
2. In the Archive Folder Path field, set the location where the archived files are to be stored.

Note
By default, Auto archive by number of alerts is enabled and alerts are archived when the number of alerts exceeds 10,000 (by default the 30,000 oldest alerts are archived).

3. To disable automatic archiving (not recommended), deselect the Auto Archive Enabled checkbox.

4. Schedule the archiving process as follows:
   - To schedule archiving at hourly intervals, select by hours, then set the interval in the adjacent field. For example, every two hours.
   - To schedule daily archiving, select by day, then select the day of the week when archiving is to take place.
   - To schedule monthly archiving, select by month, then and set the frequency (per number of months) in the adjacent field.
5  Set the age of alerts to be archived in the *Archive Alerts older than* fields, by setting both the number and time unit (days, weeks, months).

6  Click *Save*.

**Configure manual alert archiving**
You can manually initiate the archiving process at any time.

**Task**

1  On the *System* page, select the *Archives* tab, then select *Settings*.

2  Set the age of alerts to be archived in the *Archive Alerts older than* fields, by setting both the number and time unit (days, weeks, months).

3  Click *Archive Now*.

All alerts older than the set age are archived.

**Reload a whole archive**
You can access the alerts that are contained in an alerts archive by unarchiving the archive file.

**Task**

1  On the *System* page, select the *Archives* tab, then select *Archive History*.

2  In the *Archives* list, click *Unarchive* in the row for the action. The *Alerts* page is displayed, and the *Archives* drop-down list is available for selection in the *Filter* area.

3  To view the alerts for a specific archive, select the archive file from the *Archives* drop-down list, then click *Apply*.

**Reload partial archives**
You can filter the alerts that are contained in an alerts archive and unarchive only the data that meets specific criteria.

**Task**

1  On the *System* page, select the *Archives* tab, then select *Archive History*.

2  Expand the *Archive Load Filter* area.

3  From the *Archive Type* drop-down list, select the type of archive.

4  From the *Filter by* drop-down list, select *Execution Time*, then click *Add*.

5  Set additional filter properties as required, then click *Upload* to load the data that meets the filter criteria.
**System**

**Quarantining users**

---

**Rearchive alerts**

You can remove reloaded alerts from the Alerts page by rearchiving them.

**Task**

1. On the System page, select the Archives tab, then select Archive History.
2. In the Archives list, click Rearchive in the row for the action.

   The Archives drop-down list is no longer available for selection on the Alerts page.

**Note**

To maintain alert integrity, rearchiving simply removes the unarchived alerts from the alerts screen. The archive remains untouched (any actions performed on the unarchived alerts will not be kept).

**Remove an alert archive**

To conserve space, archives that are no longer relevant can be removed from the server.

**Before you begin**

The removal of an archive might not be permitted under company or legal regulations. Check your organization’s security policy before trying to remove an archive.

**Task**

1. On System page, select the Archives tab, then select Archive History.
2. In the Archives list, click in the row for the archive you want to delete.
3. When prompted for confirmation, click OK.

   The archive is deleted.

---

**Quarantining users**

If a rule action is set to Terminate and the Quarantine option is selected, a user can be placed in quarantine for a predefined number of minutes. While in quarantine, the user is unable to reconnect to the DBMSs for which the rule was triggered.

The Quarantine tab lists these parameters for users currently in quarantine:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine parameters</td>
<td>The parameters according to which the user was quarantined (for example, IP address, OS user, or application).</td>
</tr>
<tr>
<td>Start time</td>
<td>The time when the quarantine of the user began.</td>
</tr>
<tr>
<td>DBMS</td>
<td>The DBMS that the user tried to access.</td>
</tr>
<tr>
<td>Rule</td>
<td>The rule that triggered the quarantine action.</td>
</tr>
</tbody>
</table>
### Viewing clusters

The **Clusters** tab is used when the McAfee Database Security Server is deployed in cluster mode. It displays view-only information regarding the servers, including the sensors installed on each server. It is intended for use by McAfee Database Activity Monitoring users only.

For cluster configuration instructions, contact McAfee support.

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unquarantine</td>
<td>A link, which when clicked, enables you to remove the user from quarantine.</td>
</tr>
</tbody>
</table>

### Tasks

- **Configure the quarantine parameters**
- **Configure the quarantine parameters**
- **Remove a user from quarantine**

#### Configure the quarantine parameters

You can determine the parameters according to which users are placed in quarantine. It is advisable to first review your current alerts before deciding on the best way to identify a user in your network. The best option is when one parameter is always unique in your network (for example, terminal is unique in some networks, however it is not used in others).

**Task**

1. On the **System** page, select the **Quarantine** tab, then select **Settings**.

2. Select or deselect the checkboxes for the parameters that define when a user can be quarantined.

   The system applies the operator "and" to the selected parameters. For example, if you choose user and IP address, when triggered by a rule, the system checks the user name and the IP address (for example, scott and 192.168.7.7) and denies access to any subsequent SQL statements that comes from 192.168.7.7 and the user scott. Statements coming from 192.168.7.7 where the user is jerry are allowed.

3. Click **Save**.

#### Remove a user from quarantine

You can remove a user from quarantine so that they can access the DBMS.

**Task**

1. On the **System** page, select the **Quarantine** tab, then select **Quarantine list**.

2. In the **Quarantine** list, click **Unquarantine** in the row for the user.

3. Enter the reason for removing the user from quarantine, then click **Unquarantine**.

   The user is removed from both the quarantine and the **Quarantine** list, and is again able to access the DBMS.
Viewing action history

The History tab lists these parameters for actions taken in the system.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>The type of action taken (for example, Modify User Rule, Resolve Alert, Approve Sensor, or Change Role).</td>
</tr>
<tr>
<td>Modified by</td>
<td>The name of user who performed the action.</td>
</tr>
<tr>
<td>Modify date</td>
<td>The date and time of the action.</td>
</tr>
<tr>
<td>Properties</td>
<td>An icon, which when clicked, enables you to view the details of the action.</td>
</tr>
</tbody>
</table>

**Note**

You can filter this list according to specific criteria. For details about defining, saving, and applying filters, see *Filtering data*.

**Tasks**

- Set the time period for saving actions history
- View actions history details

**Set the time period for saving actions history**

You can set the amount of time after which actions are automatically deleted from the Actions History list.

**Task**

1. On the History tab, select the Delete actions older than checkbox and, in the adjacent field, enter the number of days after which to delete actions.
2. Click Save.

**View actions history details**

You can view the details of an action in the Actions History list.

**Task**

- In the Actions History list, click the Properties icon in the row for the action. The properties page is displayed for the selected rule.
Configuring and downloading server logs

The Troubleshooting tab is used to configure the server logs and download the server log files to send to McAfee support when required. It is also used to configure automatic IP address resolution.

Tasks
- Configure the server logs
- Download the server logs
- Configure automatic resolution of IP addresses

Configure the server logs

You can determine the types of server logs created as well as the maximum size of the log file.

Task
1. When instructed to do so by McAfee support, on the System page, select the Troubleshooting tab.
2. From the Log Level drop-down list, select the type of logs to be created (by default the log level is set to INFO).
3. In the Log file size field, set the maximum size of the log file (in MB).
4. Click Save.

Download the server logs

You can download and view the server logs files for troubleshooting purposes. You can also send these server log files to the McAfee support.

Task
1. On the Troubleshooting tab of the System page, click the Download Logs link. A dialog is displayed, prompting you to indicate whether you want to open or save the file.
2. Select Save to Disk, then click OK. The server logs are exported to an XML file. (The location where the file is saved depends on your default settings.)

Configure automatic resolution of IP addresses

You configure the automatic resolution of IP addresses on the Troubleshooting tab.

Task
1. On the System page, select the Troubleshooting tab, then select Resolve IP from Host for Alert.

   Note
   By default, this feature is enabled (selected). Disabling of this feature is only needed in cases of severe network load.
2. Click Save.
Viewing system messages

The Messages tab of the System page lists the system messages generated by the system in response to various conditions and events in the system, for example, when a sensor stops communicating with the server or when a license is about to expire.

If there are high severity messages, an icon appears at the top of each page indicating the number of unread high severity messages. Click the icon to view the messages.

Unread messages appear in bold type; read messages appear in regular type.

The Messages tab lists these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>The level of severity (Low, Medium, or High).</td>
</tr>
<tr>
<td>Subject</td>
<td>The subject of the message.</td>
</tr>
<tr>
<td>Body</td>
<td>The text content of the message.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>The date and time when the message was created.</td>
</tr>
<tr>
<td>Properties</td>
<td>An icon, which when clicked, enables you to view and edit the message properties.</td>
</tr>
<tr>
<td>Delete</td>
<td>An icon, which when clicked, removes the message from the System Messages list.</td>
</tr>
</tbody>
</table>

**Note**
You can filter this according to specific criteria. For details about defining, saving, and applying filters, see Filtering data.

**Tasks**
- View system message details
- Mark system messages as read or unread
- Delete a system message
- Configure system messages

View system message details

You can view the detailed properties of a message on the Message Details page.

**Task**
1. On the System page, select the Messages tab, then click the Properties icon in the message row.

   **Tip**
   To view the message details of the next message in the list, click Next Message. To view the message details of the previous message in the list, click Previous Message.

2. (Optional) To stop receiving this type of message, click the Click here to stop receiving link.
Mark system messages as read or unread
You can mark all messages as read or unread in the Messages list.

Task
- On the System page, select the Messages tab, then click Mark all as Read or click Mark all as Unread as required.

Delete a system message
If, after viewing a system message, the message is no longer relevant you can delete it from the Messages list.

Task
1. On the System page, select the Messages tab, then click [X] in the row for the message you want to delete.
2. When prompted for confirmation, click OK.
The message is removed from the list.

Configure system messages
You can configure whether alerts are generated for all system messages and/or when sensors are disconnected. You can also specify an email address destination for system messages.

Task
1. On the System page, select the Messages tab, click Message, then click Configuration.
2. To configure the system to send email messages to an email address based on the severity of the system message, enter the email address in the Send email to field, then select the severity level (Low, Normal, or High) from the drop-down list.
3. To receive alerts indicating when a sensor is disconnected, select Alert when sensor is disconnected. If you select this option, set the number of seconds to wait before considering the sensor to be disconnected and generating the alert. (The default value is 60 seconds.)
4. To receive an alert when the number of vPatch alerts in a specific time period exceeds a specific level, select Alert when server received over. If you select this option, set the number of alerts and the time period accordingly.
5. Click Save.
View backend DBMS details

You can view basic information about the backend database on the Backend DBMS tab of the System page.

The read-only DBMS details vary according to database type (HSQLDB, Oracle or MS SQL).

Task

- On the System page, click Backend DBMS to display the Backend DBMS tab.

These details are displayed for each backend DBMS.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of database (HSQLDB, Oracle or MS SQL). Note: The use of HSQLDB databases is not recommended in production environments.</td>
</tr>
<tr>
<td>Size Details</td>
<td>The file name/table space, current size, maximum size, and amount of free space. If the system is unable to detect the maximum size, it is recommended that you verify that enough space is available on the DBMS.</td>
</tr>
</tbody>
</table>

These additional details are displayed for Oracle and MS SQL databases.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The name of the database user.</td>
</tr>
<tr>
<td>IP/Host</td>
<td>The IP address or name of the host where the DBMS is located.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used to communicate with the DBMS.</td>
</tr>
</tbody>
</table>

Updates

The Updates page comprises these tabs:

- vPatch Security Updates — Enables you to manually check for and install vPatch security updates, and displays the history of previously installed updates.
- VA Security Updates — Enables you to manually check for and install VA security updates, and displays the history of previously installed updates.
- Software Updates — Enables you to manually check for and install server and sensor software updates, and displays the history of previously installed updates.
- Security Update Settings — Enables you to configure the policy for performing security updates.

Tasks

- Configure security update settings
- Manually check for/install vpatch security updates
- Manually check for and install server software updates
Configure security update settings

vPatch rules and VA tests are provided by McAfee Database Security to help monitor and prevent attacks against known vulnerabilities and to scan databases for security issues, respectively. You can determine whether these rules/tests are automatically updated, and when the automatic security updates are to take place.

**Task**

1. On the **Update** page, select the **Update Settings** tab.
2. To automatically check for all updates, select **Check for available updates automatically**.
3. Select the required auto-installation option as follows:
   - To disable the automatic installation feature, select **No auto-installation**.
   - To perform the update in real-time, select **Real-time** (auto-install when new updates are available).
   - To install updates on a specific day and time, select **Schedule installation**, then select the day of the week and indicate the time when the update is to begin.
4. Click **Save**.

Manually check for/install vPatch security updates

You can manually check for updates and/or install vPatch security updates.

**Task**

1. On the **Update** page, select the **vPatch Security Updates** tab.
2. Click **Check for new updates**.
   A list of available updates is displayed. If no updates are available, a message is displayed accordingly.
3. To install an update, select the update, then click **Install**.
   The **Security Update** dialog is displayed, indicating the version to be installed and listing the changes that are included in the new version.
4. Click **Install**.

**Note**

If you try to install a version that is older than the currently installed version, you are prompted to confirm that you really want to do so.
Manually check for/install VA security updates
You can manually check for updates and/or install VA security updates.

**Task**

1. On the **Update** page, select the **VA Security Updates** tab.
   The currently installed version is indicated in the **VA Security Updates** tab.

2. Click **Check for new updates**.
   A list of available updates is displayed. If no updates are available, a message is displayed accordingly.

3. To install an update, select the update, then click **Install**.
   The **Security Update** dialog box is displayed, indicating the version to be installed and listing the changes that are included in the new version.

4. Click **Install**.

   **Note**
   If you try to install a version that is older than the currently installed version, you are prompted to confirm that you really want to do so.

Manually check for and install server software updates
You can manually check for updates and/or install server software updates.

**Task**

1. On the **Update** page, select the **Software Updates** tab.

2. Click **Check for new releases**.
   A list of available updates is displayed.

   **Note**
   If no updates are available, a message is displayed accordingly.

3. To install an update, select the update, then click **Install**.

4. To install an update from a local file (offline installation):
   - Click **Browse** to locate and select the installation file.
   - Click **Upload**. The **Security Update** dialog is displayed, indicating the version to be installed and listing the changes that are included in the new version.
   - Click **Install**.

Manually check for/install sensor software updates
You can manually check for updates and install sensor software updates.

**Task**

1. On the **Update** page, select the **Software Updates** tab.

2. Click **Check for new sensor updates**.
A list of available updates is displayed for each platform. To install an update, select the update, then click Manual Install. If no updates are available, a message is displayed accordingly.

**Install offline updates**

You can install security updates and software updates from a file that you have downloaded or have received from McAfee support personnel.

**Task**

1. On the Update page, select the Security Updates, Server Updates, or Software Updates tab (as applicable).
2. Click the Upload an update file link.
3. Select the file (with a file extension.SUP) that you want to upload.
4. Click OK to upload the file.

**View the update history**

You can view a history of the previously installed security updates, server updates, or sensor updates, including both automatic and manual updates.

**Task**

- On the Update page, select the Security Updates, Server Updates, or Software Updates tab. A history of the updates is listed in the Updates History area, indicating the version, when installed and by whom, and installation mode (automatic or manual).

---

**Reports**

If you are using McAfee Database Activity Monitoring, you can generate a wide range of reports. By default, McAfee Database Security reports are displayed in HTML format in an external browser window. Alternatively, you can generate reports in DOC, PDF, RTF, XML or Excel formats.

You can generate System Reports or Dynamic Reports.

**Generating system reports**

These reports are currently available on System Reports tab of the Reports page:

- Alerts Per DBMS
- Most Critical Alerts
- Alerts per Rules
- Alerts per Tags
- All Rules
- Custom Rules
- vPatch Rules
- Inactive Rules
- Rules per DBMS
- Sensor Drill Down
- DBMS Drill Down
- Top Critical Alerts per single DBMS
- Top Critical Alerts per multiple DBMS
- History Actions
- Alerts per Compliance

**Task**

1. On the **Reports** page, select the **System Reports** tab, then click the icon in the Run column in the row for the required category of report.

2. Set the report criteria.

3. (Optional) Enter a brief description or comment in the Comments field. The comment is displayed at the top of the report.

4. (Optional) To generate the report as a PDF, select **PDF view**.

   **Note** By default, the report is generated in HTML format in an external browser window.

5. Click **OK**. The report is generated and displayed.

**Working with dynamic reports**

You can create multiple dynamic reports for alerts, test results, or system objects. For each report, you define one or more filters that determine which alerts, results, or objects are included in the dynamic report.

Dynamic reports can present data in summary or detailed formats. The dynamic report options are available in the Dynamic Alert Reports, Dynamic Result Reports, and Dynamic System Reports tabs of the Report page.

The Dynamic Alert Reports and Dynamic Result Reports tabs of the Reports page list the configured dynamic reports, including these parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Name</td>
<td>The name of the report (defined in the creation process).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the report (defined in the creation process).</td>
</tr>
<tr>
<td>Scheduling</td>
<td>A clock icon is displayed if scheduling is enabled for the report.</td>
</tr>
<tr>
<td>Actions</td>
<td>Icons for the available actions:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Properties" /> — Enables you to view and edit the properties of the Dynamic Report.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Run" /> — Enables to run the Dynamic Report.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Remove" /> — Enables you to delete the Dynamic Report definition.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Download" /> — Enables you to download a report.</td>
</tr>
</tbody>
</table>
Tasks

- Create a detailed dynamic report
- Create a summary dynamic report
- Schedule a dynamic report
- Run a dynamic report
- Delete a dynamic report

Create a detailed dynamic report
You can create dynamic reports for alerts or for test results. The dynamic report options are available in the Dynamic Alert Reports and Dynamic Result Reports tab of the Report page.

You can create multiple dynamic reports to meet the needs of your organization. For each report, you define one or more filters that determine which alerts or results are included in the dynamic report.

If you produce the report as a PDF or Microsoft Excel file, you can configure the report to run automatically at scheduled intervals and be sent as an email attachment.

Task

1. Select the Dynamic Alert Reports tab, the Dynamic Result Reports tab or the Dynamic System Report tab according to the required dynamic report type.

2. Click New Report.

3. In the Name field, enter a name for the dynamic report. It is recommended that the name selected reflect the nature of the report.

4. In the Description field, enter a brief description of the dynamic report.

5. From the Report type drop-down list, select Detailed.

6. In the Filter by area, set the filters to be applied to the report:
   - To define a filter, select the required criteria from the Filter by drop-down lists, then click Add. The filter is added to the Selected Filter Fields table.
   - To remove a filter from the Selected Filter Fields table, click Remove in the corresponding row.
   - To filter the report to include only data from the most recent scan, select Last Run Results. (This option is available for Dynamic VA result reports only.)

7. To set the report format, select the format type from the Report Format drop-down list.

8. From the Group by drop-down list, select the criteria for grouping data in the report (Level, DBMS, sensor or rule).

9. Set the criteria for sorting data:
   - To sort by a specific parameter in ascending order, select the parameter in the Table Column list, then click \[\text{A-Z}\] to move it to the Sort by list.
   - To sort by a specific parameter in descending order, select the parameter in the Table Column list, then click \[\text{Z-A}\] to move it to the Sort by list.
   - To remove a parameter from the Sort by list, select the parameter, then click \[\text{\rightarrow}\] to move it to the Table Column list.
The data is sorted by selected criteria in the order in which they appear in the Sort By list. Select a parameter, then click ⬅️ or ➡️ to reposition it in the Sort By list.

10 Set the fields to be displayed in the report:

- To exclude a field from the report, select the parameter in the Selected Report Fields list, then click ⬅️ to move it to the Available Report Fields list.
- To include a field in the report, select the parameter in the Available Report Fields, then click ➡️ to move it to the Selected Report Fields list.

11 To run the report based on a schedule (available only in Excel and PDF report formats), select Schedule Enabled and configure these parameters:

- From the drop-down list, select the interval at which you want the report to be run, by hours, by day, or by month, and set the relevant frequency.
- In the Start Time field, set the time of day to run the report.

12 Configure the report notification settings:

- If you want to send a notification when the report is ready, enter the email address in the Send notification by email to field.
- If you want the report to be sent as an attachment to an email message, enter the email address in the Send notification by email to field, then select Attach report.

13 Click Save to save the report without running it or click Run to generate the report.

Create a summary dynamic report

A summary dynamic report displays key report data in a bar or pie chart, accompanied by a table with the corresponding data. Summary reports can be generated in HTML, DOC, PDF, RTF or XML format.

Unless you choose the HTML format, you can configure the report to run automatically at scheduled intervals and be sent as an email attachment.

Note: Microsoft Excel format is available for detailed reports only.

Task

1 On the Reports page, select the Dynamic Alert Reports tab, the Dynamic Result Reports tab, or the Dynamic System Report tab according to the required dynamic report type.

2 Click New Report. The dynamic report properties form is displayed.

3 In the Name field, enter a name for the dynamic report. It is recommended that the name selected reflect the nature of the report.

4 In the Description field, enter a brief description of the dynamic report.

5 From the Report type drop-down list, select Summary.

6 In the Filter by area, set the filters to be applied to the report:

- To define a filter, select the required criteria from the Filter by drop-down lists, then click Add. The filter is added to the Selected Filter Fields table.
To remove a filter from the Selected Filter Fields table, click Remove in the corresponding row.

7 From the Report Format drop-down list, select the format in which the report is to be generated.

8 From the Graph type drop-down list, select the type of graphic used to display the data summary (Bar, Multi-Bar, or Pie).

**Note**
A multi-bar graph stacks data based on two different variables. For example, you can create a multi-bar graph that groups the data according to both DBMS and severity levels to view the distribution of alerts across the databases. If Multi-Bar is selected, you must define the properties assigned to the two axes.

9 From the Group by drop-down list, select the criteria for grouping data in the report (Level, DBMS, sensor or rule).

10 To run the report based on a schedule (available only in Excel and PDF report formats), select Schedule Enabled, then configure these parameters:
   - Select the interval at which you want the report to be run, by hours, by day, or by month, and set the relevant frequency.
   - In the Start Time field, set the time of day to run the report.

11 Configure the report notification settings as follows:
   - If you want to send a notification when the report is ready, enter the email address in the Send notification by email to field.
   - If you want the report to be sent as an attachment to an email message, enter the email address in the Send notification by email to field, then select Attach report.

12 Click Save to save the report without running it, or click Run to generate the report.

**View/edit the properties of a dynamic report**
You can view/edit the properties of a dynamic report on the Dynamic Alert Reports tab, the Dynamic Result Reports tab, or the Dynamic System Report tab according to the required dynamic report type (alerts or results).

**Task**

1 In the Dynamic Reports list, click in the row for the report. The properties of the dynamic report are displayed on the Dynamic Reports tab.

2 Change the report properties as required.

3 Click Save.

**Schedule a dynamic report**
You can schedule a dynamic report to run at a specific time.

**Note**
This report is available only in Excel and PDF formats.
Task

1. In the Dynamic Reports list, click in the row for the report. The properties of the dynamic report are displayed in the Dynamic Reports tab.

2. Select Schedule Enabled and configure these parameters:
   - Select the interval at which you want the report to be run, by hours, by day, or by month, and set the relevant frequency.
   - In the Start Time field, set the time of day to run the report.
   - Set the email address to receive the report output file. You need to configure the email server on the System tab first.

3. Click Save.

The report definition is updated to include the new schedule settings. The scheduled report output is saved in the McAfee Database Security Server machine to the path specified in the properties file `<Server_root>\webapps\ROOT\WEB-INF\config\reports\britConfig.properties` in the server.reports.xlsDirectory property, which is by default located in the `<Server_root>\webapps\ROOT\export\` folder.

Advanced scheduling is based on cron syntax.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Mandatory</th>
<th>Allowed Values</th>
<th>Allowed Special Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds</td>
<td>YES</td>
<td>0-59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Minutes</td>
<td>YES</td>
<td>0-59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Hours</td>
<td>YES</td>
<td>0-23</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of month</td>
<td>YES</td>
<td>1-31</td>
<td>, - * ? / L W</td>
</tr>
<tr>
<td>Month</td>
<td>YES</td>
<td>1-12 or JAN-DEC</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of week</td>
<td>YES</td>
<td>1-7 or SUN-SAT</td>
<td>, - * ? / L #</td>
</tr>
<tr>
<td>Year</td>
<td>NO</td>
<td>empty, 1970-2099</td>
<td>, - * /</td>
</tr>
</tbody>
</table>

Examples of advanced scheduling:

<table>
<thead>
<tr>
<th>Expression</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 12 * * ?</td>
<td>Run at 12 pm (noon) every day</td>
</tr>
<tr>
<td>0 15 10 ? * *</td>
<td>Run at 10:15 am every day</td>
</tr>
<tr>
<td>0 15 10 * * ?</td>
<td>Run at 10:15 am every day</td>
</tr>
<tr>
<td>0 15 10 * * ? *</td>
<td>Run at 10:15 am every day</td>
</tr>
<tr>
<td>0 15 10 * * ? 2005</td>
<td>Run at 10:15 am every day in 2005</td>
</tr>
<tr>
<td>0 0/5 14 * * ?</td>
<td>Run every 5 minutes starting at 2 pm and ending at 2:55 pm, every day</td>
</tr>
</tbody>
</table>
Run a dynamic report
You can manually run a dynamic report at any time.

Task
- In the Dynamic Reports list, click in the row for the report that you want to run.

Delete a dynamic report
You can delete a dynamic report that is no longer required.

Task
1. In the Dynamic Reports list, click in the row for the report you want to delete.
2. When prompted for confirmation, click OK.

Configure the report settings
You can opt to display the default logo on reports or you can configure the system to display a custom logo in reports.

Set the logo
It is recommended that the logo be saved as a GIF or JPG, 700x200 in size.

Task
1. On the Reports page, click Settings.
2. Select one of these options:
   - Use Default Logo — The logo that appears in the user interface is displayed in reports.
   - Use Custom Logo — A different logo is displayed in reports. If you select this option, select the graphic file with the logo.
3. Click Save.

XML API
After you enable the XML API, you can request information from the McAfee Database Security Server using a standardized HTTP GET/POST request. The response is in XML format. The detailed structure of the XML reply can be found in the XSD file under System | Interfaces | XML API.

Note
For more on enabling the XML API, see Configure the XML API.

To use the XML API, you must provide the login credentials of a user with the "Use XML API" permission granted.

The available services:
- Sensor — Returns the Sensors list.
- **Alert** — Returns the Alerts list.

**Sensor service**

To use the Sensors service, enter this URL:

<server url>/xmlapi.svc

with the service parameter set to "sensor", for example:

https://192.168.150.163:8443/xmlapi.svc?service=sensor

It also accepts these optional parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH$Name</td>
<td>The name of the sensor.</td>
</tr>
<tr>
<td>HH$Id</td>
<td>The sensor ID (as it appears in the XML API result).</td>
</tr>
<tr>
<td>HH$Hostname</td>
<td>The host name of the server where the sensor is installed.</td>
</tr>
<tr>
<td>HH$Ip</td>
<td>The IP address of the sensor</td>
</tr>
<tr>
<td>HH$Database</td>
<td>The database ID (as it appears in the XML API result).</td>
</tr>
<tr>
<td>HH$Approved</td>
<td>Comma-separated values of the approved statuses (APPROVED, DENIED or PENDING).</td>
</tr>
<tr>
<td>HH$Status</td>
<td>Comma-separated values of the communication status (ALIVE, DISCONNECTED, DELETED or STOPPED).</td>
</tr>
</tbody>
</table>

**Alert service**

To use the Alerts service, enter this URL:

<server url>/xmlapi.svc

with the service parameter set to "alert", for example:


It also accepts these optional parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH$ExecutionTimeFrom</td>
<td>Lower limit on the execution time, in one of these formats:</td>
</tr>
<tr>
<td></td>
<td>▪ Date in the format: dd MMM yyyy HH:mm:ss</td>
</tr>
<tr>
<td></td>
<td>▪ Milliseconds since 1970</td>
</tr>
<tr>
<td>HH$ResolveReason</td>
<td>The resolve reason.</td>
</tr>
<tr>
<td>HH$Id</td>
<td>The alert ID.</td>
</tr>
<tr>
<td>HH$Agents</td>
<td>Comma-separated values of the Sensor IDs (as they appear in the XML API result).</td>
</tr>
</tbody>
</table>
## Working with external databases

The McAfee Database Security Server comes bundled with an efficient in-memory backend database. The database is ideal for customers with moderate alert volumes.

The database can be replaced by a commercial database – either Oracle or MSSQL – for two main reasons:

- If you expect a large volume of alerts (more than 100k alerts between archive events), the use of an external database is needed.
- The use of an external database allows you to use your regular DBMS tools to perform backups, create your own reports, and more.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH$tag</td>
<td>The name of the tag.</td>
</tr>
<tr>
<td>HH$DbGroupName</td>
<td>The name of the DB Group.</td>
</tr>
<tr>
<td>HH$ExecutionTimeTo</td>
<td>Upper limit on the execution time, in the same format as the HH$ExecutionTimeFrom parameter.</td>
</tr>
<tr>
<td>HH$Databases</td>
<td>Comma-separated values of the Database IDs (as they appear in the XML API result).</td>
</tr>
<tr>
<td>HH$Operation</td>
<td>The SQL statement.</td>
</tr>
<tr>
<td>HH$OsUser</td>
<td>The operating system user.</td>
</tr>
<tr>
<td>HH$Severities</td>
<td>Comma-separated values of the alert severity values (LOW, MEDIUM, HIGH).</td>
</tr>
<tr>
<td>HH$SourceHost</td>
<td>Statement source host name.</td>
</tr>
<tr>
<td>HH$SourceIP</td>
<td>Statement source host IP address.</td>
</tr>
<tr>
<td>HH$ResolveNames</td>
<td>Comma-separated values of the resolve type names.</td>
</tr>
<tr>
<td>HH$RuleName</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>HH$ExecUser</td>
<td>The executing database user.</td>
</tr>
<tr>
<td>HH$ExecProgram</td>
<td>The name of the application.</td>
</tr>
<tr>
<td>HH$ClientId</td>
<td>The client ID.</td>
</tr>
<tr>
<td>HH$Module</td>
<td>The module name.</td>
</tr>
<tr>
<td>HH$ModifyDateFrom</td>
<td>The lower limit on the last modified time of the alert in the same format as the HH$ExecutionTimeFrom parameter.</td>
</tr>
<tr>
<td>HH$ModifyDateTo</td>
<td>The upper limit of the last modified time of the alert in the same format as the HH$ExecutionTimeFrom.</td>
</tr>
<tr>
<td>HH$TimeBackPeriod</td>
<td>Time back in milliseconds.</td>
</tr>
</tbody>
</table>
McAfee Database Security supports the use of these external databases:

- Oracle versions 10g and up
- MS SQL 2005 (Service Pack 2) and up

A simple CLI command is used to migrate the database. The Backend Migration Tool supports these options:

- Migrating the internal database to the external database. If at any stage you want to revert to the internal database, the data stored on the external database will be no longer accessible to the McAfee Database Security Server.
- Changing the password used to authenticate the server to the database.

This section describes how to use the Backend Migration Tool to move data from the internal database to an external database.

**Migrating the internal database to an external database**

The Backend Migration Tool is used to migrate the internal database to the external database.

The migration procedure varies slightly according to the type of database (Oracle or MSSQL), as described in these sections:

- *Migration to an MSSQL database*
- *Migration to an Oracle database*

When migrating to an external database, any existing data is automatically moved from the internal database to the external database when it is created.

**Migration to an MSSQL database**

Before using the Migration Tool to migrate to an MSSQL database, you must define the MSSQL database user. A username and password are required to complete the process. The user must have sufficient permissions to create a database.

If you do not want to grant create database permissions to the database user to be used to access the McAfee Database Security Server database, you can migrate the database manually.

**Note**

The process for starting the migration depends on the target platform where the server is installed. The task below applies to Windows platforms.

**Before you begin**

- You must be an administrator to run the Migration Tool.
- The McAfee Database Security Server must be stopped before you try to set up the external database.
- It is recommended to copy the file `server-custom.properties` located in the `<installation directory>/conf` folder and save it under another name (for example, `mcafee-custom.properties.1`).
Task

1. Manually create the databases SNTRSRV and SNTRSRV_BACKUP using a user with create database permissions.

2. Run the migration script and provide it with a database user that is now only required to have these permissions on the SNTRSRV and SNTRSRV_BACKUP databases:
   - db_datareader
   - db_datawriter
   - db_ddladmin

3. Start the migration tool in one of these ways:
   - On a Windows system: Open a command prompt (cmd), then go to the bin directory under the root install directory (for example, C:\Program Files\Mcafee\McAfee Database Security\bin\bin). Then, run the bat file: migration_tool.bat.
   - On a Linux system: Run /etc/init.d/mfe-dbs-server db-migrate.

4. When prompted to select an action, type migrate.

5. When prompted to select the database type, type mssql.

6. When prompted, type in the MSSQL username and password that you defined.

7. When prompted to enter the MSSQL Host address, type in the IP address of the Host server where the database is located.

   Note: If the external database is on the local host, the external IP address or hostname of the server should be used. Do not use localhost or 127.0.0.1.

8. When prompted to enter the MSSQL Listening Port, type in the number of the MSSQL port of the database host used for listening (for example, 1433). Verify that TCP/IP communication is enabled for that IP and port.

After the process is run, a message is displayed indicating the duration of the process and whether the process completed successfully.

When the process completes successfully, the server-custom.properties file is modified to contain properties to enable McAfee Database Security to connect to the external database.

Note: If the process fails, examine and verify that the properties listed on the screen are correct. For further assistance, contact McAfee support with the process output.

Migrate to an Oracle database

Before using the Backend Migration Tool, it is important that you define two new Oracle database users. The resulting usernames and passwords are required to complete the process. Both users should have the permissions: resource and connect. Only the first user is actually used by the McAfee Database Security Server; the second user is used for backup during upgrade scenarios.

Note: The process for starting the migration depends on the target platform where the server is installed. The task below applies to Windows platforms.
Before you begin

- You must be an administrator to run the Migration Tool.
- The McAfee Database Security Server must be stopped before you try to set up the external database.

Task

1. Start the migration tool in one of these ways:

   - On a Windows system: Open a command prompt (cmd), then go to the bin directory under the root install directory (for example, `C:\Program Files\Mcafee\McAfee Database Security\bin\bin`). Then, run the bat file: `migration_tool.bat`.
   - On a Linux system: Run `/etc/init.d/mfe-dbs-server db-migrate`.

2. When prompted to select an action, type `migrate`.

3. When prompted to select the database type, type `oracle`.

4. When prompted, type in the username and password for the first Oracle user.

5. When prompted, type in the username and password for the second Oracle user.

6. When prompted to enter the Oracle host address, type in the IP address or hostname of the server where the database is located.

7. When prompted to enter the Oracle listening port, type in the number of the Oracle listening port (for example, 1521).

8. When prompted for the Oracle SID, type in the database instance SID.

After the process is completed, a message is displayed indicating the duration of the process and whether the process completed successfully.

When the process completes successfully, the `server-custom.properties` file is modified to contain properties enabling the McAfee Database Security Server to connect to the external database. The `server-custom.properties` file is located in the `<installation directory>/conf` folder.

Note

If the process fails, examine and verify that the properties listed on the screen are correct. For further assistance, contact McAfee support with the process output.

Change the configured password for the external database

Typically, all database user passwords change periodically. When the external database is subject to such changes, the McAfee Database Security Server will not be able to connect to the external database.

The backend migration tool provides a way to change the configured password. This process is also useful for checking connectivity to the external database.

The McAfee Database Security Backend Migration Tool’s validation option is intended to create an encrypted password for accessing the external database. The resulting encrypted value is displayed on
the standard output. This value can then be copied into the McAfee Database Security Server server-
custom.properties file to change the authentication password to connect to the external database.

**Note**

The process for validating connectivity depends on the target platform where the server is installed. The task below applies to Windows platforms.

---

**Before you begin**

- You must be an administrator to run the Migration Tool.
- The McAfee Database Security Server must be stopped before you try to set up the external database.

---

**Task**

1. Start the migration tool in one of these ways:
   - On a Windows system: Open a command prompt (cmd), then go to the `bin` directory under the root install directory (for example, `C:\Program Files\McAfee\McAfee Database Security\bin\bin`). Then, run the bat file: `migration_tool.bat`.
   - On a Linux system: Run `/etc/init.d/mfe-dbs-server db-migrate`.

2. When prompted to select an action, type `validate`. This loads the properties specified in the file `server-custom.properties`.

3. When prompted, type in the username and password. If validating an Oracle database, type in the second username and password when prompted.

4. When prompted, type in the database driver or press enter to accept the default (for example, `<com.microsoft.sqlserver.jdbc.SQLServerDriver>`).

5. When prompted, type in the URL or press enter to accept the default.

   After the validation process completes, a message is displayed indicating whether the properties are correct and listing a summary of the properties.

   When prompted, indicate if you want to save the connection properties to the configuration file.

6. If you choose not to save the new configuration, you can do so later by editing the `server-
custom.properties` file located in the `<McAfee Database Security Server install dir>/conf` directory as follows:
   - If you are working with an Oracle database, copy the last two lines of the summary and replace the corresponding lines in the `server-custom.properties` file. The properties are `database.password` and `database.backup.password`.
   - If you are working with an MSSQL database, copy the last line of the summary and replace the corresponding line in the `server-custom.properties` file. The property is `database.password`.

**Note**

The exact order of the properties in the `server-custom.properties` file can vary.
Create your own database (advanced configuration)
This section describes the guidelines for independently creating an external MSSQL database.

This option is intended for use by customers who require restrictive permissions for the external database user and customers who want to create the database before running the migration tool.

If you opt to create the database on your own, these conditions must be met:

- You need to create two databases, named **SNTRSRV** and **SNTRSRV_BACKUP**, respectively.
- On each database, enable the **READ_COMMITTED_SNAPSHOT**, transaction isolation level by running these commands:
  
  ```
  ALTER DATABASE SNTRSRV SET READ_COMMITTED_SNAPSHOT ON
  ALTER DATABASE SNTRSRV_BACKUP SET READ_COMMITTED_SNAPSHOT ON
  ```

- Both databases should be owned by the user created for the DB Security server (for example, “DBSS”).
- The user should be the **dbowner** and must have (at least) these permissions:
  - **db_datareader**
  - **db_datawriter**
  - **db_ddladmin**

---

**Working with the McAfee Database Security Server in Cluster mode**

McAfee Database Security supports running the McAfee Database Security Server in clusters to provide high availability and performance.

**Tasks**

- **Configure your McAfee Database Security Servers to work in Cluster mode**
- **Troubleshooting**

**Configure your McAfee Database Security Servers to work in Cluster mode**

Configuring the McAfee Database Security Servers to work in cluster mode improves system availability and performance. Cluster mode is configured in the `server-cluster.xml` file for each server in the cluster.

**Task**

1. Install McAfee Database Security Server and configure one of the McAfee Database Security Servers to work with an external database, as described in *Working with external databases*.

2. Install McAfee Database Security Server on the other machines in the cluster computers.

4 Rename the file located in `<McAfee Database Security Server install dir>\conf\server-cluster-example.xml` to `<McAfee Database Security Server install dir>\conf\server-cluster.xml`.

5 Edit the file so it contains information about all the servers you intend to use in the cluster in this format:

```xml
- <!--
  This is an example server-cluster.xml file. It is used for
  configuring the server cluster. Each
  server element host and port configurations should match the
  Server configuration.
  Id field must be in the range of 0 to 999. Each server should
  have a unique id and the id shouldn’t be
  changed once assigned to a server.

  In none cluster mode the server uses id 0. Thus, if migrating
  to cluster mode (for example you
  have a server running and you wish to move to a cluster
  configuration) the migrated server
  should receive id 0.
  -->

- <servers>
  - <server>
    - <!--
      either ip or host name
      -->
    <host>cluster1.sample.com</host>
    - <!--
      https listen port of the server
      -->
    <port>8443</port>
    <id>0</id>
  </server>
  - <server>
    <host>cluster2.sample.com</host>
    <port>8443</port>
    <id>1</id>
  </server>
  - <server>
    <host>192.168.1.101</host>
    <port>8443</port>
    <id>2</id>
  </server>
- </servers>
```

Each server XML element should contain these fields:

- **host** — The host name or the IP address of the McAfee Database Security Server.
- **port** — The https port of the McAfee Database Security Server.
- **id** — A unique ID for each server, in the range 0–999. The McAfee Database Security Server that has been migrated to work with an external database should be assigned ID of 0. The ID should not be changed once assigned to a server.

6 Copy the file `<McAfee Database Security Server install dir>\conf\server-cluster.xml` to all the servers in the cluster.

7 On the Server working with an external database, edit your `server-custom.properties` file located in: `<McAfee Database Security Server install dir>\conf directory`. You can add to it these optional parameters:
Working with the McAfee Database Security Server in Cluster mode

- server.server.address — If the server has different internal and external IP addresses, configure here the internal IP address (as the server sees itself).
  For example, server.server.address=192.168.150.111

- server.cluster.ip.whitelist — A list of IP addresses, which are the only ones allowed to connect to the cluster, separated by semicolons.
  For example, server.cluster.ip.whitelist= 127.0.0.1;192.168.150.23

- server.cluster.secret — A shared secret for all the computers in the cluster. Each server will agree to receive connect requests only from other servers in the cluster that have the same secret. If not specified, a default internal secret is used.
  For example, server.cluster.secret=mysecret

- server.cluster.keystore — An alternative keystore location, if you want to use a location other than the one in the server.xml file (located in the <McAfee Database Security Server install dir>\conf directory).
  For example, server.cluster.keystore=C:\Program Files\McAfee\server\httpsKeystore\keystore

- server.cluster.keystore.type — The type of the alternative keystore used.
  For example, mcafee.cluster.keystore.type=JKS

- server.cluster.keepalive — The time in milliseconds after which the server assumes another cluster computer is down, if it does not receive a connection request from it. The default value is 60000.
  For example, server.cluster.keepalive=100000

8 Copy the server-custom.properties file to all servers in the cluster.

9 Restart all cluster servers.

The cluster configuration details can be viewed on the Cluster tab of the System page. For details, see Viewing clusters.

Troubleshooting

If your cluster environment is not responding, verify that:

- All server-custom.properties files on the cluster computers are identical.

- All server-cluster.xml files on the cluster computers are identical.

- All cluster servers' HTTPS ports are accessible from all other cluster computers (with the host name/IP and port as they appear in the server-cluster.xml file).

- The external DB host and port (as configured in the server-custom.properties file) are accessible from all other cluster computers.

If you are still unable to work with your server in the cluster mode configured, contact McAfee support.
Backup and recovery

The Database Security Server stores the configuration of the system (including policy profiles of each Sensor, DBMS information and more). Additionally, the server stores alerts and test result data.

This section covers the procedures necessary to back up the database server. No other backup is necessary (sensors do not store any data and therefore do not need to be backed up or restored).

A complete backup of the server is performed in three stages. The recovery process uses the backup files to restore the system.

Tasks
- Back up the server configuration files
- Back up the server backend databases
- Back up the archive files
- Recover the system

Note

In addition, we recommended saving the installation files of the latest installed server version where you can easily find them in case you need to reinstall the application.

Back up the server configuration files

The server stores its configuration files in the conf directory located at:

Windows: <Root install dir>\conf. For example: C:\Program Files\mcafee\mcafee database security\conf

The configurations stored in these files include listening ports, cluster configuration, external database configuration and customer specific custom configurations. Changes in the configuration files are made manually. We recommend backing up all configuration files each time a configuration change is made.

The server also stores a unique server identifier in the following file:

Windows: <Root install dir>\webapps\ROOT\WEB-INF\config\application\unique.txt.

This file is generated the first time the server is run.

Back up the server backend databases

The server uses a backend database to store system configurations, including policy profiles for each sensor and alerts. The server supports two types of backend databases:

- **Internal backend database (evaluation only)**: The server comes bundled with an in-process backend database. The database is only supported in product evaluations and should store a maximum of 100,000 alerts between archive events.

- **External backend database**: The server can work with Oracle or MSSQL external databases. The use of an external database is required when the server is used in production and was designed to handle a large volume of alerts. Additionally, the use of an external database enables the use of standard DBMS tools to manage the database.
**Backup and recovery**

**Back up the internal database**
The internal in-process database is file-based and stores its data in a set of files.

On Windows platforms, all data files reside in the hsqldb_data directory located at:

```
<Root install dir>\webapps\ROOT\WEB-INF\hsqldb_data
```

To back up the internal database, all files in the specified `hsqldb_data` directory must be copied.

**Note**  
Files may be copied while the server is running.

**Back up the external database**
When running the server with an external database (Oracle or MSSQL), use your regular DBMS tools to perform backups.

Back up the schema according to the database type:

- **Oracle**: Back up the full schema of the users used by server to connect to Oracle.
- **MSSQL**: Back up the Database: SNTRSRV.

**Back up the archive files**
You can configure McAfee Database Security to automatically archive alerts in a specific location and at preset intervals. Archive files storage directory is configured via the Web Console on the **System | Archives | Settings** page.

The default archive location directory on Windows platforms is:

```
<Root install dir>\webapps\ROOT\WEB-INF\archive
```

Archive files should be backed up according to company policy.

**Note**  
Archiving to an external shared storage mount point can be configured via a Windows UNC path, enabling you to use the same backup procedure as for the external storage.

**Recovery**
In the event of a system failure or disaster (such as disk failure), you can use the backup files to restore the system.

**Task**
1. Resolve the issue that caused system failure (for example, replace a failed disk).
2. Reinstall the server.

**Note**  
We recommended you install the same version as previously installed. If you need an installation file that is not available on the McAfee support portal, contact support.

3. Restore the configuration files.
4  Restore the backend database:
   - **Internal database**: Restore latest backup files to hsqldb_data dir.
   - **External database (Oracle or MSSQL)**: Use your regular DBMS tools to perform the database restore.

5  Restore the archive files.