FortiDB™

Version 4.2.0

User Guide

FORTINET
UNIFIED THREAT MANAGEMENT SOLUTIONS

FortiDB User Guide

Version 4.2.0

20 January 2011

15-32100-79408-20090311

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

FortiDB Quick Start

VA QuickStart

This guide leads you through the process that results in the creation of a vulnerability-assessment report for one of your target databases.

Note: All GUI fields marked with an asterisk (*) must be filled in or specified.

The example below assumes you will be assessing an Oracle target database. Therefore you will need to make sure that the FortiDB user for your Oracle target database has the privileges shown below. If your target database is other than Oracle, refer to the Required Privileges for Assessment column of *Privileges for Assessment*

RDBMS Type	Required Privilege(s)

Oracle	• CREATE SESSION
	• SELECT_CATALOG_ROLE
	• SELECT ON:
	  • SYS.AUDIT$
	  • SYS.REGISTRY$HISTORY
	  • SYS.USER$
	  • SYS.LINK$
	  • SYSTEM.SQLPLUS_PRODUCT_PROFILE

1. Login to FortiDB as the FortiDB `admin` user using `fortidb1!$` for the password .
2. Create a FortiDB user who can create a target database group, run an assessment, and review a report about that assessment.
   a) Go to **Administration** > **User Management** in the left-side tree menu.
   b) On the **User Management** page, select the **Add** button.
   c) On the **Add New User** page, select the **General** tab.

   Note: All GUI fields marked with an asterisk (*) must be filled in or specified.

   d) On the **General**-tab form, fill in the text boxes marked with an asterisk (*****). (Assume a user name of `vauser` and a password of `fdb!23`.)
   e) On the **Add New User** page, select the **Roles** tab.
   f) On the **Roles**-tab, select these roles from the **Available Roles** list box:
      - **Target Manager**
      - **Operations Manager**
      - **Report Manager**

   g) Select the  button in order to move those role names to the **Assigned Roles** text box.
   h) Select the **Save** button.
   i) Select the **Logout** link at the top-right of the screen in order to logout the `admin` user.
3. As the newly created user, create a target-database connection.
   a) Login to FortiDB as the FortiDB `vauser` user using `fdb!23` for the password.

You should notice the absence of an **Administration** section in the left-side navigation menu. (`vauser` cannot create, or even view, other users from within the FortiDB application.)

b) Go to **Target Management** > **Targets** in the left-side tree menu.

c) Select the **Add** button.

d) On the **Target** page, select the **General** tab.

e) Enter the information in the text boxes marked with an asterisk (*****) with settings appropriate to your target database. Assume an Oracle target with these parameters:

- **Name:** Enter a name (ex. `vatarget`)
- **Type**: Select your database type (`Oracle`)
- **DB Host Name/IP**: Enter IP address or machine name on your system that contains the Oracle target database (ex. test_machie or 172.30.12.112)
- **Port**: Enter the port number or leave the default (`1521`)
- **DB Name**: Enter the name of your target database. (ex. orcl)
- **User Name**: Enter the name of the your target database
- **Password**: Enter the password of your target database.

f) Select the **Test Connection** button to verify that your target database is reachable and that your connection parameters are correct.
You should see a 'Success' message.

g) Select the **Save** button.
`vatarget` should appear on the **Targets** page under the **Name** column header.

4 . Create a new group and add the newly created connection to your group.

Note: FortiDB runs assessments against target-database groups not individual database connections. And a group can consist of one or more target database.

a) Go to **Target Management** > **Targets Groups** in the left-side tree menu.

b) On the **Target Groups** page, select the **Add** button.

c) On the **Targets** page, enter a name for your group in the **Group Name** text box. (Here assume the group name is `mygroup`.)

d) Build a filter by filling in the following:

- In the **Column** dropdown list, choose **Name**.
- In the **Operator** dropdown list, choose **Contains**.
- In the **Value** text box, enter all or part of the **Name** of the target you created above (For example, use `targ`, a substring of the name, `vatarget`, that you assigned above.)

e) Select the **Apply** button in order to see if this filter selects the target you created above.

f) Select the **Save** icon  near the top of the page.

g) Verify that the target group you just created is then listed on the **Target Groups** page.

5 . Assess the vulnerability of the target database in your group.

a) Go to **Assessment Management** > **Assessments** in the left-side tree menu.

b) On the **Assessments** page, select the **Add** button.

c) Enter a name for your new assessment in the **Assessment Name** text box. (Here assume the assessment name is `myscan`.)

d) Associate your newly created target-database group with your assessment. On the **Assessment** page, select the **Targets** tab.

e) In the **Available Target Groups** list box in the **Target Groups**-tab, select `mygroup`, the target-database group you just created, and then select the  button in order to move `mygroup` to the **Assigned Target Groups** text box.

f) Associate the appropriate group of FortiDB-shipped policies with your assessment. On the **Add Assessment** page, select the **Policies** tab.

g) In the **Available Policy Groups** list box in the **Policy Groups**-tab, select `Oracle Policy Group` (assuming you are assessing an Oracle target database) and then select the  button in order to move that group name to the **Assigned Policy Groups** text box. If you select a Policy Group in the **Available Policy Groups** or **Assigned Policy Group**s list box, policies that belong to the Policy Group are displayed in the Active Policies list box.

Note: Although the active policies can be highlighted, you cannot choose an individual or group of active policies to execute.

h) Select the **Save** button.
You should then see a ready-to-run assessment called `myscan` on the **Assessments** page.

6 . Run your newly created assessment.

Note: FortiDB offers assessment scheduling as well as email and SNMP-trap notifications of assessment results. Here, however, we will simply run the assessment created above which does not incorporate these features.

a) Select the checkbox to the left of the `myscan` row.

b) Select the **Run** button.
After a minute or so, you should see the **Last Run Time** column in the `myscan` row get populated with a stop date and time for the assessment you just ran.

7 . FortiDB ships with several pre-defined reports that will help you analyze your assessments. Here we will examine our assessment with the *Summary Failed Report* which summarizes failed-policy results.

a) Go to **Report Management** > **Pre-Defined VA Reports** in the left-side tree menu.

b) On the **Pre-Defined Reports** page, select **Summary Failed Report.**

c) On the **Vulnerability Assessment Summary Failed Report** page, select:

- `myscan` from the **Assessment Name** dropdown list
- The start date and time associated with `myscan` from the **Assessment Time** dropdown list.
- From the **Target** dropdown list, the target group (here `vatarget`) associated with `myscan`

On the **Target Information** tab of the **Vulnerability Assessment Summary Failed Report** page, you should see the fields get populated with the parameters of your assessment.

d) Select the **Preview Report** tab of the **Vulnerability Assessment Summary Failed Report** page and, after it is compiled, a *Summary Failed Report* will appear in your browser.

e) In order to view your report in another of the supported formats, scroll down to the **Export as** drop down list, select the file format you want, and select the **Export** button.

Note: The following file formats are supported:

- PDF
- Excel
- Tab-delimited
- Comma-separated values

DAM QuickStart (TCP/IP Sniffer with Data Policy)

This guide leads you through the process that monitors your target database with TCP/IP sniffer, and results in generating alerts and exporting alerts to a report.

Note: DAM with TCP/IP Sniffer feature is only available with FortiDB appliance.

Note: All GUI fields marked with an asterisk (*) must be filled in or specified.

The example used in this guide assumes you will monitor an **Oracle target database** with the TCP/IP sniffer. You will apply a Data-Table policy and generate alerts for the Security Violation rule and Suspicious Databases Users rule. Before starting a target connection, you need to make sure that your target database is configured properly to be monitored by FortiDB. For details about configuring Oracle target databases, see *Configuring the Oracle Target Database*.

Note: To use the TCP/IP sniffer for DAM, following network environment and interconnections are required:

- Your target database server and clients use TCP/IP as protocol, and all database activities are going through LAN.
- The network switch, which your target database server connected, must support the port mirroring feature.
- Connect one ethernet port of FortiDB appliance to the mirror port (also known as SPAN port) of switch, which database server connects to.

1 . Login to FortiDB as the FortiDB `admin` user using `fortidb1!$` for the password (default administrator user and password).

2 . Create a target database connection.

a) Go to **Target Management** > **Targets**.

b) Select the **Add** button. The **Target** page will display. The **General** tab is selected.

c) Enter the information in the text boxes marked with an asterisk (*****) with settings appropriate to your target database. Assume an Oracle target with these parameters:

- **Name**: Enter your `target_name`
- **Type**:Select your database type (`Oracle`)
- **DB Host Name/IP**: Enter IP address or machine name on your system that contains the Oracle target database (ex. test_machie or 172.30.12.112)
- **Port**: Enter the port number or leave the default (`1521`)
- **DB Name**: Enter the name of your target database. (ex. orcl).
- **User Name**: Enter the name of the your target database.
- **Password**: Enter the password of your target database.
- **Data Activity Monitoring**: Make sure the 'Allow' checkbox is selected.

d) Select the **Test Connection** button to verify that your target database is reachable and that your connection parameters are correct.
You should see a 'Success' message.

e) Select **Save**.
`target_name` and related information should appear on the **Targets** page.

3 . Configure Monitoring and Data-Table policy.

a) Go to **Data Activity Monitoring** > **Monitors**. You will see your target database listed in the **Target Monitors** page.

b) Click on the name of the target.

c) In the **General** tab, setup collection method and parameters for **Audit Configuration**.

- In the **Collection Method** field, select 'TCP/IP Sniffer' (for this example).
- Select **Version** for your target database (9i, 10g, or 11g for Oracle).
- In the **Sniffer on Port**, select which FortiDB appliance port is connected to switch's mirror port.
- Check the **Save Sniffer Audit Log**, if you want to log all database activity event for audit tracking.
- Check the **Save** button to save your **Audit Configuration**.

d) Go to the **Policies** tab.

e) Select **Table** from the **Data Policies** dropdown list at the button of the screen.
f) Click **Add**.
The **Target Monitor:<target name>** page will display.
g) Configure a Table policy.

- Enter a policy name or use the default name.
- Enter a description if necessary.
- Select the **Enable** checkbox (checked by default). If checked, the policy will be enabled.
- Select the **Create new policy group for policy** checkbox (checked by default). If checked, a policy group will be created.
- Select a severity from the Severity dropdown or use the default.

h) Click the triangle icon of the **Audit Settings** section to expand.
i) In the **Select Objects to Audit** section, configure the following fields:

- Select the **Browse Object by Target** checkbox. (checked by default). If this is checked, you can select the item from the dropdown list.
- Select a schema from the **Schema** dropdown list (ex. SCOTT)
- Select a table or multiple tables you want to monitor from the **Tables** box (ex. EMP or DEPT)
- Select both **Read** and/or **Write** check boxes in the **Audit Actions** filed.
- Click the right arrow to move your selection to the **Selected Objects** table.

j) Click the triangle icon of the **Alert Rule** section to expand.
k) Configure the following fields:

- Confirm that "**Issue alert if ANY of the enabled rules are triggered**"(default) is selected.
- Select the **Security Violation** checkbox (checked by default).
- Check the checkbox of **Suspicious Database Users**.
- Click the triangle icon of **Suspicious Database Users** to expand the field.
- Select user name(s) and click the right arrow to move the selection to the **Selected users** box.
- Check the **Alert any successful access if the database user is in the list** checkbox.

l) Select **Save**. Make sure that the policy you created is listed with the green up-arrow (policy is enabled) in the Status column.

4 . Confirm the table policy group has been automatically created and associated to the target database.
a) Select the **Policy Groups** tab.
b) Confirm the table policy group which is names as "<your policy name> Group" is created and listed in the right box.

5 . Start monitoring your target.
a) Go to the **General** tab.
b) Click **Start Monitoring**.
Monitor status will show "Starting" and then "Running".

6 . Execute SQL statements with your database client side application to generate alerts.

Note: To generate alerts for the Data-Table policy that you configured, execute several SQL statements.

7 . Check alerts.
a) Go to **Data Activity Monitoring** > **Alerts**.
You should see a single or multiple alerts in the Alerts table.
b) To display the alert details, click on each alert. To close the alert details, click the triangle icon of **Alert Details**.

8 . Create a user-defined DAM report.
a) Go to **Report Management** > **User-Defined DAM Reports**.
b) Select **Add**.

c) Enter a name in the **Name** field, and a description in the **Description** field (optional).
d) Go to the **Columns** tab to specify the columns to include in the report.

- Select columns you want to include in the report, and click the right arrow to move the selections to the **Columns in Report** box.

  Note: PDF report is limited to 5 columns if you select the **Portrait** radio button, 8 columns if you select the **Landscape** radio button.

- Click **Save**.

e) Select the formats from the **Export as** dropdown list.

Note: The following file formats are supported:

- PDF
- Excel
- Tab-delimited
- Comma-separated values

f) Select **Export**.
The File Download dialog displays. You can open or save the report to a file.

DAM QuickStart (Data policy)

This guide leads you through the process that monitors your target database and results in generating alerts and exporting alerts to a report.

Note: All GUI fields marked with an asterisk (*) must be filled in or specified.

The example used in this guide assumes you will monitor an **Oracle target database** with the audit_trail parameter set to DB_EXTENDED. You will apply a Data-Table policy and generate alerts for the Security Violation rule and Suspicious Databases Users rule. Before starting a target connection, you need to make sure that your target database is configured properly to be monitored by FortiDB. For details about configuring Oracle target databases, see *Configuring the Oracle Target Database*

Depending on the setting of the audit_trail parameter in your target database, you need to select a different FortiDB collection method as shown below:

Audit_trail setting in your Oracle target database	FortiDB Collection Method
XML, EXTENDED	**XML File Agent**: For this option, you need to run the FortiDB XML file agent. To run the FortiDB XML file agent, see *Running the Oracle XML File Agent*
DB, EXTENDED (used in this example)	**DB, EXTENDED**
DB	**DB, EXTENDED**: for Oracle 9i only.

1 . Login to FortiDB as the FortiDB `admin` user using `fortidb1!$` for the password .

2 . Create a target database connection.

a) Go to **Target Management** > **Targets**.
b) Select the **Add** button. The **Target** page will display. The **General** tab is selected.
c) Enter the information in the text boxes marked with an asterisk (*****) with settings appropriate to your target database. Assume an Oracle target with these parameters:

- **Name**: Enter your `target_name`

- **Type**:Select your database type (`Oracle`)
- **DB Host Name/IP**: Enter IP address or machine name on your system that contains the Oracle target database (ex. test_machie or 172.30.12.112)
- **Port**: Enter the port number or leave the default (`1521`)
- **DB Name**: Enter the name of your target database. (ex. orcl).
- **User Name**: Enter the name of the your target database.
- **Password**: Enter the password of your target database.
- **Data Activity Monitoring**: Make sure the 'Allow' checkbox is selected.

d) Select the **Test Connection** button to verify that your target database is reachable and that your connection parameters are correct.
You should see a 'Success' message.

e) Select **Save**.
`target_name` and related information should appear on the **Targets** page.

3 . Configure a Data-Table policy.

a) Go to **Data Activity Monitoring** > **Monitors**. You will see your target database listed in the **Target Monitors** page.

b) Click on the name of the target.

c) In the **General** tab, confirm the collection method and polling frequency.

- In the **Collection Method** field, DB, EXTENDED is selected (for this example).
- Set the polling frequency (60 seconds by default).

d) Click the **Test** button to test the collection method.
The "Success" message should be shown at the top of the page.

e) Go to the **Policies** tab.

f) Select **Table** from the **Data Policies** dropdown list at the button of the screen.

g) Click **Add**.
The **Target Monitor:<target name>** page will display.

h) Configure a Table policy.

- Enter a policy name or use the default name.
- Enter a description if necessary.
- Select the **Enable** checkbox (checked by default). If checked, the policy will be enabled.
- Select the **Create new policy group for policy** checkbox (checked by default). If checked, a policy group will be created.
- Select a severity from the Severity dropdown or use the default.

i) Click the triangle icon of the **Audit Settings** section to expand.

j) In the **Select Objects to Audit** section, configure the following fields:

- Select the **Browse Object by Target** checkbox. (checked by default). If this is checked, you can select the item from the dropdown list.
- Select a schema from the **Schema** dropdown list (ex. SCOTT)
- Select a table or multiple tables you want to monitor from the **Tables** box (ex. EMP or DEPT)
- Select both **Read** and/or **Write** check boxes in the **Audit Actions** filed.
- Click the right arrow to move your selection to the **Selected Objects** table.

k) Click the triangle icon of the **Alert Rule** section to expand.

l) Configure the following fields:

- Confirm that "**Issue alert if ANY of the enabled rules are triggered**"(default) is selected.
- Select the **Security Violation** checkbox (checked by default).
- Check the checkbox of **Suspicious Database Users**.
- Click the triangle icon of **Suspicious Database Users** to expand the field.

- Select user name(s) and click the right arrow to move the selection to the **Selected users** box.
- Check the **Alert any successful access if the database user is in the list** checkbox.

m) Select **Save**. Make sure that the policy you created is listed with the green up-arrow (policy is enabled) in the Status column.

4 . Confirm the table policy group has been automatically created and associated to the target database.

a) Select the **Policy Groups** tab.
b) Confirm the table policy group which is names as "<your policy name> Group" is created and listed in the right box.

5 . Start monitoring your target.

a) Go to the **General** tab.
b) Click **Start Monitoring**.
Monitor status will show "Starting" and then "Running".

6 . Execute SQL statements in your target database to generate alerts.

Note: To generate alerts for the Data-Table policy that you configured, execute several SQL statements.

7 . Check alerts.

a) Go to **Data Activity Monitoring** > **Alerts**.
You should see a single or multiple alerts in the Alerts table.
b) To display the alert details, click on each alert. To close the alert details, click the triangle icon of **Alert Details**.

8 . Create a user-defined DAM report.

a) Go to **Report Management** > **User-Defined DAM Reports**.
b) Select **Add**.
c) Enter a name in the **Name** field, and a description in the **Description** field (optional).
d) Go to the **Columns** tab to specify the columns to include in the report.

- Select columns you want to include in the report, and click the right arrow to move the selections to the **Columns in Report** box.

  Note: PDF report is limited to 5 columns if you select the **Portrait** radio button, 8 columns if you select the **Landscape** radio button.

- Click **Save**.

e) Select the formats from the **Export as** dropdown list.

Note: The following file formats are supported:

- PDF
- Excel
- Tab-delimited
- Comma-separated values

f) Select **Export**.
The File Download dialog displays. You can open or save the report to a file.

DAM QuickStart (Metadata policy)

This guide leads you through the process that monitors your target database and results in generating alerts for a Metadata policy and export an alert list from monitoring your target databases.

Note: All GUI fields marked with an asterisk (*) must be filled in or specified.

The example used in this guide assumes you will monitor an **Oracle** target database with the audit_trail parameter set to DB_EXTENDED. You will apply a Data-Table policy and generate alerts for the Security Violation rule and Suspicious Databases Users rule. Before starting a target connection, you need to make sure that your target database is configured properly to be monitored by FortiDB. For details about configuring Oracle target databases, see *Configuring the Oracle Target Database*

Depending on the setting of the audit_trail parameter in your target database, you need to select a different FortiDB collection method as shown below:

Audit_trail setting in your Oracle target database	FortiDB Collection Method
XML, EXTENDED	**XML File Agent**: For this option, you need to run the FortiDB XML file agent. To run the FortiDB XML file agent, see *Running the Oracle XML File Agent*
DB, EXTENDED (used in this example)	**DB, EXTENDED**
DB	**DB, EXTENDED**: for Oracle 9i only.

1. Login to FortiDB as the FortiDB `admin` user using `fortidb1!$` for the password .
2. Create a target database connection.
   a) Go to **Target Management** > **Targets**.
   b) Select the **Add** button. The **Target** page will display. The **General** tab is selected.
   c) Enter the information in the text boxes marked with an asterisk (*****) with settings appropriate to your target database. Assume an Oracle target with these parameters:
      - **Name**: Enter your `target_name`
      - **Type**:Select your database type (`Oracle`)
      - **DB Host Name/IP**: Enter IP address or machine name on your system that contains the Oracle target database (ex. test_machie or 172.30.12.112)
      - **Port**: Enter the port number or leave the default (`1521`)
      - **DB Name**: Enter the name of your target database. (ex. orcl).
      - **User Name**: Enter the name of the your target database.
      - **Password**: Enter the password of your target database.
      - **Data Activity Monitoring**: Make sure the 'Allow' checkbox is selected.
   d) Select the **Test Connection** button to verify that your target database is reachable and that your connection parameters are correct.
   You should see a 'Success' message.
   e) Select **Save**.
   `target_name` and related information should appear on the **Targets** page.
3. Configure a Metadata-Tables policy.
   a) Go to **Data Activity Monitoring** > **Monitors**. You will see your target database listed in the **Target Monitors** page.
   b) Click on the name of the target.
   c) In the **General** tab, confirm the collection method and polling frequency.
      - In the **Collection Method** field, DB, EXTENDED is selected (for this example).
      - Set the polling frequency (60 seconds by default).
   d) Click the **Test** button to test the collection method.
   The "Success" message should be shown at the top of the page.
   e) Go to the **Policies** tab.
   f) Select the checkbox of **Tables** of Privilege policy  .

g) Click **Enable**.
The status icon of the Tables policy becomes a green arrow.

4 .Start monitoring your target.
a) Go to the **General** tab.
b) Select **Start Monitoring**.
Monitor status should show "Running". If you see "NEED_RECONFIGURE" message, go to the Policies tab and click the **Reconfigure*** button.

5 .Execute actions in your target database to generate alerts.

Note: To generate alerts for the Metadata-Table policy you configured, execute several SQL statements for your target databases. For example, execute the following statements:

```
create table table1 (column1 int, column2 char);
drop table table1;
```

6 .Check alerts.
a) Go to **Data Activity Monitoring** > **Alerts**.
You should see several alerts in the All Alerts page.
b) To display the alert details, select each alert. To close the alert details, click the triangle icon of **Alert Details**.
c) To change the alert status from "Unacknowledged" to "Acknowledged", select the checkbox(es) of the alerts you want to change the status, and select "Acknowledged" in the **Status** dropdown list.
d) Click **Apply**. The color of the status icon will change.

7 .Create an alert report.
a) Select a view from the **View** dropdown list to display alerts you want to include in the report.
b) Select one of the formats from the **Export as** dropdown list.

Note: The following file formats are supported:

- PDF
- Excel
- Tab-delimited
- Comma-separated values

c) Select **Export**.
The File Download dialog displays. You can open or save the report to a file.

DAM QuickStart (Compliance policy)

This guide leads you through the process that monitors your target database and results in generating a compliance report.

Note: All GUI fields marked with an asterisk (*) must be filled in or specified.

The example used here assumes you will monitor an **MS SQL Serve**r target database. Before starting a target connection, you need to make sure that your target database is configured properly to be monitored by FortiDB. For details about configuring MS SQL Server target databases, see *Configuring the MS SQL Server Target Database*

1 .Login to FortiDB as the FortiDB `admin` user using `fortidb1!$` for the password .
2 .Create a target database connection.
a) Go to **Target Management** > **Targets**.
b) Select the **Add** button. The **Target** page will display. The **General** tab is selected.
c) Enter the information in the text boxes marked with an asterisk (*****) with settings appropriate to your target database. Assume an MS SQL Server target with these parameters:

- **Name**: Enter your `target_name`
- **Type**: Select `Microsoft SQL Server`
- **DB Host Name/IP**: Enter IP address or machine name on your system that contains the Oracle target database.
- **Port**: `1433 (default)`
- **Connect At: Server Level** is selected (default)
- **DB Name**: Enter the name of your MS SQL Server target database is shown and grayed out (ex. master)
- **User Name**: Enter a name of an MS SQL Server database user.
- **Password**: Enter the password of the user.
- **Data Activity Monitoring**: Make sure the 'Allow' checkbox is selected.

d) Select the **Test Connection** button to verify that your target database is reachable and that your connection parameters are correct.
You should see a 'Success' message.

e) Select **Save**.
`target_name` and related information should appear on the **Targets** page.

3 . Configure a compliance policy.

a) Go to **Policy Management > DAM Policies**.

b) Select **Compliance Policies** from the **View** dropdown list. The Compliance policy should be only listed in the table.

c) Click on **Compliance** in the **Policy Name** column.
The **Edit Policy: Compliance** page displays.

d) Configure a compliance policy in the **Edit Policy** page.

- Enter a description if necessary.
- Select the **Enable** checkbox. If checked, the policy will be enabled.
- Select a severity from the Severity dropdown or use the default.

e) Click the triangle icon of the **Audit Settings** section to expand. In this example, you will generate "History Of Privilege Changes" compliance report. For generating "History Of Privilege Changes", you don't need to specify audit settings.

f) Select **Save**. Make sure that the policy you created is listed with the green up-arrow (policy is enabled) in the **Status** column.

4 . Associate the policy group to the MS SQL Server target database.

a) Go to **Data Activity Monitoring** > **Monitors**.

b) Click on the name of your target database. The Target Monitor: <your target name> page displays. The **General** tab is selected.

c) In the **General** tab, configure the following settings:

- In the **Collection Method** field, SQL Trace is selected.
- Enter a full path of the existing trace folder in the Trace Folder field. (Ex. C:\SQLTrace)
- Set the polling frequency (60 seconds by default).

d) Click the **Test** button to test the collection method.
The "Success" message should be shown at the top of the page.

e) Go to the **Policy Groups** tab.

f) Select **Compliance Policies** and click the right arrow to move to the right box.

g) Click **Save**.

5 . Start monitoring your target.

a) Go to the **General** tab.

b) Click **Start Monitoring**.
Monitor status should show "Running".

6 . Execute SQL statements in your target database to generate data.

Note: To generate data for History of Privilege Changes, execute SQL statements to change privileges.

7 . Create a compliance report.

a) Go to **Report Management** > **Compliance Reports** in the left-side tree menu.
b) Select **History Of Privilege Changes** of the compliance reports (for this example).
c) Configure the Generate Audit Compliance report.

- Select **PDF** from the **Export as** dropdown list (default).
- Enter W/R Reference if necessary.
- Set the **Date Range** you want to see data in the report.
- Confirm you see your target database name in the left box. If there is no data, the target name does not appear in the box.

d) Select **Export**.
The File Download dialog displays. You can open or save the report to a file.

Installation (Standalone users only)

Introduction

This topic explains general information of FortiDB installation.

The following table summarizes FortiDB installation.

Category	Descriptions	Notes
Installer Types	• **Windows Installation:** GUI For Windows installation, you should use an Administrator account to install FortiDB. For details on Windows installation, refer to *Windows Installation*. • **UNIX (Solaris, AIX, Linux) Installation:** Command Line Interface For Solaris or AIX installation, and for Linux installations which use an Oracle repository database, you can use, for the account that will install FortiDB: • a non-root user account For Solaris installations involving `pkgadd`, you should also know the owner and group for this account. For details on UNIX installation, refer to *UNIX Installation*.	For both security and performance reasons, Fortinet recommends that the machine where FortiDB will be installed be dedicated to the FortiDB software and not run other memory- or processor-intensive applications. Furthermore, it is advisable to start with a fresh installation of the operating system, and have a minimum number of services running.
Application Types	• **Tomcat** for Windows and UNIX	
FortiDB Repository	• **Derby:** shipped with FortiDB No manual setup is required. • **PostgreSQL** For setting up PostgreSQL repository, refer to *Configuring a PostgreSQL Repository* • **Oracle** For setting up Oracle repository, refer to *Configuring an Oracle Repository*. • **MS SQL Server**	You should not use the FortiDB application to assess its own repository database. For all repository types except Derby, make sure that your character-encoding setting is **UTF-8**. **Note:** For performance reasons, Fortinet recommends that you put your repository database on a different machine than that used for the FortiDB application. If you are using the Derby

Category	Descriptions	Notes
	For setting up MS SQL Server repository, refer to *Configuring an MS SQL Server Repository*.	repository that ships with the FortiDB application, this will not be possible.
System Requirements	See the Supported Hardware section of the Release Notes accompanying this version for a list of currently supported hardware and software.	
FortiDB Location	You can install FortiDB in any directory. Once installed, <FortiDB-install directory> represents the installed location.	
Installation Confirmation	Following the installation process, you can test the success of a New or Upgrade installation by opening a browser and entering a URL like this: `http://<fortidb_host>:<port>/fortidb` 'fortidb_host' is FortiDB machine or IP address, 'port' is the application server port. If your installation is successful, you will see Login page with which your FortiDB administrator can login to, and perform administrative tasks with, FortiDB. For the FortiDB administrator, the initial, default username is admin and the initial, default password is fortidb1!$	For using DAM (Data Activity Monitoring), the FortiDB user should be "admin" user. For using VA (Vulnerability Assessment), "admin" user should be used only for performing administrative tasks such as adding new users and performing backups. In order to maintain separation of duties, you should create other users, and assign them the appropriate roles for using FortiDB VA.
Initial FortiDB Administrator name and password	For the FortiDB administrator, the default username is admin and the initial, default password is fortidb1!$	After login, "admin" user should change the password from User Management page.

Prerequisites

This is a prerequisites list you need to prepare and consider prior to installing FortiDB.

System Prerequisites

This is a prerequisites list for your computer system.

Prerequisite or Requirement	Detail	Comments
Disk space	200 MB of free disk space. Additional space will be required for log files, reports and assessment-result archives.	This is a minimum requirement. In order to optimally use FortiDB, consult with a FortiDB representative for recommendations more suited to your individual situation.
Memory	A minimum of 1024 MB of system memory, 512 MB of which are dedicated to the FortiDB application	This is a minimum requirement. In order to optimally use FortiDB, consult with a FortiDB representative for recommendations more suited to your individual situation.
Processor	The processor requirements for both Windows and Linux are: Intel-based platforms configured with one or more P4 (or higher) processors. The processor requirement for Solaris is SPARC-based platform configured with one or more processors	

Prerequisites for Installation

This is a prerequisites list you need to prepare prior to installing FortiDB.

Prerequisite or Requirement	Detail	Comments
User account for FortiDB installation	Create a user account that you will use in order to install FortiDB. For Windows, it should be an Administrator-level account. For Linux or Solaris, it should be a non-`root` account.	
Location for FortiDB	Choose a directory in which you want to install FortiDB.	If you choose a location where a previous version of FortiDB exists, an Upgrade installation will be performed. **Note:** Choose a path whose name does NOT contain a space. For example, this would not work: C:\Program Files\FortiDB due to the space between 'Program' and 'Files'.
DB type for your repository database	Choose from Derby, MS SQL Server, Oracle, and PostgreSQL	Derby ships with FortiDB at no charge and gets set up during the FortiDB installation. For MS SQL Server, Oracle, and PostgreSQL, you should set up your

Prerequisite or Requirement	Detail	Comments
		repository database before installing FortiDB. See the FortiDB Repository section.
Name of host machine for repository database	You will need to specify the hostname or IP address for the machine containing your MS-SQL, Oracle, PostgreSQL, or DB2 repository database.	
Port number for repository database	Choose an available port number above 1024	
Database name/SID for repository database	Specify the name (or SID) of the database you will use for the FortiDB repository database.	
Username for repository-database user	You should set up a database user account before installing FortiDB and know the account name before installing FortiDB.	
Password for repository-database user account	You should know the database user's password before installing FortiDB.	
Application Server HTTP Port Number	Choose an available port number above 1024	
Application Server HTTPS Port Number	Choose an available port number above 1024	
Application Server Shutdown Port Number	Choose an available port number above 1024	

FortiDB Repository

FortiDB supports the following databases as FortiDB internal repository. For all repository types except Derby, the specific settings are required.

- **Derby** (shipped with FortiDB)
- **PostgreSQL**: For setting PostgreSQL repository, see *Configuring a PostgreSQL Repository*
- **Oracle:** For setting Oracle repository, see *Configuring an Oracle Repository*
- **MS SQL Server:** For setting MS SQL Server repository, see *Configuring a MS SQL Server Repository*

Note: For all repository types except Derby, make sure that your character-encoding setting is UTF-8.

Configuring a PostgreSQL Repository

This topic describes configuring a PostgreSQL database to use as the FortiDB repository. If you use PostgreSQL 8.x as your local repository, you need to create the language pack in order to use the FortiDB archive feature properly.

1. Create a database to use for FortiDB local repository (for example, "fortidb") with UTF8 encoding. For FortiDB installation, the following information is necessary.
   - Database name for FortiDB local repositoy
   - User name of FortiDB local repository
   - Password of FortiDB local repository user
2. Create the language pack. To Create the language pack, plpgsql by executing the following command:

   ```
   createlang -h 127.0.0.1 -d <database_name> -U <database_user> plpgsql
   ```

   - <database_name> is the database name
   - <database_user> is the database user name
3. Make sure the language pack is installed properly by executing the following command:

   ```
   psql -U <database_user> -c "select * from pg_language"
   ```

   - <database_user> is the database user name

   As a result of this command, you will see the row of "plpgsql" in the pg_language table.

Configuring an Oracle Repository

This topic describes configuring an Oracle database to use as the FortiDB repository.

1. Create a tablespace for FortiDB that has the following values or minimum parameter settings:
   - Block Size (B): at least 16K
   - Total SGA size: at least 500MB
   - Total PGA size: at least 100MB
   - Segment Space Management: Automatic
   - Extent Management: Local
2. Create a user for FortiDB which have the following privileges:
   - CREATE SESSION
   - CREATE TABLE
   - CREATE SEQUENCE
   - `UNLIMITED QUOTA` for a FortiDB-dedicated tablespace.
3. Consider I/O contention. For example, put your database and log files on separate disks.
4. Create a datafile for the FORTIDB tablespace. For example:
   - File Name: FORTIDB.DBF
   - File Directory: C:\oralce\product\10.2.0\oradata\orcl\
   - Tablespace: FORTIDB
   - File size: 500M
   - Automatically extend datafile when full (AUTOEXTEND)
5. Here is an example of the parameters in init.ora (for Oracle 10g):

   ```
   *.db_name='fortidb'
   *.db_block_size=8192
   *.sga_target=584M
   *.pga_aggregate_target=194M
   ```

```
*.db_create_file_dest='/home/oracle/product/10.2.0/db_1/oradata/fdb'
*.db_recovery_file_dest='/home/oracle/product/10.2.0/db_1/
flash_recovery_area'
*.db_recovery_file_dest_size=2G
*.undo_management='AUTO'
*.undo_tablespace='UNDOTBS1'
*.audit_file_dest='/home/oracle/product/10.2.0/db_1/admin/fdb/adump'
*.user_dump_dest='/home/oracle/product/10.2.0/db_1/admin/fdb/udump'
*.core_dump_dest='/home/oracle/product/10.2.0/db_1/admin/fdb/cdump'
*.background_dump_dest='/home/oracle/product/10.2.0/db_1/admin/fdb/bdump'
*.compatible='10.2.0.3.0'
*.control_files='/home/oracle/product/10.2.0/db_1/oradata/fdb/
control01.ctl'
*.db_file_multiblock_read_count=16
*.job_queue_processes=10
*.open_cursors=300
*.processes=150
```

Configuring an MS SQL Server Repository

This topic describes configuring an MS SQL Server database to use as the FortiDB repository. The instruction of this topic uses MS SQL Server 2008 Management Studio as an example. **WARNING: The user ID and schema name must be same for the FortiDB repository.**

1 . Create the database “fortidb”

a) Log in as “sa”
b) Right-click on Databases.
c) Click New Database.
d) Enter “fortidb” as the database name.
e) Configure the database meets the following requirement:

- Has an initial data-file size of at least 300 MB
- Has an initial log-file size of at least 20 MB
- Has a collation value that allows for case-sensitivity.

Note: A case-sensitive collation value will have the characters “CS” appended to the Collation Designator. For example, the collation value SQL_Latin1_General_CP1_CS_AS is for U.S. English systems.

f) Click OK.

2 . Create the system login “fortidb”

a) Go to Security
b) Right-click on Logins.
c) Select New Login
d) Enter “fortidb” as the login name
e) Use SQL authentication and enter your own password
f) Uncheck the enforce password expiration checkbox
g) Select “fortidb” in the Default database field
h) To set the user mappings, go to the User Mapping page
i) Check “fortidb”. The user column on that row should now show “fortidb"
j) With that row selected, select the db_owner permission (in the lower box, which should say Database role membership for: fortidb”
k) Click OK

3 . Create the fortidb schema.

Note: The schema name has to be the same as the login name that you created in the previous step.

a) Log in as “fortidb” with the password you created in step 2.
b) Go to Databases > fortidb > Security.
c) Right click on Schemas and select New Schema
d) Enter “fortidb” in the Schema name filed and Schema owner field
e) Click “OK”
f) Go to Databases > fortidb > Security > Users.
g) Right-click “fortidb” user, and select Properties.
h) Enter “fortidb” in the Default schema field
i) Click OK

4 .Verify that the login “fortidb” is mapped to the proper schema “fortidb” and user “fortidb”
a) In your sa login, go to > Security > Logins
b) Right-click on fortidb, and select Properties.
c) In the User Mapping page, verify that the row for “fortidb” shows “fortidb” for both user and default schema

UNIX Installations

This topic introduces two ways in which you can install FortiDB on UNIX.

In order to install FortiDB on UNIX, the following installation utilities are available:

- Interactive, console-based installation for all of the operating systems that FortiDB supports
- `pkgadd` utility for Solaris

UNIX Console Installations

This topic explains how to install FortiDB on UNIX using the console-based installation type.

1 .Satisfy all prerequisites in the Installation Checklist.
2 .Execute the installer file supplied by Fortinet using this syntax: `sh <installer_file>`

Using pkgadd to Install FortiDB on Solaris

This topic explains how to install FortiDB with the `pkgadd` utility on Solaris.

In order to install FortiDB on Solaris, using the `pkgadd` utility:

Note: You must use an Oracle database for your FortiDB repository if you want to use `pkgadd`.

Note: Your prompt responses for `pkgadd` installations are not validated. This means that an unsuccessful installation could result in an inaccurate "successful installation" message at the end of the `pkgadd` process.

1 .Satisfy all prerequisites in the *Prerequisites* section.
2 .Put the Solaris package for FortiDB in a directory of your choosing and then execute the following command as `root`:

```
pkgadd -d <full path to Solaris package for FortiDB> -R <FortiDB-install
 directory>
```

Uninstalling pkgadd Installations on Solaris

This topic explains how to uninstall FortiDB installations installed with the `pkgadd` utility on Solaris.

1 .Stop FortiDB:

```
<FortiDB-install directory>/bin/stop
```

2 .Remove the package:

```
pkgrm -R <FortiDB-install directory>
```

Uninstalling FortiDB on UNIX

This topic explains how to uninstall FortiDB on UNIX.

1. In order to uninstall FortiDB on UNIX, go to the `<FortiDB-install directory>/uninstall` directory
2. Execute:
   `uninstall`

Windows Installations

This topic explains how to install FortiDB on Windows.

Installation is available via:

- A GUI-based installer
- A silent installer

Windows GUI Installations

This topic explains how to install FortiDB on Windows using the GUI.

1. Satisfy all prerequisites in the Prerequisites section.
2. Open the installer EXE file supplied by FortiDB.
3. Follow the instructions presented by the GUI installer.

Uninstalling FortiDB on Windows

This topic explains how to uninstall FortiDB on Windows.

1. Go to the *<FortiDB-install directory>\uninstall* directory
2. Execute:
   `uninstall.exe`

   The Uninstall FortiDB dialog displays.
3. Click the **Uninstall** button. All items will be uninstalled.
4. Click **Done.**

Post Installation Operations (Tomcat)

These are operations you might need to perform after installing FortiDB with a Tomcat application server.

Operation or Item	Descriptions
Starting and Stopping FortiDB	You might find it necessary to start and or stop FortiDB manually. For example, when updating or replacing your FortiDB license file. Or, after rebooting on UNIX , you might need to manually start FortiDB. When FortiDB is stopped, it saves state information within the internal database. When you log back in; this information is retrieved and the databases that were open prior to shutdown are reopened once again. Since state information is periodically saved during your session, most of the state can be restored--even if FortiDB goes down due to a power failure or other similar problems occur. • In order to manually start FortiDB:

Operation or Item	Descriptions
	• On Windows, you can use either the <*FortiDB-install directory*>*bin**start.bat* batch file or the **Start->Programs->FortiDB ->Start FortiDB** menu choice. • On UNIX, use the <*FortiDB-install directory*>/*bin*/*start* script. • In order to manually stop FortiDB: • On Windows, you can use either the <*FortiDB-install directory*>*bin**stop.bat* batch file or the **Start->Programs->FortiDB ->Stop FortiDB** menu choice. • On UNIX, use the <*FortiDB-install directory*>/*bin*/*stop* script.
Changing the FortiDB Administrator Password	For security reasons, it is highly recommended that you change the password for the FortiDB administrator user account (admin) after installation.
Installing a New License	FortiDB requires a license key in order to operate and ships with a temporary one. About two weeks before your license expires, you may see a notice warning you that your license is about to expire. You should then contact your FortiDB sales representative for an extended license. To install the new license: **1 .**Stop FortiDB. **2 .**Replace *license.properties* with the new license file in <*FortiDB-install directory*>/*conf* **3 .**Restart FortiDB.
Troubleshooting	FortiDB produces log files that can assist troubleshooting. These are files that Fortinet Support may need to assist you: • <*FortiDB-install directory*>/*logs*/*.log* • <*FortiDB-install directory*>/*tomcat*/*logs*/*.log*
Managing Disk Space	FortiDB log, archive, and report files all consume disk space which you must manage in order to conserve disk space. So you might want to backup these files, delete them and then restore them if needed.
Important Directories	You may occasionally need to know about these directories • <*FortiDB-install directory*>/*bin* contains utility files including those that allow manual starting and stopping of FortiDB • <*FortiDB-install directory*>/*conf* contains your license file, encryption-key files, installation-properties file, and your report logo files. • <*FortiDB-install directory*>/*data*/*archives*/VA contains assessment-archive files • <*FortiDB-install directory*>/*data*/*reports* contains report files • <*FortiDB-install directory*>/*doc* contains the Administration, Quick Start, and Installation Guides

Operation or Item	Descriptions
	• *<FortiDB-install directory>/etc/conf/pentest* contains Pen Test-related files • *<FortiDB-install directory>/etc/snmp* contains the SNMP-trap dictionary file for FortiDB • *<FortiDB-install directory>/logs* contains error and other log files • *<FortiDB-install directory>/tomcat/logs* contains log files for the Tomcat application server • *<FortiDB-install directory>/uninstall* contains the uninstall executable

Important FortiDB Files and Folders (in *<FortiDB-install directory>/conf*)	• *license.properties* (specifies the length of, and number of target-databases allowed during, the FortiDB license period.)
	• *.keyFile* (needed for the encryption of passwords and assessment archives)
	• *.keystore* (needed for target-database connections involving SSH)
	• *reportlogos* directory (contains images for report logos)
	• The *<FortiDB-install directory>/etc* directory contains:
	  • Pen Testing dictionary and db-type-specific files
	  • XML files with samples of importable target-database information
	  • FortiDB-specific MIB file for SNMP notifications
	  • a *templates* directory containing *server.xml* (this file is for internal FortiDB use only).

Tomcat Troubleshooting

This topic contains information about troubleshooting a FortiDB installation involving a Tomcat application server.

Tomcat Logs

You can troubleshoot installation problems by reviewing information in Tomcat's log files. The log files are located in these directories:

- <FortiDB-install directory>/logs
- <FortiDB-install directory>/tomcat/logs
- <FortiDB-install directory>/tomcat/webapps/fortidb/WEB-INF/logs

Upgrading FortiDB

This topic describes instructions to upgrade from an earlier version of FortiDB

Upgrade Instructions

In order to perform an Upgrade installation from earlier version of FortiDB, follow these steps:

1 .(Optionally) backup your repository database.

2 . Shutdown your existing FortiDB process or service.
Depending on your platform type, use the following instructions to shutdown FortiDB:

- If your FortiDB application resides on a UNIX platform, execute *<FortiDB-install directory>/bin/stop*
- If your FortiDB application resides on a Windows platform, either execute *<FortiDB-install directory>* *bin**stop.bat* or stop the FortiDB Application Server service.

3 . Execute the FortiDB installer file.

4 . Point to the directory that contains your existing FortiDB installation.

5 . Follow the subsequent instructions.

Login

Login Steps

You must have a valid FortiDB license in order to login.

Open the FortiDB application in your browser. Depending upon its location with respect to your browser location and depending upon your chosen port number, that will require a specific URL.

In the FortiDB Login page, take the following steps:

1 .Enter your assigned username.
2 .Enter your assigned password.
3 .Select the **Login** button.
4 .Using the navigation panel on the left side of the page, go to the FortiDB component of interest.

Changing Your Password

This topic describes how your FortiDB users can change their passwords.

1 .Login.
2 .Select the **Change Password** link on the top of any page in the FortiDB application.
3 .Enter you existing password in the **Old Password** text box.
4 .Enter your proposed new password in the **New Password** text box.

Note: Your password must meet the criteria for acceptable passwords.

5 .Enter your proposed new password again in the **Reenter New Password** text box.
6 .Select the **OK** button.

Password Rules

The following table indicates the rules for creating your password.

Rule Category	Descriptions
Mandatory Length	By default, no mandatory length is set. You can set the length limitation in System Configuration. Please see the Minimum Password Length properties in *System Properties List*
Mandatory contents	• At least one number • At least one special character from this set: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./
Prohibited Contents	• Any spaces • User name • User name reversed

Appliance - Basic

Before Using Appliance

Default Settings

- The default IP address/subnet of port1 is 192.168.1.99/255.255.255.0
- The default administrator user/password is admin/fortidb1!$
- Web administration is available with access of https://ip_address/
- Connect your terminal to appliance's console port with 9600/8N1 (or check hardware specification for particular model)

Setup Appliance Before Using

- Connect to appliance with terminal console or network cable, login with CLI or Web Administration, to change IP Address and Netmask.
- Change time setting and specify correct Time Zone, Save and Reboot the appliance. (FortiDB needs to be same time zone with target database server, for monitoring function).
- Change default password of user 'admin'.
- Connect FortiDB appliance to your network, make sure it can reach your database server. Setup static route in FortiDB if need.
- If need monitor database with TCP/IP sniffer, connect FortiDB appliance's another port to your network switch's SPAN port. The switch must have TCP/IP traffic of your database activity.

System Information

The System Information page displays basic information about the FortiDB unit. FortiDB administrators, whose access profiles permit maintenance read and write access, can change the FortiDB firmware.

Serial Number	The serial number of the FortiDB unit. The serial number is specific to the FortiDB unit and does not change with firmware upgrades. Use this number when registering your FortiDB unit with Fortinet.
Uptime	The time in days, hours, and minutes since the FortiDB was started or last rebooted.
System Time	The current time according to the FortiDB internal clock. Select the **Change** link to change the time. For details, see *Setting the System Time*.
Host Name	The name of the host name of FortiDB unit. For details on changing the name, see *Changing the FortiDB Host name*.
Firmware Version	The version of the firmware installed on the FortiDB unit. Select Update to upload a new version of the firmware. For details on

updating the firmware, see *Changing the Firmware Version*.

Note: Please set the correct Time Zone before using the appliance. To monitor the target database, your appliance must be same time zone as database server.

Setting the System Time

This topic describes how to set the system time to ensure correct report time ranges and scheduling and accurate logging.

1. Go to Appliance > **System Information** on the left-side tree menu.
2. Select the **Change** link to change the system Time.
   The **Time Settings** page displays.
3. You have options to set the time as follows.

Options	Description
System Time	The current FortiDB system date and time. Select the **Refresh** button to update the display of the current FortiDB system date and time.
Time Zone	Select the FortiDB unit's time zone from the **Time Zone** dropdown list. The **Automatically adjust clock for daylight saving changes** checkbox switches the clock setting between daylight saving time and non-daylight saving time. **Note:** Changing Time Zone requires rebooting the system to take the change into effect.
Set Time	Select to set the FortiDB system date and time to the values you set in the **Year**, **Month**, **Day**, **Hour**, **Minute** and **Second** fields.
Synchronize with NTP Server	Select to use an NTP server to automatically set the system date and time. You must specify the server and synchronization interval. Alternatively, select Set Time. • Server: Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see http://www.ntp.org. • Sync Interval: Specify how often the FortiDB unit should synchronize its time with the NTP server. For example, a setting of 1440 minutes causes the FortiDB unit to synchronize its time once a day.

4. Select **OK.**

Changing the FortiDB Host Name

This topic describes how to change the FortiDB unit host name.

1 .Go to **System Information** under **Appliance**.
2 .In the **Host Name** field of the System Information section, select the **Change** link.
The **Edit Host Name** dialog displays.
3 .In the **Host Name** field, type a new host name.
4 .Select **OK**.
The new host name is displayed in the **Host Name** field.

Changing FortiDB Firmware

This topic describes how to upgrade the FortiDB firmware. When changing the firmware image, the FortiDB unit will either keep or reset its configuration. Fortinet recommends backing up all configuration settings from your FortiDB unit before upgrading.

1 .Download the firmware image file to your management computer.
For FortiDB units with a valid technical support contract, firmware images can be downloaded from the Fortinet Technical Support web site, https://support.fortinet.com.
2 .Log on to FortiDB as the administrative user.
3 .Go to **Appliance** > **System Information**.
4 .In the **Firmware Version** field, select the **Update** link.
5 .Type the path and file name of the firmware image file, or select the **Browse** button and locate the firmware image file.
6 .Select **OK**.
7 .Select **Update.** The FortiDB unit uploads the firmware image file, upgrades to the new firmware version, restarts. This process takes a few minutes.

Note: All data created in the previous version stays intact after updating the firmware version. If you want to reset all device settings and configuration, and delete log data on the hard drive, you can use `execute format disk` command using CLI. For details, see Command Line Interface section.

System Resources

The System Resources section displays usage of the FortiDB unit's resources, including CPU, memory (RAM) and hard disk.

CPU Usage	The current status of CPU usage. This field displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
Memory Usage	The current status of memory usage. This field displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
Hard Disk Usage	The current status of hard disk usage. This field displays the amount of hard disk space used.

Unit Operation

The Unit Operation section allows administrator to reboot, reset data, or format hard disk to appliance.

Device Information	Display the device model, and connection status of Ethernet Ports.
Operation	Reboot, Reset Data, Format Hard Disk.

Network Configuration

You can configure the FortiDB unit to operate in your network in the **Network Configuration** page or using the CLI. Basic network settings include those for interfaces, DNS settings and static routes.

Note: You can specify IP address/network-mask pairs with either:

- Dotted-decimal format; e.g., 192.168.1.1/255.255.255.0
- Bit representation; e.g., 192.168.1.1/24

Interface

You can configure the interfaces on the FortiDB unit, including interface names, device IP, and Access.

Interface	The name of the network interface on the FortiDB unit.
Device IP/Netmask	The IP address and network mask configured for the interface.
Access	A list of the administrative access methods available on the interface.
Status	The status of the network interface. • A green arrow indicates the interface is up. Select Modify icon to disable the port. • A red arrow indicates the interface is down. Select Modify icon to enable the port.
Modify	Select Modify to change the interface settings.

Changing the Interface Settings

This topic describes how to change the FortiDB interface settings.

1. Go to **Network** under **Appliance.**
2. Select the **Interfaces** tab.
3. In the row corresponding to the interface you want to change, select **Modify**.
4. Configure the following options:

Options	Description
Enable checkbox	You can change the interface status by using this checkbox. To disable the port, uncheck the checkbox. To enable the port, check the checkbox.

Options	Description
Interface Name	The interface name cannot be changed.
Device IP/Netmask	Enter an IP address and network mask. For example, 192.168.10.3 / 255.255.255.0
Access	Select which methods of administrative access should be available on this interface. • **HTTP** allows HTTP connections to the FortiDB. HTTP connections are not secure and can be intercepted by a third party. • **HTTPS** allows secure HTTPS connections to the FortiDB. • **PING** allows response to ICMP pings, which are useful for testing connectivity. • **SSH** allows SSH connections to the FortiDB CLI. • **TELNET** allows Telnet connections to the FortiDB CLI. Telnet connections are not secure, and can be intercepted by a third party.

5 .Select the **Save** button.

DNS

You can configure primary and secondary DNS servers to provide the name resolution required by FortiDB features.

Changing the DNS settings

This topic describes how to configure DNS settings.

1 .Go to **Network** under **Appliance**.
2 .Select the **DNS** tab.
3 .Enter an IP address for a primary and secondary DNS server.

Options	Description
Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter a secondary DNS server IP address.

4 .Select the **Apply** button.

Routing

The Routing tab displays the FortiDB unit's static routes.

Destination IP/Netmask	The destination IP address and netmask for packets that FortiDB sends to.
Gateway	The IP address of the router where FortiDB forwards packets.

Interface	The names of the FortiDB interfaces through which intercepted packets are received and sent.
Modify	Select to change the route configuration settings or delete them. For changing route settings, select  . For deleting the route settings, select  .

Adding Route settings

This topic describes how to add FortiDB unit's static routes.

1. Go to **Network** under **Appliance.**
2. Select the **Routing** tab.
3. Select the **Add** button.
   The **Edit Route** page displays.
4. Enter the following options.

Options	Description
Destination IP/Netmask	The destination IP address and netmask for packets that FortiDB sends to.
Gateway	The IP address of the router where FortiDB forwards packets.
Interface	Select a FortiDB interface name from the pull-down list.

5. Select the **Save** button.

Deleting Route Settings

This topic describes how to delete FortiDB unit's static routes.

1. Go to **Network** under **Appliance**.
2. Select the **Routing** tab.
3. In the row corresponding to the routes you want to change, select  to delete the route settings.
   The confirmation dialog displays.
4. Select **OK.**

Changing Route Settings

This topic describes how to change FortiDB unit's static routes.

1. Go to **Network** under **Appliance**.
2. Select the **Routing** tab.
3. In the row corresponding to the routes you want to change, select the modify icon to modify the route settings.
4. Enter the following options.

Options	Description
Destination IP/Netmask	The destination IP address and netmask for packets that FortiDB sends to.
Gateway	The IP address of the router where FortiDB forwards packets.
Interface	The names of the FortiDB interfaces through which intercepted packets are received and sent.

5 .Select the **Save** button.

Configuring Network Settings using the CLI

This topic describes the steps to configure your network settings using the CLI. For details about each command, refer to the Command Line Interface section.

1 .Set the IP address and netmask of the LAN interface:

```
config system interface
  edit <port>
  set ip <ip_address> <netmask>
  set allowaccess (http https ping ssh telnet)
end
```

where:

- <port> can be one of port1- port4.
- <ip_address> is the interface IP address.
- <netmask> is the interface netmask.

Sample Command:

```
config system interface
 edit port1
 set ip 192.168.100.159 255.255.255.0
 set allowaccess ping https ssh
end
```

2 .Set the primary and optionally the secondary DNS server:

```
config system dns
  set primary <dns-server_ip>
  set secondary <dns-server_ip>
end
```

where:

- <dns-server_ip> is the primary or secondary DNS IP server address

Sample Command:

```
config system dns
 set primary 65.39.139.52
 set secondary 65.39.139.62
end
```

3 .Set the default gateway:

```
config system route
  edit <seq_num>
  set device <port>
  set gateway <gateway_ip>
end
```

where:

- <seq_num> is an unused routing sequence number starting from 1 to create a new route.
- <port> is the port used for this route.
- <gateway_ip> is the default gateway IP address for this network.

Sample Command:

```
config system route
 edit 1
 set device port1
 set gateway 172.30.62.254
```

```
end
```

4 .Set a network protocol (NTP) server:

```
config system ntp
    set server <server_ip>
    set status (enable | disable)
end
```

where:

- <server_ip> is the IP address or fully qualified domain name of the NTP server.

Sample Command:

```
config system ntp
 set server 172.30.62.81
 set status enable
end
```

Managing Firmware

Fortinet periodically updates the FortiDB firmware to include enhancements and address issues. After you have registered your FortiDB system, FortiDB firmware is available for download at http://support.fortinet.com. Only the FortiDB administrators, whose access profiles contain system configuration read and write privileges, and the FortiDB admin user can change the FortiDB firmware.

Backing up Your Data and Configuration

Fortinet recommends backing up all data and configuration settings from your FortiDB unit before upgrading. This ensures all data and configuration settings are not lost if you require upgrading or resetting FortiDB unit and want to restore data and configuration settings.

Note: Always backup your configuration before installing a patch release, upgrading, or when resetting to factory defaults.

Backing Up your Configuration using the CLI

This topic describes how to backup up your data and current configuration using the CLI. You will need an FTP server to back up the current configuration from the CLI.

1 .Log into the CLI.

2 .Enter the following command to back up your local database, system-configuration settings, archives and reports:

```
execute backup all-settings <ftp server> <filepath> <username> <password>
 [cryptpasswd]
```

For details about backup and restore using the CLI, see the All-Settings Backup and All-Settings Restore sections in *Appliance - Command Line Interface*.

3 .After successfully backing up your configuration files from the CLI, proceed with upgrading FortiDB firmware.

Upgrading FortiDB Firmware using the Web-based Manager

This topic describes how to upgrade the FortiDB firmware. When changing the firmware image, the FortiDB unit will keep its data and configuration.

1 .Download the firmware image file to your management computer.

For FortiDB units with a valid technical support contract, firmware images can be downloaded from the Fortinet Technical Support web site, https://support.fortinet.com.

2 .Log on to FortiDB as the administrative user.

3 .Go to **Appliance** > **System Information**.

4 .In the **Firmware Version** field, select the **Update** link.

5 .Type the path and file name of the firmware image file, or select the **Browse** button and locate the firmware image file.

6 .Select **OK**.

7 .Select **Update.** The FortiDB unit uploads the firmware image file, upgrades to the new firmware version, restarts. This process takes a few minutes.

Note: All data created in the previous version stays intact after updating the firmware version. If you want to reset all device settings and configuration, and delete log data on the hard drive, you can use `execute format disk` command using CLI. For details, see Command Line Interface section.

Upgrading FortiDB Firmware using the CLI

To use the following procedure, you must have a TFTP or FTP server the FortiDB unit can connect to. You must also log in using the admin administrator account.

1 .Make sure the FTP or TFTP server is running.

2 .Copy the new firmware image file to the FTP or TFTP server.

3 .Log into the CLI.

4 .Make sure the FortiDB unit can connect to the FTP or TFTP server.
You can use the following command to ping the computer running the FTP or TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

5 .Enter the following command to copy the firmware image from the TFTP server to the FortiDB unit:

```
execute restore image ftp <filename> <ftp_ip>
execute restore image tftp <filename> <tftp_ip>
```

Where <filename> is the name and location of the firmware image file and <ftp_ip> or <tftp_ip> is the IP address of the FTP or TFTP server. For example, if the firmware image file name is image.out and the IP address of the FTP or TFTP server is 192.168.1.168, enter:

```
execute restore image tftp image.out 192.168.1.168
```

The FortiDB system responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 .Type `y`.
The FortiDB system uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

7 .Reconnect to the CLI.

8 .To confirm the new firmware image is successfully installed, enter:

```
get system status
```

Installing FortiDB Firmware

This procedure installs a specified firmware image and resets the FortiDB system to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware version.

To use this procedure, you must connect to the CLI using the FortiDB console port and a RJ-45 to DB-9 or null-modem cable. This procedure reverts the FortiDB system to its factory default configuration.

For this procedure you:

- Access the CLI by connecting to the FortiDB console port.
- Install a TFTP server that you can connect from the FortiDB interface. The TFTP server should be on the same subnet as the internal interface.

Installing Firmware using Boot Loader Menu

This procedure installs a specified firmware image and resets the FortiDB system to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware version.

1. Connect to the FortiDB CLI through your console port.
2. Get and copy your current network settings as your reference, by executing the following command:

```
show
```

Note: After installing a new image, your network settings are reset to the factory defaults. You need to re-configure network settings in order to access to the web-based manager.

3. Make sure the TFTP server is running.
4. Copy the new firmware image file to the TFTP server.
5. Make sure the internal interface is connected to the same network as the TFTP server. To test the connection, enter:

```
execute ping <tftp_ip_address>
```

6. Enter the following command to restart the FortiDB.

```
execute reboot
```

The FortiDB system responds with the following message:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

7. Type `y` to display the boot loader menu.
As the FortiDB system starts, a series of system startup messages is displayed. When one of the following messages appears:

```
Press any key to display configuration menu.......
```

Immediately press any key to interrupt the system startup.

Note: You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiDB system reboots and you must log in and repeat the execute reboot command.

If you successfully interrupt the startup process, one of the following messages appears:

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default
[C]:  Configuration and information
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,C,Q,or H:
```

8. Type `G` to get the new firmware image from the TFTP server.
The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

9. Type the address of the TFTP server and press Enter.
The following message appears:

```
Enter Local Address [192.168.1.188]:
```

10. Type an IP address that can be used by the FortiDB unit to connect to the TFTP server.

The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter firmware image file name [image.out]:
```

11. Enter the firmware image file name (and location) and press Enter.
The TFTP server uploads the firmware image file to the FortiDB unit. Some unit models may display the following message:

```
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
```

12. Type `D`.
The FortiDB unit installs the new firmware image and restarts. The installation might take a few minutes to complete. If the installation is successfully done, you will get the FortiDB CLI prompt.

13. Configure your network settings. To configure your network settings, please refer to *Configuring Network using the CLI.*.

Restoring your Configuration Settings using the CLI

The following steps restore your FortiDB configuration settings using the CLI.

1. Log into the CLI.
2. Enter the following command to copy the backup configuration settings to restore the file on the FortiDB unit:

```
execute restore all-settings <ftp server> <filepath> <username> <password>
 [crptpasswd]
```

Note: This operation will replace your current settings and necessitate a reboot. For details about backup and restore using the CLI, see the All-Settings Backup and All-Settings Restore sections in *FortiDB-Specific Commands*.

3. Use the show shell command to verify your settings are restored, or log into the web-based manager.

Administration

User Management

The User Management page allows you to add, delete users, and enable and disable users. You can display users by roles using the **View By Role** dropdown list.

Columns	Descriptions
Selection	Check or uncheck the checkbox to delete the users, or enable/disable the users.
User Status	•  indicates an enabled user. An account can be enabled at any time by a user who has the Security Administrator role. •  indicates a disabled user. An account can be disabled at any time by a user who has the Security Administrator role. •  indicates a locked user account. An account can be locked after unsuccessful login attempts
User Type	• **Normal** - FortiDB local user, with specified password. • **LDAP** - LDAP user with username only. When LDAP user login, FortiDB will connect LDAP server to authenticate. Define the LDAP server properties in **Global Configuration**first if want to define LDAP user.
User Name	User defined user name
First Name	The user's first name
Last Name	The user's last name
Email Address	The user's email address
Phone Number	The user's phone number
Other	Other information of the user

Adding (or Modifying) a User

This topic describes the task of adding (or modifying) FortiDB users and assigning them certain roles. Each of the built-in FortiDB roles allow your users to perform certain FortiDB operations.

1 .Go to the **User Management** page.

Note: Currently enabled users are marked with a  icon to the left of their User Name. Currently disabled users are marked with a  icon to the left of their User Name.

2 .Select the **Add** button. (or, to modify a user's settings, select the **User Name** of the user whose settings you want to change.)

3 .On the **General** tab of the **Add New User** page (or **User Details** page, if you are modifying an existing user), enter all mandatory items.

Note: Items marked with an asterisk (*) are mandatory.

4 .Select **User Type** - Normal or LDAP. For Normal user, you need input user's Password. For LDAP user, you need configure the LDAP server in **Global Configuration** first.
When choosing a password, use one that follows these rules:

Rule Category	*Description*
Mandatory Length	By default, no mandatory length is set. You can set the length limitation in System Configuration. Please see the Minimum Password Length properties in *System Properties List* .
Mandatory Contents	• At least one number • At least one special character from this set: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./
Prohibited Contents	• Any spaces • User name • User name reversed

Example: `wru2rxy?` is a valid password.

5 .On the **Roles** tab on the **User Details** page, select one or more of the entries in the **Available Roles** list box and add them to the **Assigned Roles** list on the right by selecting on the right-arrow button.

Note: In order to remove role(s) from your user, select them in the **Assigned Roles** list box and select the left-arrow button.

6 .On the **Targets** tab on the **User Details** page, if you want the user to manage specific targets only, choose 'Manage Limited Targets' radio button, select one or more of the entries in the **Available Targets** list box and add them to the **Assigned Targets** list on the right by selecting on the right-arrow button.

Note: In order to remove targets(s) from your user, select them in the **Assigned Targets** list box and select the left-arrow button.

7 .If you want a new user to be initially disabled (and, therefore, unable to login), select the **Set user status as "disabled" immediately** checkbox. (In order to disable an existing user, go to the **User Management** page, select the checkbox to the left of the user(s) of interest, and select the **Disable** button.)

Role-Dependent Privileges

This topic maps the built-in FortiDB roles with their privileges.

Privileges by Role

Once a given role has been assigned to a user, that user can only perform certain FortiDB operations.

The following tables show which privileges are mapped to the roles associated with users.

Table 1 : Privileges by Role

Role	Privileges
Operations Manager	• Review target-database connection information. • Review target group connection information

Role	Privileges
	• View Pre-Defined Policies (PDPs) and User-Defined Policies (UDPs) • View DAM Policies (Data, Metadata, Privilege, and Compliance Policies) • Create, modify, delete, and run assessments • Start/Stop monitoring • View DAM Alerts • Read results of FortiDB-shipped reports • Read results of Custom reports • Perform Penetration Tests • View the Privilege Summary
Policy Manager	• Import/export and enable/disable Pre-Defined Policies (PDPs) for VA • Import/export and enable/disable Metadata, Privilege, and Compliance Policies for DAM • Import/export and enable/disable User-Defined Policies (UDPs) for VA and Data Policies for DAM • Add Policy Groups for VA and DAM • Create, modify and delete User-Defined Policies (UDPs) for VA and Data Policies for DAM
Report Manager	• Review target-database connection information. • Review target group connection information • Review Assessment settings • Read results of FortiDB-shipped reports • Generate DAM compliance reports • Read results of Custom reports • View the Privilege Summary
Security Administrator	• Create, modify, delete, and enable/disable FortiDB users • Configure and modify user-role assignments • View the Entitlement report
System Administrator	• Import/export and enable/disable Pre-Defined Policies (PDPs) • Import/export and enable/disable User-Defined Policies (UDPs) • Archive and restore assessment results • Change system properties • Enable/View Audit trail
Target Manager	• Create, modify, and delete and import/export connections to target databases • Create, modify , and delete target groups • Perform Auto Discovery of target databases • Review Assessment settings • Review the Privilege Summary

Privileges by License Type

Privileges are enabled based on what type of license is being used.The following tables show which privileges are enabled for the different type of licenses.

Table 2 : Privileges by License Type

License Type	Privileges
VA Only	• Policy Manager: View/Modify VA policies • Operations Manager: Create, modify, delete, and run assessments • Report Manager: Generate VA reports • Target Manager: All privileges for this role enabled • System Administrator: All privileges privileges for this role enabled • Security Administrator: All privileges for this role enabled
DAM Only	• Policy Manager: View/Modify DAM policies • Operations Manager: start/stop monitoring, view DAM Alerts, view/edit DAM Alert Groups • Report Manager: Generate DAM reports • Target Manager: All privileges for this role enabled • System Administrator: All privileges for this role enabled • Security Administrator: All privileges for this role enabled
VA and DAM	• All privileges for the different roles enabled

User Management Icon Descriptions

Here are the User Management icon descriptions:

Table 3 : User Management Icon Descriptions

Icon	Description	Comments
	An Enabled user account	An account can be enabled at any time by a user who has the Security Administrator role.
	A Disabled user account	An account can be disabled at any time by a user who has the Security Administrator role.
	A Locked user account	An account can be locked after unsuccessful login attempts

Limited Targets Management

FortiDB user can be defined to manage all targets, or manage assigned target(s) only.

In the **Targets** tab of user add/edit page, you can choose "Manage all targets" or "Manage limited targets".

Once choose "Manage limited targets", you can select available targets to assign to user.

The user with limited targets access, will only be able to manage VA/DAM/Reports of assigned targets.

This target management definition also depends on **Role Privileges**. For example, you need have "Target Manager" role privilege first, to edit any target.

Deleting Users

This topic describes how to delete FortiDB users.

1. Go to the **Users** page.
2. Select the checkbox(es) corresponding to the user(s) you want to delete.

3 . Select the **Delete** button.

Entitlement Report

The Entitlement Report shows you all of your FortiDB users, their account status, and their granted roles.

Columns	Meaning	Description
Status	User status	• indicates an enabled user account • indicates a disabled user account • indicates a locked user account
Username	User defined user name	The user entry in the User Management page is displayed.
First Name	First name of the user	The user entry in the User Management page is displayed.
Last Name	Last name of the user	The user entry in the User Management page is displayed.
Other	Other information about the user	The user entry in the User Management page is displayed.
	System Administrator role	• indicates the user has the System Administrator role. • indicates the user does not have the System Administrator role.
	Security Administrator role	• indicates the user has the Security Administrator role. • indicates the user does not have the Security Administrator role.
	Target Manager role	• indicates the user has the Target Manager role. • indicates the user does not have the Target Manager role.
	Policy Manager role	• indicates the user has the Policy Manager role. • indicates the user does not have the Policy Manager role.

Columns	Meaning	Description
	Operations Manager role	•  indicates the user has the Operations Manager role. •  indicates the user does not have the Operations Manager role.
	Report Manager role	•  indicates the user has the Report Manager role. •  indicates the user does not have the Report Manager role.

Sort: You can sort the Entitlement Report by clicking on any of the column headers. That header is used as your sort key.

 **Note:** The sorted result will be retained when you export the report.

For example, you can sort by **Status**

Export: You can export the Entitlement Report as a PDF, Excel, comma-delimited, or tab-delimited file. Just choose the desired format in the **Export as** dropdown and Select the **Export** button.

Global Configuration

The Global Configuration page allows you to change FortiDB system property values in the following tabs:

Tabs	Description
All	Properties in a read-only manner. You must select one of the other tabs in order to add or change property values
Assessment	Properties related to assessment
Notification	Properties related to Email, SNMP and Syslog
Reporting	Properties related reports generation
User profile/Security	Properties related to user profile and security
Target	Properties for additional JDBC settings for each database type
LDAP Server	Properties related LDAP server for user authentication
Monitor	Properties related Data Activity Monitoring

Changing the System Properties

1. Log in as System Administrator.
2. Go to **Administration** > **System Configuration** of the left-side tree menu.
3. Click one among the following tabs.
   - Assessment
   - Notification

- Reporting
- User profile/Security
- Target

4 .Set the value of the property you want to change.
5 .Select **Save**.

Restoring the Default Values of System Properties

1 .Log in as System Administrator.
2 .Go to **Administration** > **System Configuration** of the left-side tree menu.
3 .Click one among the following tabs.

- Assessment
- Notification
- Reporting
- User profile/Security
- Target

4 .Check the checkbox(es) of the properties you want to restore the default values.
5 .Click the **Restore Defaults(s)** button.
6 .Select **Save**.

System Properties List

This topic presents a list of all the properties that you can configure.

Assessment

Property	Purpose	Possible Values and Default Values
Enable Localhost Auto Discovery	Enables Auto Discovery to be performed on the machine containing the FortiDB application.	`true` or `false`. The default value is false.
Number of Concurrent Assessments	Total number of assessments which can run simultaneously. The optimum value of this parameter depends on your environment but tuning this parameter will affect assessment performance and CPU usage by FortiDB. **Note:**Assuming at least one target database per assessment, the `numberOfConcurrentScans` can never exceed `numberOfConcurrentTargetScans`.	The default value is 5.
Number of Concurrent Target Assessments	Total number of target-databases that can be assessed simultaneously during the `numberOfConcurrentScans` assessments. The optimum value of numberOfConcurrentTargetScans depends on your environment but tuning this parameter will affect assessment performance and CPU usage by FortiDB. **Note:**Assuming at least one target database per assessment, the	The default value is 20.

Property	Purpose	Possible Values and Default Values
	`numberOfConcurrentScans` can never exceed `numberOfConcurrentTargetScans`.	
SSH Key File (Appliance only)	The file that contains the private key used for all SSH connections. Oracle OSVA and DB2 only. The **Browse** button allows you to locate and set your SSH key file. After setting your key file, select the **Save** button. **Caution:**If you select Restore Default(s) and then Save button, your key file that you set will be deleted. Please keep your own copy of the file in a safe place.	There is no default key set in the appliance. The private key file type, RSA or DSA, can be uploaded. Any uploaded key files will be renamed as id_rsa or id_dsa, depending on the type of key that was uploaded. If you uploads a key file and a key file already exists in the appliance, the old key will be replaced with the new key.
MSSQL Server Level Exclusions	A comma separated list of the databases that will be skipped when a "Server Level" scan of a MS SQL target is done.	model,tempdb,pubs, msdb,Northwind
Sybase Server Level Exclusions	A comma separated list of the databases that will be skipped when a "Server Level" scan of a Sybase target is done.	model,tempdb,pubs2, pubs3,jpubs,sybsyntax, sybsecurity,sybsystemdb, sybsystemprocs
Enable Pen Test	When set to `true`, the Pen Test capability is enabled. When set to `false`, which is the default, the Pen Test capability is disabled.	`true` or `false`. The default value is `false`.
Enable Pen Test For All Users in Database (Standalone only)	When set to `false`, FortiDB uses the user names in <dbtype>user.txt, where dbtype represents the target-database type and is one of these strings: • ora for Oracle • sql for MS-SQL • db2 for DB2 UDB • syb for Sybase • mysql for MySQL When set to `true`, FortiDB ignores the user names in <dbtype>user.txt.	`true` or `false`. The default value is `true`.
Pen Test Method	The Login method actually logins in to your target databases. **Caution:**Be careful when using this method. Since its login attempts may be unsuccessful, it can result in preventing any,	• 1=Login method • 2=Hash-based method • 3=Hybrid

Property	Purpose	Possible Values and Default Values
	even approved, users from logging in to your target database. The Hash-based method is a safer, offline approach, but is available for only Oracle and MS SQL target databases. (A 'hash' is the value obtained after encrypting a clear-text string.) With the Hybrid method, FortiDB attempts the best available method. If the hash-based method is available, as will be the case with Oracle and MS-SQL targets, FortiDB uses it.	The default value is `Hybrid`. (If you select the Hash-based method for Sybase or DB2 targets, none of the Pen Test rules will be applied, your assessment result will be essentially empty, and no error will be signaled.)
Pen Test Password Dictionary	A file containing the passwords to be checked when executing the Dictionary Penetration test. The **Browse** button allows you to select your dictionary file. You need to select the **Save** button to complete your selection.	"Built-in Dictionary" indicates that the default dictionary is being used. "User Dictionary" indicates that you have uploaded your own dictionary file. The filename of the dictionary you upload will not appear here. **Note:**When you restore the default dictionary by checking the checkbox, and selecting **Restore Default(s)** and then **Save**, your dictionary file will be deleted from the system.

Notification

Property	Purpose	Possible Values and Default Values
Email Server Host Name	The SMTP email server hostname or IP address. Email notifications cannot be sent when the (empty) default value for this property is used.	
Email Server Port	The server port number associated with `emailServerHostName`.	The default value is 25.
Email Server User Name	The user name associated with `emailServerHostName`. Need input the user and password, if the email server need authentication to send email, and leave empty if doesn't.	
Email Server Password	The password associated with `emailServerHostName`.	

Property	Purpose	Possible Values and Default Values
From Address	The email address used to fill the 'From' field in email notification.	
SNMP Community String	The SNMP community name.	The default value is `public`.
SNMP Receiver Host	The SNMP receiver host. SNMP-trap notifications cannot be sent when this field is empty.	
SNMP Receiver Port	The SNMP receiver port number.	The default value is `162`.
Syslog Receiver Host	The Syslog receiver host. Syslog notifications cannot be sent when this field is empty.	
Syslog Receiver Port	The Syslog receiver port number.	The default value is `514`.

Reporting

Property	Purpose	Possible Values and Default Values
Company Logo	Location and name of file containing your company's logo. When you locate and specify a new image via the **Browse** button and then save it via the **Save** button, it will be placed in *<FortiDB-install directory>/conf/reportlogos* for subsequent use in your reports.	
Company Name	The company name to be displayed on VA reports.	Fortinet
DAM Report Encoding	The charactor encoding used for DAM report generating.	UTF-8

User Profile/Security

Property	Purpose	Possible Values and Default Values
Idle Account Expiration	The number of days a user can be inactive after which the account expires.(This does not apply to the FortiDB superuser, `admin`.) An expired account is “locked” and can be unlocked by a user with Security Administrator privileges.	The default value is -1.
Max Number of Failed Login Attempts	The number of login attempts allowed before user account is locked. (This does not apply to the FortiDB superuser, `admin`.)	The default value is -1.

Property	Purpose	Possible Values and Default Values
Days Until Password Expiration	The number of days after which an unchanged password expires.	The default value is -1.
Minimum Password Length	The minimum length of a user password.	The default value is -1.
Enable Local Audit Trail	Enables or disables FortiDB local Audit Trail. When set to true, Audit Trail is enabled. When set to false, Audit Trail is disabled.	The default value is `false`.

Target

Property	Purpose	Possible Values and Default Values
Additional Oracle JDBC Settings	List of additional key=value pair(s), separate by semicolon, for all database connections of the same type.	
Additional SQL Server JDBC Settings	List of additional key=value pair(s), separate by semicolon, for all database connections of the same type.	If you use NTLM v2 authentication, enter `useNTLMv2=true` If need force to use SSL encryption, enter `SSL=require`
Additional Sybase JDBC Settings	List of additional key=value pair(s), separate by semicolon, for all database connections of the same type.	See below note for using Encrypted Password connection
Additional DB2 JDBC Settings	List of additional key=value pair(s), separate by semicolon, for all database connections of the same type.	
Additional MySQL JDBC Settings	List of additional key=value pair(s), separate by semicolon, for all database connections of the same type.	

Note: If use Sybase Encrypted Password connection (set the 'net password encryption reqd' to 1 or 2 in Sybase server), enter:

```
ENCRYPT_PASSWORD=true;
RETRY_WITH_NO_ENCRYPTION=true;
JCE_PROVIDER_CLASS=org.bouncycastle.jce.provider.BouncyCastleProvider
```

LDAP Server

Property	Purpose	Possible Values and Default Values
Server Name/IP	LDAP server name or IP address.	

Property	Purpose	Possible Values and Default Values
Port	LDAP server port.	389
Common Name Identifier	Name of user identifier in LDAP user path.	If the user path is like "cn=username,ou=dept,dc=com", this value should be "cn". If the user path is like "un=username,ou=dept,dc=com", this value should be "un".
Distinguished Name	Distinguished name of LDAP user.	For the user with path "cn=username,ou=dept,dc=com", this value should be "ou=dept,dc=com".
Bind Type	LDAP authentication type.	`none` or `Simple`, default is `Simple`.

Monitor

Property	Purpose	Possible Values and Default Values
Sniffer Audit Log Keep Duration	Days for storing sniffer audit log data.	30 or empty (FortiDB will use 30 days as default value if this setting is empty)

Archive and Restore

This topic describes the FortiDB archiving and restoring process and gives some guidelines for its use.

All data for assessment and monitoring/auditing in the FortiDB repository can be moved to archive files in order to conserve repository space and improve performance. There are three types of dataset archived and restore.

- Assessment data
- Alert data
- Auditing data

When data is archived, the information is exported to a file. When data is restored, the information is imported in FortiDB repository. You can choose whether you want to delete the archived file after restoring, or keep it by the Delete archive file after restore checkbox.

FortiDB archives are stored within encrypted files. Depending upon your assessment or monitoring frequency and upon the number and type of policies and target databases involved, the files can consume a large amount of space. So, you could move the files to a separate location and then move them back when needed.

Note:

If you want to report on an archived data, you need to restore the archive containing that data.

If you delete a completed assessment's configuration settings after archiving, that information cannot be restored. For example, if you delete a target-database connection after archiving its assessment information, that information cannot be restored.

The entry in the **Timestamp** column on **Restore** tab represents the day and time that the archive was performed.

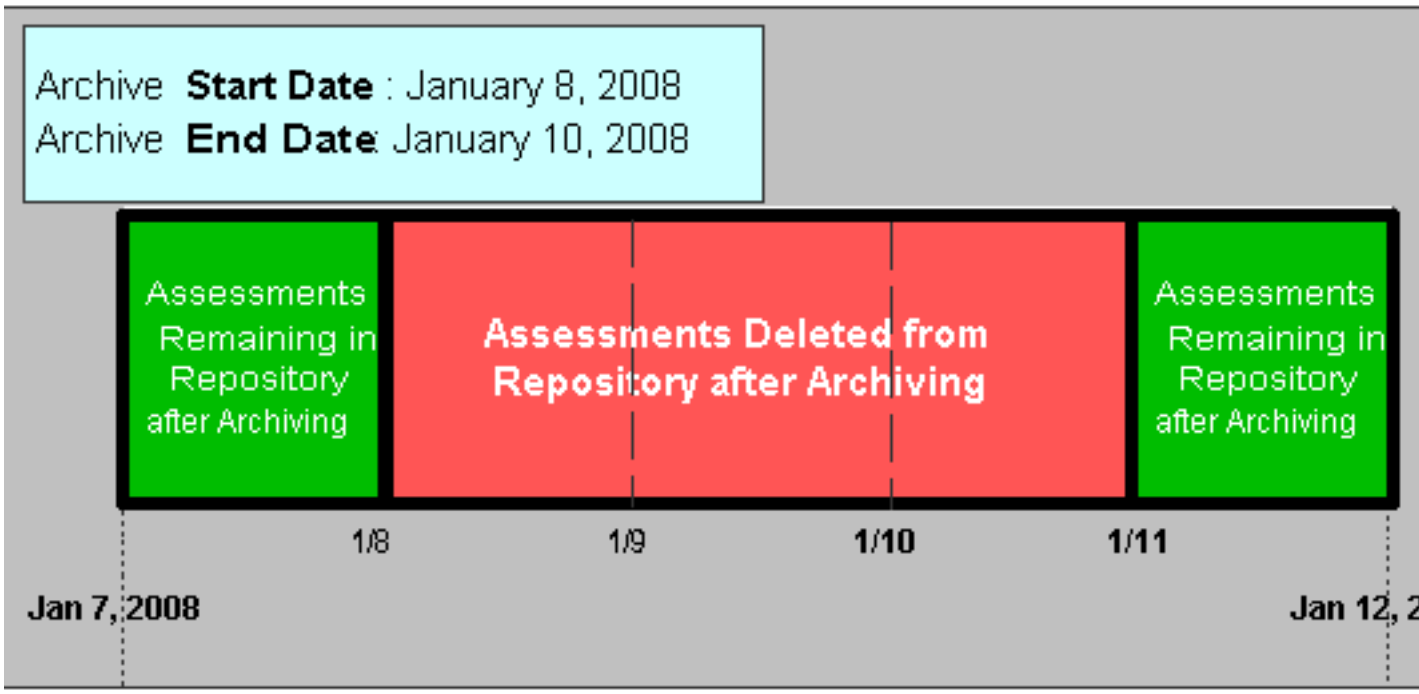
Once restored and in order to prevent duplicate records in the FortiDB repository, any records already in the FortiDB repository will not be restored again during the restore process.

About Archiving

This topic illustrates the effect of archiving on the contents of your repository and describes a possible archiving strategy.

Effect of Archiving

The following figure illustrates the effect of an archive whose start date is January 8, 2008 and whose end data is January 10, 2008.



An Archiving Strategy

Depending upon your data volume, you should decide on an archive strategy and frequency. You should also decide if you want your archive to commence immediately or not.

For example, assume you decide to keep no more than four months worth of data in your FortiDB repository at any given moment. In this case, you might wait four months after installing FortiDB before you first archive. Then specify (in the **Archive Period** field of the **Archive** tab) "3 Month(s) and older".

Three months worth of data would then remain in your repository.

You could either run a "3 Month(s) and older" archive manually every month or automate the process by scheduling it to occur at a prescribed interval or on a certain day of the week or month.

Archiving Immediately

This topic describes how to archive data immediately. To archive immediately, take the following steps:

1. Go to **Administration** > **Archive/Restore** of the left-side tree.
2. Select the **Archive** tab.
3. Specify a start and end date for your archive. The date ranges 0:00 am to 0:00 am of the next date.

Note: The archive includes data which starts from 0:00 am of the start date, and ends 0:00 am of the end date you specify.

4 .Select the **Archive Now** button.
You should then see "`Archiving Completed`" message in the **Status** area in the upper-right corner of the page.

Scheduling an Archive

This topic describes how to archive data via a schedule. To schedule archiving, take the following steps:

1 .Go to **Administration** > **Archive/Restore** of the left-side tree menu.
2 .Select he **Archive** tab.
3 .In the **Archive period** section, specify the archive period for which you want to archive data. Here you can specify the number of days, weeks, or months, prior to the current date, that you want as the last date for data in the archive.
For example: "3 Month(s) and older" would result in an archive that contained results for all assessments, and monitoring/auditing except those run in the last 3 months
4 .In the **Run time** section, specify a **Start at** time or, in the **Recurrence pattern** section, specify either the **Hourly**, the **Daily**, **Weekly**, or **Monthly** radio button.

- If you choose the **Hourly** radio button, you can then specify the hourly interval in the **Every __ hours** field.
- If you choose the **Daily** radio button, you can then specify the daily interval in the **Every __ days** field.
- If you choose the **Weekly** radio button, you can then specify the weekly interval in the **Every __ week(s) on** field. You should then specify on which day(s) of the week you want to run your archive by selecting one or more of the appropriate day checkbox(es).
- If you choose the **Monthly** radio button, you can then specify which day during the month and which months during the year you want your archive to run. There are checkboxes for you to specify in which months you want to run your assessments. The **Day** radio button and adjacent dropdown list allows you to specify the numeric day for your archive to run in each specified month. Alternatively, you may specify the day in each month, such as the 'first Monday', using the two dropdown lists.

5 .If you want your schedule to go into effect immediately, select the **Enable Auto Archive** check box.
6 .Select the **Save Schedule** button.

Restoring the Archived Data

This topic describes how to restore the archived data.

1 .Go to **Administration** > **Archive/Restore** of the left-side tree menu.
2 .Select the **Restore** tab.
3 .Select the radio button next to the archive file of interest.
4 .(Optionally) Select the **Delete archive file after restore** checkbox if you want the archive file to be deleted after a successful restoration.
5 .Select the **Restore** button.
You should then see "`Restoring Completed`" message in the **Status** area in the upper-right corner of the page.

Note: If an error occurs during the restoration of any records, the containing archive file will not be deleted -- even if the **Delete archive file after restore** checkbox was selected.

Local Audit Trail

This topic describes FortiDB's Audit Trail feature. This feature allows you to capture the following information:

- All users activities: add/delete/update users, add/delete/update policies or policy groups, add/delete/update targets or target groups, add/delete/run assessments, archive, restore, log on, and updates in system configuration.
- System activities: start and stop.

You can filter audit trail records for display by dates in the audit trail page. You can also export the list to a tab-delimited text which you can open from any spreadsheets application.

Notes: To display the audit trail, the user must have a Administrator role.

Columns	Descriptions
Timestamp	The date and time of the action that was taken place.
Action	The action that was taken place.
By	The user who took the action. For example, admin, any specific users, or internal.  **Note:** When the actions are invoked by FortiDB such as scheduled scan, scheduled archive, start FortiDB, or stop FortiDB, this column shows “internal”.
Location	The location where the action was taken place. For example, locally or from any specific location, shown as IP address or host name of the login user.  **Note:** When the actions are invoked by FortiDB such as scheduled scan, scheduled archive, start FortiDB, or stop FortiDB, this column shows “internal”.
Object Name	The object which the action was taken place against.

Audit Trail Examples

```
Timestamp:2009-02-26 16:06:47
Action: Update
By: admin
Location: 172.30.63.50
Object Name: VA Policy: DVA IBM DB2 UDB 02.11 Latest Fixpak not installed
---------------
Timestamp:2009-02-26 15:36:31
Action: Scan
By: jsmith
Location: 172.30.63.40
Object Name: VA Scan: Latest Patch Policies

----------------
```

```
Timestamp:2009-09-09 15:02:25
Action: Add
```

```
By: admin
Location: 172.30.63.50
Object Name: DAM Policy Group: tablePolicy1_2 Group
---------------
```

Enabling Audit Trail

1. Log in as System Administrator.
2. Go to **Administration** > **System Configuration** of the left-side tree menu.
3. Select the **User Profile/Security** tab.
4. Set the value of **Enable Audit Trail** to `true`.
5. Select **Save**.

Filtering Audit Trail

This topic explains how to filter the audit trails.

1. Select the **Audit Trail** link in the **Administration** section of the left-side tree-navigation menu.
2. Enter a start date in the **Start Date** field and an end date in the **End Date** field or click the calendar icon and select dates.
3. Select the **Apply** button to display the audit trail records within the range of the period you selected in the step 2. A list of audit trail records is displayed in a chronological order.
4. Optionally, you can sort the list by clicking on any of the column headers. The header is used as your sort key.
5. To export the audit trail list to a tab-delimited text file which will be understood by any spreadsheets application, select the **Export** button.

Deleting Audit Trail

This topic explains how to delete the Audit Trail list.

1. Go to the **Audit Trail** link in the **Administration** section of the left-side tree-navigation menu.
2. To filter audit trail records that you want to delete, enter a start date in the **Start Date** field and an end date in the **End Date** field, or click the calendar icon and select dates.
3. Select the **Apply** button to display the audit trail within the range of the period you selected in the step 2. A list of audit trail is shown.
4. Select the **Delete** button to delete the list.

Note: Once you delete a list, the data is not retrievable. We recommend you save data by exporting to a file before deleting.

Target Management

Manage Target Database

For assessment or monitoring of your target databases, you first need to create target-database connections. From the Targets page, you can organize all target databases you want to perform assessment or monitoring. The following table describes columns, buttons, and icons used in the Targets page.

Columns	Descriptions
Status (Connection status)	•  indicates a target database for which the information is incomplete •  indicates a target database for which the information is complete
Status (Monitoring Status)	•  indicates the target has not been initialized for monitoring. The user must go to Data Activity Monitoring > Monitors, and open the target and click Test and Save button. •  indicates the target is not monitored. •  that monitoring is starting •  indicates that monitoring is stopping. •  indicates the target is being monitored but some of the policies could not be configured. •  indicates that monitoring is active. •  indicates that monitoring is not running. An attempt to start the monitor failed. •  indicates that the FortiDB is has disconnected from the agent. The target has not received a heartbeat from the remote agent. To fix this state, start the agent. The agent will automatically connect to FortiDB. You do not need restart monitoring.
Name	User defined target connection name. When clicked, the target connection page (General tab) displays.
DB Name	Database name of your target database
DB Host Name/IP	Database host name or IP address of your target database machine
Port	Port number to use for the target connection

Columns	Descriptions
DB Type	Database type of your target. ORACLE, MSSQL, DB2, SYBASE, or MYSQL

Buttons and Fields

Buttons and Fields	Descriptions
View dropdown	Filters a display of the target list
Search / New Group	Search the target by column's filtering, or create a new group with search criteria
Add	Add a new target
Delete	Delete the selected target
Import	Import a target list file from exported XML file
Export selected to XML	Export selected targets to XML file
Export all to XML	Export all targets to XML file
Export all to PDF	Export a target list to PDF file

Adding (or Modifying) a Target Connection

This topic describes the task of creating or modifying target-database connections.

1. Go to To **Target Management** > **Targets**
2. Select the **Add** button. (or, to modify a target, click on the name of the target database you would like to change.)
3. In the **General** tab of the **Target** page, enter the requested information, taking the following items into consideration.
   - In the **Name*** field, do not use spaces for the name.
   - In the **Type*** field, if you choose Oracle or DB2, you may then need to fill out information on the **SSH** tab.)
   - In the **DB Host Name/IP*** field, enter the DB host name or IP address of the machine containing your target database.
   - In the **Port*** field, enter the port number or keep the default for your target database.
   - For MS SQL or Sybase only, check the appropriate **Database Level** or **Server Level** radio button in the **Connect At** field. If you select **Server Level** scan, you can exclude databases you specified using MSSQL Server Level Exclusions property and Sybase Server Level Exclusions property values. For details, see *System Properties List*
   - 

     Note:

     FortiDB supports SSL encrypted connection to MS SQL Server.

     FortiDB will connect SQL Server with encrypted connection if set "ForceEncryption=Yes" in SQL Server, and connect with no encrypted connection if "ForceEncryption=No".

     Input value "SSL=require" in *Additional JDBC Settings* if want force FortiDB to use encrypted connection.
   - In the option **Data Activity Monitoring**, enable the checkbox "Allow" if you want monitor the target.
   - If you are connecting to a DB2 target, must specify the **Retrieval Method** in the DB2 Options tab.

DB2 Retrieval Method	*Comments*
SSH	See *SSH Connections for Oracle and DB2*
***db2level* command**	This method requires that you specify: • The output of the *db2level* command or the name of a text file containing that output. • The output of the *get dbm cfg* command.
User SQL query for connection	This method requires DB user has privilege of executing stored procedure. Use this method, FortiDB will get necessary information for target definition from DB2 server through SQL query.

4 .(Optionally) you may select the **Classification** and **Contact Info** tabs of the **Database Form** and enter the information there.

Note: Entries made here may be useful as filtering criteria for subsequent grouping of your targets.

5 .(Optionally) in order to test your connection, select the **Test Connection** button after you have specified all the required information.

6 .Once you have specified your target information, you can save it by selecting the **Save** button.

SSH Connections for Oracle and DB2

FortiDB allows you to connect to Oracle and DB2 target databases using SSH.

FortiDB offers these SSH access methods:

- **Password** method which utilizes just a user name and password.
- **Implicit Key Pair** method which uses SSH key file entered through the SSH Key File property value. For details about SSH key file property and how to set your SSH key file, see *Using SSH Target-Database Connections*.
- **Explicit Key Pair** (Standalone only) which assumes:
  - That your private key resides in the directory named *.ssh* under the directory in the Key Path field
  - That you will enter a pass phrase that is a part of your private key

Using SSH Target-Database Connections

This topic describes the task for using SSH in order to connect to target databases.

1 .Select the **SSH** tab.

2 .Specify a port number or use the default of 22.

3 .Specify an access method among the choices.

Note: The Explicit Key Pair option is for standalone users only.

Access Method	*Associated Information*
Password	Enter appropriate values into the **User Name** and **Password** fields.
Implicit Key Pair	Enter just a **User Name**. FortiDB will use the SSH key file entered through the SSH Key File property value. To set your SSH key file:

Access Method	*Associated Information*
	1 . Select **System Configuration** in the left-side navigation menu. **2 .**Select the **Assessment** tab. **3 .**Select **Browse** button in the SSH Key File property and locate your SSH private key file. **4 .**Select the **Save** button. **Note:** When **User Name** is empty, FortiDB will use the name of the user that started FortiDB.
Explicit Key Pair (Standalone Only)	Enter: • A **User Name** for the FortiDB SSH user • A **Key Path** which represents the location, on your SSH client machine, of your private key. You need to create ./ssh directory under the directory shown in this field and copy the private key in ./ssh directory you created. • (Optionally) a **Pass Phrase** FortiDB will attempt to use the private key (and, if specified, pass phrase) located in **Key Path** location at run time.

4 . Select the Test SSH Connection button to check if the connection has been established.

SSH Environment (for standalone users)

You must have a working SSH environment by which you can remotely login to different target-database machines. (See your System Administrator if you need help setting up a working SSH environment.) Here are some items to consider:

Item	Description
Public Key handling	For either the Explicit or Implicit Key Pair methods, you must secure-copy the public key, which you generate on the SSH client. Secure-copy it to your SSH server and then append it to the a*uthorized_keys* file located in the *.ssh* directory within the home directory of the FortiDB SSH user.
Private Key handling	For either the Explicit or Implicit Key Pair methods, you should generate *id_dsa* or *id_rsa* private keys and copy them to the *.ssh* directory under user's home directory on the SSH client machine. In a Windows environment, depending on Operating systems, the private key should resides in /.ssh directory under user's home

Item	Description
	directories, such as C:\Documents and Settings\All Users. In order to place the private key, take the following steps: 1 .Select the **SSH** tab from the Target page. 2 .Select **Explicit Key Pair** in the **Access Method** field. The user's home directory is shown in the Key Path field. 3 .Create ./ssh directory under the directory shown in the **Key Path** field. 4 .Copy the private key to ./ssh directory you created.
SSH Client Location	The SSH client should be on your FortiDB machine.
SSH Server Location	The SSH server should be on your target-database machine.
User account for SSH User	You must create a user account on your target-database machine for the FortiDB SSH user.

DB2 Target Specific Instructions	For DB2 targets, you may need to execute, for the OS user that you created for FortiDB on your target-database machine, the following. For example, if you are the `db2inst3` user and you use the *bash* shell, add this to your *.bashrc*:
	`if [ -f /home/db2inst3/sqllib/db2profile ]; then`
	`  . /home/db2inst3/sqllib/db2profile`
	`fi`

Using the OSVA Feature with Oracle Targets	If you are using the FortiDB OSVA feature for Oracle target databases on Solaris platforms, you will need to specify the **Home Directory**, **Owner**, and owner's **Group** of your target database.

Enabling OS-Level PDP (Solaris, AIX)

This topic describes how to enable OSVA Pre-Defined Policies for Oracle target database on Solaris or AIX machine. In order to be able to run OS-Level PDPs against Solaris or AIX target machine, make sure that your SSH connections have been established. The steps to enable OS-Level PDP are:

1 .Select the **Enable OSVA** check box.
2 .Select **Solaris** or **AIX** for the operating system from the pull-down list.
In your target machine, make sure the environment variable includes "opatch" command path.
3 .Enter Oracle home directory. The $ORACLE_HOME environment. Ask your Oracle DBA for this information.
4 .Enter Oracle Owner name. Ask your Oracle DBA for this information.
5 .Enter Oracle User Group name (Typically dba or oinstall). Ask your Oracle DBA for this information.

6 .Select the Save button.

Additional JDBC Settings

FortiDB uses JDBC to connect target database, you can specify additional JDBC settings for particular connection need.

Specify Additional JDBC Settings

Goto **Administration** > **Global Configuration** > **Target**, input the Value for specific type of database.

Please note that the setting will apply to all targets belong to same type.

Specify JDBC Setting for MS SQL Server to force using SSL encryption

When SQL Server sets the "ForceEncryption=No" and want to FortiDB connect SQL Server with SSL encryption, input following value for SQL Server JDBC Settings:

```
SSL=require
```

Specify JDBC Setting for Sybase connection with "Encrypted Password" option

For Sybase "Encrypted Password" option (set the 'net password encryption reqd' to 1 or 2 in Sybase server), need input following value for Sybase JDBC Settings:

```
ENCRYPT_PASSWORD=true;RETRY_WITH_NO_ENCRYPTION=true;
JCE_PROVIDER_CLASS=org.bouncycastle.jce.provider.BouncyCastleProvider
```

Deleting Target Database Connections

This topic describes how to delete target-database connections.

1 .Go to **Target Management** > **Targets**.
2 .Select the checkbox(es) corresponding to the **Name**(s) of the target-database connection(s) you want to delete.
3 .Select the **Delete** button.

Exporting Target Database Data

This topic describes how to export target-database information.

- Click **Export All** button to export all targets information to a XML file.
- To export select target(s):
  - Change target group with **View** dropdown list, or use **Search/New Group** button to search target(s)
  - Select target(s) with checkboxes, click **Export** button to export.
- Click **Export All to PDF** button to export targets list to a PDF file. Please note that the exported PDF contains parts of target information only, cannot used for importing.
- After click export button, a dialog box will help you to choose a directory in which you can save the file to your disk.

Importing Target Database Data

This topic describes how to import target-database information.

1 .Prepare an XML file containing target-database information you want to import. In order to help insure that your file will import successfully, consider:
  - Export your target-database information from an existing FortiDB machine in order to provide you an example of a file that should import properly. For standalone users, you can use one of the example

files in <*FortiDB-install directory*>/etc/import-target as an example of a file that should successfully import.

- For element values, consider that:
  - Your new target names should be unique. If you import a target with the same name of the existing target, the existing target-database information will be updated by that in the imported file.
  - You need to populate all required elements. If your imported XML file does not have values for all required elements, an Incomplete status will be indicated in the (target-status) column.
  - Do not change any encrypted values. For passwords, use clear text which, in turn, will be encrypted during Import.
  - Do not change the Database Type element value.

2 .Go to **Target Management** > **Targets** of the left-side tree menu.

3 .Select the **Import** button.
The **Target Import** page should display.

Note: Target database data is imported based on the **Name**. If the same **Name** already exists in the target list, the existing target-database data in the target list will be overwritten by the imported data.

4 .Enter the path to the XML file you want to import, or select the **Browse** button and select the XML file you want to import.

5 .Select the **Import** button. Here are the column descriptions:

Columns names	Description
Name	Contains the value of the <name> element is shown.
Results	Indicates whether the imported targets are New, Updated, or Failed.
Complete	Contains Complete or Incomplete. Incomplete means that one or more required elements have a missing value.
Message	Indicates the reason that the Results column shows Failed.

6 .Select the **Continue** button to complete the import.

Target Groups

The Target Groups page shows all pre-defined target groups.

There are the following pre-defined target groups.

- DB2 Database Group
- MySQL Database Group
- Oracle Database Group
- MS SQL Server Database Group
- Sybase Database Group

In this page you can:

- Add a new target group by selecting **Add**. See *Adding a Target Group*
- Modify the target group by selecting the group name.
- Delete the user-defined target groups by selecting the group and click **Delete**.

Adding (or Modifying) a Target Group

This topic describes the task of creating target-database groups by using filtering criteria.

1. Go to **Target Management** > **Targets** in the left-side tree menu.
2. Click the **Add** button to add a new target group. (or, to modify a target group, click the name of the target-database group you would like to change.)
3. On the subsequent **Targets** page, fill in the text boxes
   a) Use the **Group Name** text box for entering (or modifying) a name that will show up in the saved target-group list. Use the optional **Description** text box to describe your filtering/grouping criteria.
   b) In order to create a filtering condition, select a **Column** on which you would like to filter, an **Operator** that associates the **Column** with a **Value**, and a **Value** that the **Column** must match.

   Note: The value you enter in the Value box is case-sensitive.

   c) In order to cancel a target-database grouping operation, click the **Cancel** button.
   d) You can add or subtract filtering-criteria rows by selecting the **+ (plus)** or **- (minus)** buttons, respectively.

   You may add additional criteria by adding rows to the **Column/Operator/Value** table. Multiple rows represent additional criteria.

   Note: You cannot use the same **Column** in multiple rows. For example, you cannot establish a criteria that includes a row for Location = 'London' and a row for Location = 'New York'.

   Here are some examples of filtering criteria:

   Table 4 : Filtering Criteria Examples

Attribute	Operator	Value	Return Possibilities
Location	Contains	nd	all databases in Lo*nd*on
Database Type	Equals	DB2	all DB2 databases

4. Select **Apply** to test your filtering criteria.
5. Select the **Save Group** button to save your new group.
   Your new group will be displayed in the **Target Groups** page.

Deleting Target Groups

This topic describes how to delete target-database groups.

1. Go to **Target Management** > **Target Groups**.
2. Select the checkbox(es) corresponding to the **Name**(s) of the target-database group(s) you want to delete.
3. Select the **Delete** button.

Required Settings for Monitoring Target Databases

In order to properly monitor your target databases and generate alerts, you need to configure your target databases before starting monitoring. Depending upon your target databases, different settings are necessary. For details about required settings of each target database type, see the following sections.

- *Configuring Monitoring with TCP/IP Sniffer*
- *Configuring the Oracle Target Database*
- *Configuring the MS SQL Server Target Database*

- *Configuring the Sybase Target Database*
- *Configuring the DB2 Target Database*
- *Configuring the MySQL Target Database*

Configuring Monitoring with TCP/IP Sniffer

FortiDB appliance supports monitor data activity through TCP/IP sniffer, with Oracle, MS SQL Server, DB2 and Sybase.

Environment Required for TCP/IP Sniffer

- Your target database server and clients use TCP/IP as protocol, and all database activities are going through LAN.
- The network switch, which your target database server is connected, must support the port mirroring feature.
- Connect one Ethernet port of FortiDB appliance to the mirror port (also known as SPAN port) of switch, which database server is connecting to.

Configure FortiDB for TCP/IP Sniffer

- Define the target database first, and make sure the **Allow** option for **Data Activity Monitoring** is checked.
- Configure the Target Monitor, select **TCP/IP Sniffer** for Collection Method, in General tab.
- Select your target database version. Following is the supported database versions.
  - Oracle: 9i, 10g, 11g
  - MS SQL Server: 2000, 2005, 2008
  - DB2: UDB 9.1, 9.5, 9.7
  - Sybase: ASE 12.5, 15.0, 15.5
- For MS SQL Server, if server enabled SSL encryption connection, need specify the **SSL Certificate Private Key** and **Key Password**(if have) for FortiDB. The SSL Certificate is configured in server side for SSL encryption
- Specify which FortiDB's Ethernet port is connecting to network switch for sniffer.
- Enable **Save Sniffer Audit Log**, if you want to logs activity event for auditing. Sniffer log will be kept 30 days by default. Go to **Administration > Global Configuration > Monitor**, change **Sniffer Audit Log Keep Duration** for how many days to store the log data.

Configuring the Oracle Target Database

This topic describes required settings of Oracle databases. To monitor the Oracle target database, FortiDB provides several methods that users can choose depending on their circumstances.

Collection Methods

FortiDB collects Oracle audit information using the following methods:

Note: When you change a collection method from one option to the other, you need to stop monitoring first, and after changing the collection method, start monitoring.

Collection Methods (dropdown list)	Values of the Oracle audit_trail parameters	Required Agent?
TCP/IP Sniffer	None	No See *Configuring Monitoring with TCP/IP Sniffer* for detail
DB, EXTENDED	DB, EXTENDED	No
DB, EXTENDED	DB	No

Collection Methods (dropdown list)	Values of the Oracle audit_trail parameters	Required Agent?
		For Oracle 9i only. Please see the notes below for limitation of this method.
XML File Agent	XML, EXTENDED	**Yes** FortiDB's XML file agent provides high performance for auditing the Oracle target database. To use the XML file agent option, you need to run the FortiDB XML file agent in your target database. For details about how to run the Oracle XML file agent, go to *Running the Oracle XML File Agent*
SGA Agent	None	**Yes** FortiDB SGA agent utilizes the Oracle System Global Area (SGA), a group of shared memory areas, dedicated to an Oracle instance. FortiDB allows users to collect data via the SGA agent from your target database. The FortiDB SGA agent requires less performance overhead, and the database-side configuration is not necessary. For your Oracle target database, EZCONNECT parameter allows the FortiDB agent to connect to the Oracle database by specifying the connection strings: hostname[or IP]:portnumber/SID. To add EZCONNECT parameter, take the following steps: **1 .** Go to $ORACLE_HOME/network/admin/sqlnet.ora **2 .** Open sqlnet.ora with your editor. **3 .** Add EZCONNECT parameter as follows: `NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)` For the SGA agent option, you must run the FortiDB SGA agent in your target database. For details about how to run the SGA agent, go to *Running the Oracle SGA Agent*
Net Agent	None	**Yes** FortiDB's Net agent collects data activities to Oracle target database through TCP/IP. To use the Net agent option, you need to run the FortiDB Net agent in your target database. For details about how to run the Oracle Net agent, please refer the document released with FortiDB Net Agent.

Note: Limitation of using method 'DB' for Oracle 9i

1 .Table and Table Column Policy - Cannot retrieve the SQL statement text
2 .Table/User/Session Policy - No effect with Suspicious Location rule
3 .Session Policy - No effect with Extremely Long Session rule and High Read Ratio rule

Target Preparation for the Compliance Policy

FortiDB Compliance Policy allows you to capture all types of activities and stores the data in the internal repository. To generate Compliance reports properly, you need to execute "create trigger" commands.

Take the following steps in your Oracle target database:

1 .Copy the following scripts in a file.

```
CREATE OR REPLACE TRIGGER FORTIDB_get_application AFTER LOGON ON DATABASE
WHEN (user != 'SYS')
DECLARE l_program VARCHAR2(50);
l_machine VARCHAR2(50);
BEGIN
SELECT substr(program, 1, 43), substr(machine, 1, 20) INTO l_program,
l_machine FROM v$session
WHERE audsid = sys_context('USERENV','SESSIONID');
dbms_session.set_identifier(l_program || ':' || l_machine);
EXCEPTION WHEN OTHERS THEN ROLLBACK;
END;
/
```

2 .Login as sys as sysdba to your Oracle instance.
3 .Execute the file.

User Privileges for Monitoring/Auditing

In order to monitor/audit the Oracle target databases, the database users must have the following privileges:

Data Policies	Privilege Policies	Metadata Policies
For Collection Method 'DB, EXTENDED' and 'XML File Agent' • CREATE SESSION • SELECT_CATALOG_ROLE • DELETE_CATALOG_ROLE • AUDIT ANY • AUDIT SYSTEM • SELECT SYS.AUD$ • SELECT on the monitored tables or SELECT ANY TABLE **For Collection Method 'TCP/IP Sniffer', 'SGA Agent', 'Net Agent'** (Privileges need for browsing database to define data policy) • CREATE SESSION • SELECT_CATALOG_ROLE	• CREATE SESSION • SELECT_CATALOG_ROLE • DELETE_CATALOG_ROLE • AUDIT SYSTEM	• CREATE SESSION • SELECT_CATALOG_ROLE for use with auditing: • CREATE SESSION • AUDIT SYSTEM • SELECT_CATALOG_ROLE

Data Policies	Privilege Policies	Metadata Policies
• SELECT on the monitored tables or SELECT ANY TABLE		

To grant privileges to a user, use the GRANT statement. Some examples are:

```
GRANT SELECT_CATALOG_ROLE TO username
GRANT DELETE_CATALOG_ROLE TO username
```

Enabling FortiDB to Delete Audit Records

To enable FortiDB to delete audit records from the SYS.AUD$ table you must give the FortiDB user delete privileges on the SYS.AUD$ table. This privilege should only be granted to the FortiDB user if you understand the implications. The SYS.AUD$ contains all audit records not only the audit records generated for FortiDB monitoring. When FortiDB delete audit records it deletes all audit records. See Audit Management for more information regarding the delete audit records feature. Use this grant statement:

```
grant delete on SYS.AUD$ to username
```

Running the Oracle XML File Agent (UNIX, Windows)

This section contains instructions on how to configure and run FortiDB's Oracle XML file agent to monitor multiple Oracle databases(SIDs). The agent, when active, periodically pushes Oracle's audit log data to FortiDB server for further processing.

Prior to configuring and starting FortiDB agent:

1. Have a login credential with read and write access to each of Oracle database audit log directory under monitor. Use this login to configure and run FortiDB agent. Run *show parameters audit_file_dest;* using Oracle SQLPlus utility to obtain your Oracle database audit directory. On Windows platform, in order to install the agent as a Windows service, the login credential must be in administrator group. The group can be removed from the login credential once the installation completes.
2. Have a Java Virtual Machine (JVM) 1.6+ installed with *JAVA_HOME* environment variable correctly configured, and its *bin* directory is first on execution path. On 64 bit x86_64 Windows systems, do not use the native x86_64 JVM, but use the x86 JVM instead in order to get FortiDB agent to run under Windows system services. There is no performance issue about this limitation.

To configure and run the Oracle XML file agent, take the following steps.

1. Prepare your Oracle target database. See *Configuring the Oracle Target Database*
2. In FortiDB Target Management, create a connection to an Oracle target database (this step is required to make a connection to the agent).
3. Unpack a copy of FortiDB agent installer to a directory using login credential mentioned in the prerequisite step.
4. Copy *agent.properties.sample file* from agent's *doc* directory to agent's *conf* directory, and change the file name to *agent.properties.*
5. Edit the *agent.property* file.
   a) Open the *agent.property* file using a text editor.
   b) Enter the values for the following properties.

Parameters	Descriptions	Required or Optional
agentType	Enter ORA_XML	Required
brokerAddress	Enter IP address or resolvable host name of the FortiDB server.	Required

Parameters	Descriptions	Required or Optional
brokerPort	FortiDB Communication Server Listening port.	Optional. The default value is 9116.
agentDBAddress:	Enter your target database IP Address. This value must match FortiDB's target configuration.	Required
agentDBPort:	Enter your target database listening port. This value must match FortiDB's target configuration.	Required
pollingInterval	Enter the positive integer in milliseconds for the polling interval.	Optional. The default value is 60000 (60 seconds) for Oracle XML.
removeAuditFile	Remove DB2 audit file outputs after sending to FortiDB	Not required. This parameter is only for DB2 target databases.

6 . Install the agent service (Windows only).
   a) Go to agent's bin directory
   b) Execute the following command:
   ```
   fdbagent install
   ```
   c) Open Windows Services Control Panel, and configure *FortiDB Database Monitoring Agent* to run with the same log on id that is used to unpack the FortiDB agent bundle.

7 . Start the FortiDB agent.
   - For Windows, Linux or Solaris:
     1 . Go to agent's bin directory.
     2 . Execute the following command:
     ```
     $ fdbagent start
     ```
     To stop the agent, execute:
     ```
     $ fdbagent stop
     ```
   - For other platforms:
     1 . Go to agent's bin directory.
     2 . Execute the following command:
     ```
     $ nohup ./fdbagentapp &
     ```

8 . To test the collection method with the agent, go to **Data Activity Monitoring** > **Monitors**. For details about collection methods, see *Choosing a Collection Method*

Running the Oracle SGA Agent (Solaris)

You can monitor only **Oracle 10gR2 on Solaris**, using the Oracle SGA agent. To run the Oracle SGA agent, take the following steps.

1 . Prepare your Oracle target database. See *Configuring the Oracle Target Database*
2 . In FortiDB Target Management, create a connection to an Oracle target database (this step is required to make a connection to the agent).
3 . Download the Oracle XML agent to your target database machine. For details about downloading the Oracle XML agent, please ask FortiDB technical support.
4 . Create a directory and unzip the Oracle agent in the directory.

5 .Copy agent.properties.sample file from /fdbagents/doc directory to fdbagent/conf directory, and change the file name to "agent.properties".

6 .Edit the agent property file.

a) Open the agent.property file using a text editor.

b) Enter the values for the following properties.

Parameters	Descriptions	Required or Optional
agentType	Enter ORA_SGA	Required
brokerAddress	Enter IP address or resolvable host name of the FortiDB server.	Required
brokerPort	FortiDB Communication Server Listening port.	Optional. The default value is 61616.
agentDBAddress:	Enter your target database IP Address. This value must match FortiDB's target configuration.	Optional. This value is normally discovered at startup, but if ping `hostname` shows 127.0.0.1 as its address, then you need to replace it with the actual IP address.
agentDBPort:	Enter your target database listening port. This value must match FortiDB's target configuration.	Required
pollingInterval	Enter the positive integer in milliseconds for the polling interval.	Optional. The default value is 60000 (60 seconds) for Oracle SGA.
removeAuditFile	Remove DB2 audit file outputs after sending to FortiDB	Not required. This parameter is only for DB2 target databases.

7 .Start the FortiDB agent.

Note: To run the agent, Java SE 6 (JDK 6) is required.

1 .Go to /fdbagent/bin directory.

2 .Execute the following command:

```
$ ./fdbagent start
```

To stop the agent, execute:

```
$ ./fdbagent stop
```

8 .To test the collection method with the agent, go to **Data Activity Monitoring** > **Monitors**. For details about collection methods, see *Choosing a Collection Method*

Configuring the MS SQL Server Target Database

This topic describes required settings of MS SQL Server databases. To monitor the MS SQL Server target database, FortiDB provides several methods that users can choose depending on their circumstances.

Collection Methods

FortiDB collects MS SQL Server data using the following method:

Collection Methods (dropdown list)	Prerequisite	Required Agent?
TCP/IP Sniffer	See *Configuring Monitoring with TCP/IP Sniffer* for detail	No
SQL Trace	Make sure the SQL Server has audit trace folder (ex. C:\SQLTrace), and must enter the full path of folder in FortiDB's monitoring definition.	No
Net Agent	You must install the Net Agent in host of SQL Server first. For details about how to run the MSSQL Net Agent, please refer the document released with FortiDB Net Agent.	Yes

User Privileges for Monitoring with TCP/IP Sniffer or Net Agent

The user specified in target database, must be member of **sysadmin**.

User Privileges for Monitoring with SQL Trace

In order to connect to the MS SQL target databases from FortiDB, the database user must have the following privileges:

Data Policies	Privilege Policies	Metadata Policies
Member of sysadmin	**For Collection Method 'SQL Trace'** SELECT on: • sys.columns • sys.database_role_members • sys.database_permissions • sysobjects • sys.database_principals • sys.sql_logins EXECUTE on: • sp_helpsrvrolemember **For Collection Method 'TCP/ IP Sniffer' and 'Net Agent'** • No privilege is required	**For Collection Method 'SQL Trace'** SELECT on: • information_schema.columns • sysindexes • sysobjects • information_schema.routines • sys.objects obj • sys.sql_modules • information_schema.views **For Collection Method 'TCP/ IP Sniffer' and 'Net Agent'** • No privilege is required

For MS SQL Server, use the following command to add a login as a member of sysadmin;

```
sp_addsrvrolemember 'username', 'sysadmin'
```

Configuring the Sybase Target Database

This topic describes required settings of Sybase databases for monitoring.

Collection Methods

FortiDB collects Sybase data using the following method:

Collection Methods (dropdown list)	Prerequisite	Required Agent?
TCP/IP Sniffer	See *Configuring Monitoring with TCP/IP Sniffer* for detail	No
MDA(Monitoring and Data Access)	Before monitoring your Sybase target database, you need to perform the following procedures: • Create the sybsecurity database • Install installsecurity • Configure MDA (Monitoring and Data Access) tables And see *Preparing Sybase Using MDA* for preparation.	No

Procedures for Using MDA

Create the sybsecurity Database

To create the sybsecurity database, execute the following commands (you need to change the value of physname to your actual sybase path):

```
disk init name = "auditdev", physname = "C:\sybase\data\sybaud.dat", size =
 5120
go
disk init name = "auditlog", physname = "C:\sybase\data\sybaudlog.dat", size =
 1024
go
create database sybsecurity on auditdev log on auditlog
go
```

Install installsecurity

The SQL script installsecurity contains all required stored procedures and audit tables. To install installsecurity, take the following steps. For example, the script is located under $SYBASE/ASE-15_0// scripts.

1. Go to the scripts directory. For example, $SYBASE/ASE-15_0/scripts.
2. Execute the following command:

```
isql -Usa -P<password> < instsecu
```

3. Restart the database.

Configure MDA Tables

FortiDB uses Sybase MDA tables for collecting audit information. You must configure your server to enable MDA. For configuring Sybase MDA tables, perform the following procedures.

1. Grant mon_role to the database user to connect to FortiDB. To grant mon_role to the user, execute the following script:

```
grant role mon_role to <user name>
```

Note: You may need to disconnect/reconnect to activate 'mon_role' when you just granted this role to the login you're currently using.

2. Prepare Sybase with MDA tables. See *Preparing Sybase with MDA tables*
3. Connect to Sybase. For details about connecting to the target database, see *Managing Target Databases*

4 .Clear MDA buffer. This step should be taken only after the first connection. To clear MDA buffer, execute the following commands:

```
select top 1 * from dbo.monSysSQLText
go

select top 1 * from dbo.monSysStatement
go
```

Preparing Sybase using MDA (Monitoring and Data Accesses)

This topic describes preparing the Sybase target database to monitor, using Sybase MDA tables. The following steps are required to monitor Sybase target databases.

Setting "tempdb" database for MDA

In order to monitor Sybase target database with FortiDB, it is recommended to have more than 100MB free area for "tempdb" database. To set the size of "tempdb", take the following steps:

1 .Connect to master database as "sa" user.

2 .Check the size of "tempdb". For example, execute as follows:

```
sp_helpdb
go

name           db_size       owner dbid   created    status
-------------- ------------- ----- ------ -----------------

 ------------------------------------------------------------------------
master               13.0 MB sa         1 Dec 07, 2007
        mixed log and data
model                 4.0 MB sa         3 Dec 07, 2007
        mixed log and data
sybmgmtdb            75.0 MB sa         4 Dec 07, 2007
        select into/bulkcopy/pllsort, trunc log on chkpt, mixed log and
data
sybsystemdb           3.0 MB sa     31513 Dec 07, 2007
        mixed log and data
sybsystemprocs      120.0 MB sa     31514 Dec 07, 2007
        trunc log on chkpt, mixed log and data
tempdb                4.0 MB sa         2 Nov 11, 2008
        select into/bulkcopy/pllsort, trunc log on chkpt, mixed log and
data
text_db               5.5 MB sa         5 Dec 07, 2007
        trunc log on chkpt, mixed log and data
```

3 .Allocate disk space to “tempdb”. For example, to allocate 500 MB, which is 256000 pages, execute as follows:

```
disk init name = "tempdb_data01",
physname = "/export/home/sybase/data/tempdb_data01.dat",
size = 256000
go
```

4 .Allocate disk space on the new device to “tempdb” . For example, execute as follows:

```
alter database tempdb on tempdb_data01 = 500
go

Extending database by 256000 pages (500.0 megabytes) on disk tempdb_data01
```

Setting Logon Trigger for Session Policies

In order to get session information, creating a table to store session information, and set logon trigger are required. To set logon trigger to get session information, take the following steps:

1. Drop the previous created "FortiDB_audit" table if there is any. For example, to drop the table "FortiDB_audit", execute as follows:

```
drop table master.dbo.FortiDB_audit
go
```

2. Create a table to store logon information. For example, to create the table "FortiDB_audit" in the master database, execute as follows:

```
create table master.dbo.FortiDB_audit
(
spid smallint,
kpid int,
suid int,
loginname varchar(30),
dbusername varchar(30),
dbid smallint,
dbname varchar(30),
program_name varchar(30) null,
hostprocess varchar(30) null,
ipaddr varchar(64) null ,
loggedindatetime datetime
 )
go
```

3. Create a procedure for logon trigger. For example, to create the procedure "login_proc", execute as follows:

```
use master
go

drop procedure login_proc
go

create procedure login_proc
as
begin
insert into master.dbo.FortiDB_audit
select
S.spid,
S.kpid,
S.suid,
suser_name(),
user_name(),
S.dbid,
db_name(),
S.program_name,
S.hostprocess,
S.ipaddr,
S.loggedindatetime
from master.dbo.sysprocesses S
where S.spid = @@spid
end
go
```

4. Create logon trigger. To create logon trigger, execute as follows:

```
sp_logintrigger 'master.dbo.login_proc'
go

Global login trigger updated.
```

If sp_logintrigger is not installed, recreate master database procedures. For example, execute the following script.

For UNIX:

```
isql -Usa -P<password> -i$SYBASE/ASE-15_0/scripts/installmaster
```

For Windows:

```
isql -Usa -P<password> -i$SYBASE/ASE-15_0/scripts/installmstr
```

If you need to drop the global trigger, execute:

```
sp_logintrigger 'drop'
go
```

5 . Grant execute logon trigger for all users as follows:

```
grant execute on dbo.login_proc to public
go
```

Setting MDA parameters

To set MDA parameters, take the following steps:

1 . Configure MDA parameters. Set the following parameters: (the following commands are examples for Linux. For Windows, you need to enter "go" for each execution.)

```
sp_configure "enable cis", 1
sp_addserver loopback, null, @@servername (not required for 15.0.2 or later)
set cis_rpc_handling on (not required for 15.0.2 or later)
exec loopback...sp_who (note: 3 dots)
sp_configure "errorlog pipe active", 1
sp_configure "deadlock pipe active", 1
sp_configure "wait event timing", 1
sp_configure "process wait events", 1
sp_configure "object lockwait timing", 1
go
```

(For monSysStatement table)

```
sp_configure "statement statistics active",1
sp_configure "statement pipe max messages",30000
sp_configure "per object statistics active",1
sp_configure "statement pipe active" ,1
go
```

(for monSysSQLText table)

```
sp_configure "max SQL text monitored" , 8192
sp_configure "SQL batch capture", 1
sp_configure "sql text pipe max messages", 30000
sp_configure "sql text pipe active", 1
go
```

The following parameter values are recommended:

```
sp_configure "max memory" , 256000
sp_configure "event buffers per engine", 2000
sp_configure "plan text pipe max messages", 100
sp_configure "errorlog pipe max messages", 30000
sp_configure "deadlock pipe max messages", 100
go
```

2 . Restart Sybase database.

3 . Enable MDA. To enable MDA, set the following parameter:

```
sp_configure "enable monitoring" , 1
go
```

4 . Go to Step 3 of "Configure MDA Tables".

Configuring the DB2 Target Database

This topic describes required settings of the DB2 databases. In DB2 target databases, there are the following users involved in monitoring.

Collection Methods

FortiDB collects DB2 data using the following method:

Collection Methods (dropdown list)	Prerequisite	Required Agent?
TCP/IP Sniffer	See *Configuring Monitoring with TCP/IP Sniffer* for detail	No
DB2 Agent	See below sections for detail.	Yes

Use and Privileges need for Using DB2 Agent

Required DB2 users	Roles	Required privileges
DB2 user to connect to FortiDB	Connects FortiDB to the DB2 target database	**SECADM** (auditing privilege). See Step5 of *Setting the DB2 Target Database*
DB2 Instance owner	DB2 instance owner	Privileges as the DB2 instance owner
DB2 user for running the agent	Run the DB2 agent. This user should be the same user of the DB2 instance owner	For Windows, this user should belong to the **DB2ADMNS** group. For details about how to run the agent, see *Running the DB2 Agent* .

Configure DB2 Target and DB2 Agent

In order to start monitoring DB2 target databases, you need to perform the following tasks in your target database.

- *Setting the DB2 Target Database for DB2 Agent*
- *Running the DB2 Agent on Windows*

Setting DB2 Target Database for DB2 Agent

In order to connect FortiDB to a DB2 target database, and monitor it with DB2 Agent, you need to set your target database properly. To set your DB2 target database, take the following steps:

1. Reset the instance level audit if you had previously configured auditing. To reset the instance level audit, execute the following command:

   ```
   db2audit configure reset
   ```

2. Start db2audit. To start db2audit, execute the following command:

   ```
   db2audit start
   ```

3. Set the instance level audit for monitoring login failure. To set the instance level audit, execute the following command:

   ```
   db2audit configure scope context status failure
   ```

4. Set Audit buffer. To set Audit buffer (AUDIT_BUF_SZ) for an instance, run the following commands:

   ```
   db2 update dbm cfg using AUDIT_BUF_SZ 10000
   ```

Note: The default audit buffer is 0 (no setting).

5 .Grant SECADM privilege to the FortiDB connection user to execute audit. To grant the privilege, execute the following command:

```
db2=> GRANT SECADM ON DATABASE TO USER <user_name>

where <user_name> is the FortiDB connection user name.
```

Note: For Windows, the FortiDB connection user must belong to the DB2ADMINS or DB2USERS group. For UNIX, AIX, or Linux, the FortiDB connection user can be a non-instance owner. By default, the DB2admin user does not have the "SECADM" privilege.

6 .Connect to FortiDB for monitoring. For details about connecting to FortiDB, go to "Managing Target Databases".

7 .Run the DB2 agent for monitoring DB2 target databases. For details about running the DB2 agent, go to "Running the DB2 Agent".

Configuring and Running the DB2 Agent

This section contains instructions to how to configure and run FortiDB's DB2 agent to monitor multiple DB2 databases.

The following consists of list of prerequisites prior to configuring and running FortiDB DB2 agent.

1 .FortiDB DB2 agent is responsible to periodically request DB2 database to dump its audit data to file system location belonging to FortiDB DB2 agent temporary directory. The agent then pushes the audit files to FortiDB server and finally removes them. This means, FortiDB DB2 agent must have read and write access to the audit data files. To do that, FortiDB DB2 agent must run under the same credential that runs the DB2 server (ie the instance owner of the DB2 instance under monitor). On Windows platform, in order to install the agent as a Windows service, the login credential must be in administrator group. The group can be removed from this login credential once the installation completes.

2 .Have a Java Virtual Machine (JVM) 1.6+ installed with *JAVA_HOME* environment variable correctly configured, and its *bin* directory is first on execution path. On 64 bit x86_64 Windows systems, do not use the native x86_64 JVM, but use the x86 32 bit JVM instead in order to get FortiDB agent to run under Windows system services. There is no performance issue about this limitation.

3 .Have a copy of FortiDB Agent installer.

To configure and run FortiDB DB2 agent, take the following steps.

1 .Prepare your DB2 target database. See *Configuring the DB2 Target Database*

2 .Unpack a copy of FortiDB agent installer to a directory using login credential mentioned in the prerequisite step.

3 .Copy and edit the agent property file.

a) Copy the file named *agent.properties.sample* from agent's doc directory to agent's conf directory and change the file name to *agent.properties*

b) Open the agent.property file using a text editor.

c) Enter the values for the following properties.

Parameters	Descriptions	Required or Optional
agentType	Enter DB2.	Required
brokerAddress	Enter IP address or resolvable host name of the FortiDB server.	Required
brokerPort	FortiDB Communication Server Listening port.	Optional. The default value is 9116.

Parameters	Descriptions	Required or Optional
agentDBAddress:	Enter your target database IP Address. This value must match FortiDB's target configuration.	Required.
agentDBPort:	Enter your target database listening port. This value must match FortiDB's target configuration.	Required
pollingInterval	Enter the positive integer in milliseconds for the polling interval.	Optional. The default value is 60000 (60 seconds) for DB2.
removeAuditFile	true or false. To remove DB2 audit file outputs after sending to FortiDB, enter true.	Optional. The default is true.

4 .Execute DB2 Agent Setup.
   a) Go to agent's bin directory.
   b) Execute:

```
DB2AgentSetup
```

   to configure your DB2 to write audit contents to FortiDB DB2 agent temporary directory.

5 .Install the agent service (Windows only).
   a) Go to agent's bin directory
   b) Execute:

```
fdbagent install
```

   c) Open Windows Services Control Panel, and configure *FortiDB Database Monitoring Agent* to run with the same log on id that is used to unpack the FortiDB agent bundle.

6 .Start the FortiDB agent.
   - For Windows, Linux or Solaris:
     1 .Go to agent's bin directory.
     2 .Execute the following command:

```
$ fdbagent start
```

     To stop the agent, execute:

```
$ fdbagent stop
```

   - For other platforms:
     1 .Go to agent's bin directory.
     2 .Execute the following command:

```
$ nohup ./fdbagentapp &
```

7 .Confirm db2audit settings. To confirm that the audit data path and audit archive path are filled in correctly, execute the following command:

```
> db2audit describe
```

   For example, the following audit settings display.

```
DB2 AUDIT SETTINGS:
```

```
Audit active: "TRUE"
Log audit events: "FAILURE"
Log checking events: "FAILURE"
Log object maintenance events: "FAILURE"
Log security maintenance events: "FAILURE"
Log system administrator events: "FAILURE"
Log validate events: "FAILURE"
Log context events: "FAILURE"
Return SQLCA on audit error: "FALSE "
Audit Data Path: "C:\DB2\fdbagent\bin\..\tmp\db2audit\flush\"
Audit Archive Path: "C:\DB2\fdbagent\bin\..\tmp\db2audit\archive\"

AUD0000I  Operation succeeded.
```

8. To test the collection method with the agent, go to **Data Activity Monitoring** > **Monitors**. For details about collection methods, see *Choosing a Collection Method*

Configuring the MySQL Target Database

This topic describes configuring the MySQL target database. To monitor MySQL databases, you need to configure the MySQL general log.

This topic explains:

- *Setting MySQL General Log*

Setting MySQL General Log

This topic describes setting MySQL general log table.

1. Add parameters to my.cnf file (For Windows, my.ini).
   a) Go to %MYSQL_HOME directory.
   b) Open my.cnf (for UNIX) or my.ini (for Windows) with your text editor.
   c) Add the following parameters in [mysqld] section.

```
general_log=1
log_output=TABLE
```

   d) Restart MySQL databases.
2. Change the definition of "mysql.general_log" table.
   a) Switch the engine from CSV to MyISAM. To switch the engine from CSV to MyISAM, execute the following commands (the default is ENGINE=CSV).

```
mysql> SET GLOBAL general_log = 'OFF';
mysql> ALTER TABLE mysql.general_log ENGINE = MyISAM;
mysql> SET GLOBAL general_log = 'ON';
```

3. Check the definition of "mysql.general_log" table. Execute the following SQL command:

```
mysql> show create table mysql.general_log;

+-------------
+-------------------------------------------------------------------
----------------------------------------+
| Table       | Create Table
----------------------------------------+
| general_log | CREATE TABLE `general_log` (
  `event_time` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE
 CURRENT_TI
MESTAMP,
  `user_host` mediumtext NOT NULL,
  `thread_id` int(11) NOT NULL,
  `server_id` int(11) NOT NULL,
```

```
  `command_type` varchar(64) NOT NULL,
  `argument` mediumtext NOT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8 COMMENT='General log' |
+-------------+-----------------------------------------
```

4. Check if logging started. Execute the following command:

```
mysql> select * from mysql.general_log;

+---------------------+-----------------------------------+-----------
+--------
---+--------------+----------------------------------+
| event_time          | user_host                         | thread_id |
 server_
id | command_type | argument                          |
+---------------------+-----------------------------------+-----------
+--------
---+--------------+----------------------------------+
| 2009-07-29 16:44:23 | root[root] @ localhost [127.0.0.1] |         1 |
 0 | Connect      | root@localhost on mysql           |
| 2009-07-29 16:44:23 | root[root] @ localhost [127.0.0.1] |         1 |
 0 | Query        | select @@version_comment limit 1 |
| 2009-07-29 16:44:37 | root[root] @ localhost [127.0.0.1] |         1 |
 0 | Query        | show create table general_log    |
| 2009-07-29 16:45:19 | root[root] @ localhost [127.0.0.1] |         1 |
 0 | Query        | set global general_log='OFF'     |
| 2009-07-29 16:46:18 | root[root] @ localhost [127.0.0.1] |         1 |
 0 | Query        | select * from mysql.general_log  |
+---------------------+-----------------------------------+-----------
+--------
---+--------------+----------------------------------+
5 rows in set (0.00 sec)
```

FortiDB User Privileges

This section indicate the privileges necessary for a target database user who connects ForiDB to the target database. This user name is used in the FortiDB Target connection page, in order to connect to the target database for Assessment, and Monitoring/Auditing.

To grant privileges to the FortiDB user, use the GRANT statement. Some examples are:

```
GRANT SELECT_CATALOG_ROLE TO <username>
GRANT SELECT ON dbo.syscolumns TO <username>
GRANT SELECT ON SYSIBM.SYSCOLAUTH TO <username>
GRANT ROLE SSO_ROLE TO <username>
```

For MS SQL Server, use the following command to add a login as a member of sysadmin;

```
sp_addsrvrolemember 'username', 'sysadmin'
```

Privileges for Assessment

To run assessment, the FortiDB users for your target databases need the following privileges:

DB2 UDB

Required Privileges for	Required Privileges
Assessment	• CREATE TABLE • SELECT on the following SYSIBM tables: • SYSCOLAUTH

Required Privileges for	Required Privileges
	• SYSDBAUTH • SYSINDEXAUTH • SYSPLANAUTH • SYSSCHEMAAUTH • SYSTABAUTH • SYSTBSPACEAUTH

Privileges Summary Use	• SELECT on the following SYSCAT tables:
	  • COLAUTH
	  • DBAUTH
	  • INDEXAUTH
	  • PACKAGEAUTH
	  • SCHEMAAUTH
	  • TABAUTH
	  • TBSPACEAUTH
	• SELECT on the following SYSIBM tables:
	  • SYSCOLAUTH
	  • SYSDBAUTH
	  • SYSINDEXAUTH
	  • SYSPLANAUTH
	  • SYSSCHEMAAUTH
	  • SYSTABAUTH
	  • SYSSYSTABLESPACES
	  • SYSTBSPACEAUTH
	  • SYSUSERAUTH

Pen Test Use	• SELECT on the following SYSCAT tables:
	  • COLAUTH
	  • DBAUTH
	  • INDEXAUTH
	  • PACKAGEAUTH
	  • SCHEMAAUTH
	  • TABAUTH
	  • TBSPACEAUTH
	• SELECT on the following SYSIBM tables:
	  • SYSCOLAUTH
	  • SYSDBAUTH
	  • SYSINDEXAUTH
	  • SYSPLANAUTH
	  • SYSSCHEMAAUTH
	  • SYSTABAUTH
	  • SYSTBSPACEAUTH
	  • SYSUSERAUTH

MSSQL 2000

Required Privileges for	Required Privileges

Assessment	• SELECT on:
	  • MASTER.DBO.SPT_VALUES
	  • MASTER.DBO.SYSALTFILES
	  • MASTER.DBO.SYSDATABASES
	  • MASTER.DBO.SYSLOGINS
	  • MASTER.DBO.SYSXLOGINS
	  • SYSCOLUMNS
	  • SYSMEMBERS
	  • SYSOBJECTS
	  • SYSPROTECTS
	  • SYSUSERS
	• EXECUTE on:
	  • MASTER.DBO.XP_CMDSHELL
	  • MASTER.DBO.XP_INSTANCE_REGENUMVALUES
	  • MASTER.DBO.XP_INSTANCE_REGREAD
	  • MASTER.DBO.XP_LOGINCONFIG
	  • MASTER.DBO.XP_LOGININFO
	  • MASTER.DBO.XP_REGENUMVALUES
	  • MASTER.DBO.XP_REGREAD
	  Note: The MS-SQL sysadmin role is an additional requirement if you want to use these policies during your assessment:
	  • DVA MSSQL 01.01 password field empty
	  • DVA MSSQL 01.02 password is the same as login name

Privileges Summary Use	• For each individual MS-SQL 2000 database you want to connect to, SELECT on:
	  • MASTER.DBO.SYSDATABASES (for MS-SQL 2000 server-level connections)
	  • SYSMEMBERS
	  • SYSOBJECTS
	  • SYSPROTECTS
	  • SYSUSERS

Pen Test Use	• SELECT on:
	  • MASTER.DBO.SYSDATABASES (for MS-SQL 2000 server-level connections)
	  • MASTER.DBO.SYSXLOGINS
	  • SYS.DATABASE_ROLE_MEMBERS
	  • SYSMEMBERS
	  • SYSOBJECTS
	  • SYSPROTECTS
	  • SYSUSERS (for each individual MS-SQL 2000 database you want to connect to)

MSSQL 2005/2008

Required Privileges for	Required Privileges

Assessment	• SELECT on:
	  • MASTER.DBO.SPT_VALUES
	  • MASTER.DBO.SYSALTFILES
	  • MASTER.DBO.SYSDATABASES
	  • MASTER.DBO.SYSLOGINS
	  • MASTER.DBO.SYSXLOGINS
	  • SYS.COLUMNS
	  • SYS.MEMBERS
	  • SYS.OBJECTS
	  • SYS.PROTECTS
	  • SYS.USERS
	• EXECUTE on:
	  • MASTER.DBO.XP_CMDSHELL
	  • MASTER.DBO.XP_INSTANCE_REGENUMVALUES
	  • MASTER.DBO.XP_INSTANCE_REGREAD
	  • MASTER.DBO.XP_LOGINCONFIG
	  • MASTER.DBO.XP_LOGININFO
	  • MASTER.DBO.XP_REGENUMVALUES
	  • MASTER.DBO.XP_REGREAD
	  Note: The MS-SQL `sysadmin` role is an additional requirement if you want to use these policies during your assessment:
	  • DVA MSSQL 01.01 password field empty
	  • DVA MSSQL 01.02 password is the same as login name
	  • DVA MSSQL 05.36 List database logins that are part of the local Administrators group
	  • DVA MSSQL 05.37 Verify SQL Server not run as local System Administrator
	  • DVA MSSQL 05.42 Default MS SQL Listener Port Report

Privileges Summary Use	• SELECT on:
	  • MASTER.SYS.DATABASES (for MS-SQL 2005 server-level connections)
	• For each individual MS-SQL 2005 database you want to connect to, SELECT on:
	  • SYS.DATABASE_PERMISSIONS
	  • SYS.DATABASE_PRINCIPALS (for each individual MS-SQL 2005 database you want to connect to)
	  • SYS.DATABASE_ROLE_MEMBERS
	  • SYS.OBJECTS

Pen Test Use	• SELECT on: • MASTER.SYS.DATABASES (for MS-SQL 2005 server-level connections)

Required Privileges for	Required Privileges
	• SYS.DATABASE_PERMISSIONS • SYS.DATABASE_PRINCIPALS (for each individual MS-SQL 2005 database you want to connect to) • SYS.DATABASE_ROLE_MEMBERS • SYS.OBJECTS • SYS.SQL_LOGINS

Oracle

Required Privileges for	Required Privileges

Assessment	• CREATE SESSION
	• SELECT_CATALOG_ROLE
	• SELECT on:
	  • SYS.AUDIT$
	  • SYS.LINK$
	  • SYS.REGISTRY$HISTORY (Oracle 10g only)
	  • SYS.USER$
	  • SYSTEM.SQLPLUS_PRODUCT_PROFILE

Privilege Summary Use	• SELECT on:
	  • ALL_USERS
	  • DBA_COL_PRIVS
	  • DBA_ROLE_PRIVS
	  • DBA_ROLES
	  • DBA_SYS_PRIVS
	  • DBA_TAB_PRIVS

Pen Test Use	• SELECT on:
	  • ALL_USERS
	  • DBA_COL_PRIVS
	  • DBA_ROLE_PRIVS
	  • DBA_ROLES
	  • DBA_SYS_PRIVS
	  • DBA_TAB_PRIVS
	  • SYS.USER$

Sybase

Required Privileges for	Required Privileges

Assessment	• The SSO_ROLE and:
	  • If the Sybase Server is using SybSecurity, you need:
	  • On the MASTER database, you need to add the FortiDB user to the database, and you need SELECT on:
	  • SYSSRVROLES
	  • SYSLOGINROLES

Required Privileges for	Required Privileges
	• SYSSECMECHS • SYSDATABASES (AUDFLAGS column) • SYSLOGINS (AUDFLAGS column) • On any user-defined databases, you need to add the FortiDB user to the database, and you need SELECT on: • SYSUSERS • If the Sybase Server is not using SybSecurity, you need SELECT on: • SYSSRVROLES • SYSLOGINROLES • SYSSECMECHS • SYSDATABASES (AUDFLAGS column)
Privilege Summary Use	• For each individual database you want to connect to, SELECT on: • MASTER.DBO.SYSDATABASES (for server-level connections) • SYSOBJECTS • SYSPROTECTS • SYSUSERS
Pen Test Use	• SELECT on: • MASTER.DBO.SYSDATABASES (for server-level connections) • SYSOBJECTS • SYSPROTECTS • SYSUSERS (for each individual database you want to connect to)

MySQL

Required Privileges for	Required Privileges
Assessment	• SELECT on: • mysql.user • mysql.db • mysql.columns_priv • mysql.tables_priv
Privilege Summary Use	• SELECT on: • `INFORMATION\_SCHEMA`.* • mysql.user • Granted User privilege: • SHOW DATABASES
Pen Test Use	• SELECT on: • mysql.user

Privileges for Monitoring Data

To monitor data, the FortiDB user for your target database need the following privileges:

RDBMS Type	Required Privilege(s)
Oracle	**For Collection Method 'DB, EXTENDED' and 'XML File Agent'** • CREATE SESSION • SELECT_CATALOG_ROLE • DELETE_CATALOG_ROLE • AUDIT ANY • AUDIT SYSTEM • SELECT SYS.AUD$ • SELECT on the monitored tables or SELECT ANY TABLE **For Collection Method 'TCP/IP Sniffer', 'SGA Agent', 'Net Agent'** (Privileges need for browsing database to define data policy) • CREATE SESSION • SELECT_CATALOG_ROLE • SELECT on the monitored tables or SELECT ANY TABLE
MSSQL	Member of sysadmin
Sybase	**For MDA** • No privilege is required for the MDA table **For Collection Method 'TCP/IP Sniffer'** (Privileges need for browsing database to define data policy) • User who can browse database object
DB2 UDB	**For DB2 Agent** • SECADM privilege **For Collection Method 'TCP/IP Sniffer'** (Privileges need for browsing database to define data policy) • User who can browse database object

Privileges for Monitoring Privilege

To monitor privileges, the FortiDB user for your target database need the following privileges:

RDBMS Type	Required Privilege(s)
Oracle	• CREATE SESSION • SELECT_CATALOG_ROLE • DELETE_CATALOG_ROLE • AUDIT SYSTEM
MSSQL	**For Collection Method 'SQL Trace'** SELECT on:

RDBMS Type	Required Privilege(s)
	• sys.columns • sys.database_role_members • sys.database_permissions • sysobjects • sys.database_principals • sys.sql_logins EXECUTE on: • sp_helpsrvrolemember **For Collection Method 'TCP/IP Sniffer' and 'Net Agent'** • No privilege is required
Sybase	No privilege is required for the MDA table, or TCP/IP Sniffer
DB2 UDB	SECADM privilege for DB2 Agent No privilege is required for TCP/IP Sniffer

Privileges for Monitoring Metadata

To monitor metadata, FortiDB target database users need the following privileges:

RDBMS Type	Required Privilege(s)
Oracle	• CREATE SESSION • SELECT_CATALOG_ROLE for use with auditing: • CREATE SESSION • AUDIT SYSTEM • SELECT_CATALOG_ROLE
MSSQL	**For Collection Method 'SQL Trace'** SELECT on: • information_schema.columns • sysindexes • sysobjects • information_schema.routines • sys.objects obj • sys.sql_modules • information_schema.views **For Collection Method 'TCP/IP Sniffer' and 'Net Agent'** • No privilege is required
Sybase	No privilege is required for the MDA table, or TCP/IP Sniffer
DB2 UDB	SECADM privilege for DB2 Agent

RDBMS Type	Required Privilege(s)
	No privilege is required for TCP/IP Sniffer

Auto Discovery

Auto Discovery facilitates the creation of target-database connections by searching your network for potential target databases.

Auto Discovery scans your specified IP-address range, database-type specification, and port numbers for potential target databases.

Considerations for Successful Discovery of DB2

Consider the following when attempting to discover DB2 target databases:

- DB2 targets will not be discovered if TCP port 523 is in the CLOSED state for whatever reason. Causes for this could include dedicated firewall devices, router rules, or host-based firewall software.
- For successful discovery, the DB2 Administration Server (DAS) should be running.

Considerations for Successful Discovery of MS SQL Server

Consider the following when attempting to discover MS SQL Server target databases:

In order to display the correct version of MS SQL Server target databases, make sure that:

- Your MS SQL Server instance is up and running
- Your MS SQL Server Browser service is up and running

Running Auto Discovery

This topic describes how to perform Auto Discovery.

Note: To run Auto discovery, the FortiDB Administrator (the `admin` user that ships with FortiDB) or a user with the Target Manager role is required.

1. Go to **Target Management** > **Auto Discovery** of the left-side tree menu.
2. In order to discover a single database, enter the IP address in the **From** field and leave the **To** field blank. If you want to discover multiple databases, enter a range of IP addresses by using both the **From** field and **To** field.
3. Select the **Add** button. The discovered IP address(es) should be added to the list of IP addresses.

   Note: In order to delete an IP address (or address range) already on the list, select the checkbox on the left of the IP address or range and select the **Remove** button
4. Specify database types to attempt discovery for and their respective port ranges to discover from the list.
   a) Select or clear the checkbox(es) on the left of the list.
   b) Add or edit the port ranges in the **To** and **From** fields.
5. Select one or more IP address rows and then select the **Begin Discovery** button. One of the following status messages will be displayed at the top of the screen.

Status	Meaning
Running...	This status appears on the right side of the view header next to the "Status". The "processing" icon appears next to the page title. The Discovery Result page will display.

Status	Meaning
No databases found	There was no database of the specified IP address found.
Idle	Has one of these meanings: • User cancelled the Auto Discovery process before completion. • This is the status after `Running...` • This is the status after `No databases found`

Note: If you need to stop running Auto Discovery, select the **Abort** button to abort.

6 .The Auto Discovery Results page displays.

-  indicates that this database was discovered.
-  indicates that this database was added to the targets list.

Adding Targets from Auto Discovery

This topic describes how to add target-database configuration to the **Targets** page from the **Auto Discovery Results**.

1 .Run Auto Discovery.

2 .Select the checkbox(es) next to the targets you want to add to your list of target databases.

3 .Select the **Add to Targets** button at the bottom.

4 .Go to the **Targets** page where you should see that the auto-discovered targets databases have been added to the **Targets** list.

VA Policy Management

About VA Policies

VA policies are best-practice business rules that are applied during assessments. FortiDB is per-populated with hundreds of policies for security and compliance to address security standards.

Policy Types

There are two types of policies you can use for database-vulnerability assessments.

- Pre-Defined Policies --- Fortinet adaptation of a Best Practice policy in database security. In addition to numerous database-vulnerability policies, Fortinet also provides policies that help you perform operating-system (OS) level assessments such as making sure that your OS version is appropriate for the version of your target database.
- User-Defined Policies --- Customer-, or third-party-, adaptation of an industry-, or company-, specific security policy. UDPs are constructed with conventional or procedural SQL.

You can use the policy groups that ship with FortiDB or create your own.

Policy Updates

Fortinet updates its policies several times a year with an XML file containing new or enhanced policies. Fortinet recommends that you import this list in order to stay current. You can get the latest policies from FortiGuard Center. For details, please refer to Managing Pre-Defined Policies(PDPs).

Exporting and Importing Policies

If you want to move the FortiDB policies to another machine, you can export them, as XML files, from the FortiDB source application's repository and then import them to a FortiDB target application's repository.

Note: Database Type, Severity and Classification are not validated when importing. So, before importing policies, make sure that the element contents in your XML file are accurate. You can export one or more policies in order to see a sample of what that content should be.

Policy Version

Each policy has a policy version. With the policy version, you can keep a track of:

- Pre-defined policies you imported, and ran assessments.

  The policy version number will be incremented when you import the PDP Updates.
- User-defined policies you updated.

  When you update your User-Defined Policy (UDP) in the Modify User Defined Policy page, the policy version number stays same. If you want to update the policy version number, you need to export your UDP, and change the policy version number before importing the policy. When you import your UDP with an equal or lower policy number than the original policy number, the policy will not be imported.

Note: The restored data from an old archive (prior to v3.2.1) will have the latest version of policies at the time you restored.

Policy Groups

Assessments use policy groups. A policy group must contain at least one policy.

These are the policy groups shipped with FortiDB.

- DB2 Policy Group
- MySQL Policy Group
- Oracle Policy Group
- Pen Test Policy Group
- SQL Server Policy Group
- Sybase Policy Group

Policy States

At any given moment, FortiDB policies will be in one of several states:

State (applicable icon, if any)	Indicates that:
Enabled ()	Subsequent assessments will use this policy.
Disabled ()	Subsequent assessments will not use this policy.
Modified and Enabled ()	A previously existing policy has been modified by an import and subsequent assessments will use this policy.
Modified and Disabled ()	A previously existing policy has been modified by an import and subsequent assessments will not use this policy.
New and Enabled ()	A new policy has been added by an import and subsequent assessments will use this policy.
New and Disabled ()	A new policy has been added by an import and subsequent assessments will not use this policy.

VA Pre-Defined Policies (PDP)

On the **Policies** page, you can manage Pre-Defined Policies in the Pre-Defined Policies tab. To view only certain policies, you can use the **View** dropdown list at the top of the page. You can also import additional polices or updates to existing policies.

The following table indicates columns and meanings in the pre-defined policies list.

Columns	Descriptions
Status	• Enabled () • Disabled () • New and Enabled () • New and Disabled () • Modified and Enabled ()

Columns	Descriptions
	• Modified and Disabled ( )
Name	Pre-defined policy name
DB Type	Oracle, Sybase, DB2, MS SQL Server, or MySQL
Severity	User defined severity level. There are 5 levels of severity: • Informational (default) • Cautionary • Minor • Major • Critical
Classification	Unclassified, Configuration, Password, Privilege, Database server, Host System.

- The **View** dropdown enables you to limit the policies that you view to only those within a certain policy group.
- The  button enables you to create a new policy group.
- The **Enable** button enables you to activate the policies for which a checkbox has been checked.
- The **Disable** button enables you to deactivate the policies for which a checkbox has been checked.
- The **Import** button enables you to import new or updated policies into the FortiDB repository.
- The **Export** button enables you to export the all policies on the screen as an XML file.

Exporting Pre-Defined Policies

This topic describes how to export Pre-Defined Policies (PDPs).

1. Go to **Policy** > **VA Policies** of the left-side tree menu.
2. Select the **Pre-Defined Policies** tab (default).
3. In the **View** dropdown list, select All or a policy group you want to export.

   Note: The checkboxes next to the individual policies have no effect when exporting. No matter how many checkboxes you check, all items on the screen will be exported
4. Select the **Export** button.
5. Save the XML file.

Importing Pre-Defined Policies (for Appliance Users)

This topic describes how FortiDB appliance users can import Pre-Defined Policies (PDPs) using the Fortinet Distribution Network (FDN).

This task includes importing those new and updated policies that FortiDB periodically offers its customers in order to keep their policy sets current and effective.

1. Go to **Policy** > **VA Policies** of the left-side tree menu/

   Note: If you choose the **Policies Groups** link, you will then have to select an existing policy **Name** to be taken to the **Policies** page.
2. Select the **Import** button.
   The **Pre-Defined Policy Update** page displays.
3. Select or clear the **Disable new and modified rules after import** checkbox.
   - If checked, new and modified rules are disabled after import.

- If unchecked, new and modified rules are enabled after import.

4 .Select or clear the **Identify new and modified rules with icons** checkbox.

- If checked, new and modified rules will be distinguished with an appropriate icon.
- If unchecked, new and modified rules will not be distinguished from any other policy.

Note: Fortinet recommends that you select this checkbox.

5 .Select the **Import Updates from FortiGuard Center** button.
This button attempts a connection with, and then an automatic download from, the FortiGuard Center.

If this is a successful operation, you will get a message like: “Updated 12 policies of 544 found in file.” The downloaded update file contains all policies. However, only the policies that have modifications are actually updated in your system. In this example, the downloaded update file contained a total of 544 policies only 12 of which needed to be updated in your system. The other 532 policies in the update file were identical to those already in your system.

Note: Appliance users can also import policy updates by using the **Select XML file to be uploaded** field. After clicking the Browse button and selecting the xml file to upload, and select the Import button.

Importing Pre-Defined Policies (for Standalone Users)

This topic describes how FortiDB users can import Pre-Defined Policies (PDPs) by uploading XML files containing these policies.

Before performing this task, you may need to download one or more XML files from a designated FortiDB web or FTP site.

This task includes importing those new and updated policies that FortiDB periodically offers its customers in order to keep their policy sets current and effective.

1 .Go to **Policy** > **VA Policies** of the left-side tree menu.

Note: If you choose the **Policies Groups** link, you will then have to Select an existing Name to be taken to the **Policies** page.

2 .Select the **Import** button.
The **Pre-Defined Policy Update** page displays.

3 .Enter the path to the XML file you downloaded, or select the **Browse** button and select the XML file.

4 .Check or uncheck the **Disable new and modified rules after import** checkbox.

- If you check this, the new and modified rules after import are deactivated.
- If you uncheck this, the new and modified rules after import are activated.

5 .Select or clear the **Identify new and modified rules with icons** checkbox.

- If you select this, you can identify new and modified rules with icons.
- If you clear this, you cannot identify new and modified rules with icons.

6 .Select the **Import** button.
Policies will be imported to the list on the **Policies** page.

OS-Level Pre-Defined Policies

FortiDB OS-Level PDP is the Pre-Defined Policy that uses SSH and a client-side script, containing OS commands, in order to gather and evaluate information about the target's operating system.

To run assessments against Oracle target machine using OS-Level PDPs, see *Enabling OS-Level PDP.*

OS-Level PDP and Permission Requirements

This topic describes specific OS-Level PDP and their permission requirements.

Guarded Item Description (proposed change)	Purpose	Required Permissions
OSVA ORCL 01.01 Oracle Critical Patches (opatch)	Returns: • opatch version • applied critical patch numbers	Oracle 9i, 10g or 11g: • The SSH user needs execute permission on opatch • The SSH user's PATH variable should include the location of opatch Oracle 10g and 11g: • The SSH user needs read, write, and execute permissions on opatch • The SSH user needs read, write, and execute permissions on $ORACLE_HOME/cfgtoollogs/opatch/lsinv
SVA ORCL 01.02 Oracle Owner-Login Check	Alerts if Oracle owner, which is specified on the FortiDB Database Connection GUI, is not in /etc/passwd.	The SSH user needs read permission on /etc/passwd with cat and grep commands
OSVA ORCL 01.03 Oracle DBA-Group Check	Alerts if dba is not in /etc/group file	The SSH user needs read permission on /etc/group with cat and grep command
OSVA ORCL 01.04 Oracle DBA-Group-Member List	Returns a list of members of the dba group from /etc/passwd and /etc/group	The SSH user needs read permission on /etc/passwd and /etc/group with cat and grep command
OSVA ORCL 01.05 Oracle Process-Owner Check	Alerts if Oracle process is being run by a non-Oracle user such as root, or bin.	The SSH user needs execute permission ps and grep command
OSVA ORCL 01.06 Oracle Excessive Directory & File Permissions Check	Alerts if other permissions, on the Oracle Home directory (and its contents) specified on the Create/Modify Database Connection screen, include both read and write (and not execute)	The SSH user needs other read and execute permissions on the $ORACLE_HOME directory. For example setup instructions, see Using Minimally-Privileged User with an ACL.
OSVA ORCL 01.07 Oracle Correct Directory/File Owner & Group Check	Alerts if files and directories under the Oracle Home directory specified on the Create/Modify Database Connection screen, do not have correct owner and group	The SSH user needs other read and execute permissions on the $ORACLE_HOME directory. For example setup instructions, see Using Minimally-Privileged User with an ACL.

	permissions. Exempt from this check are: • $ORACLE_HOME/bin/oracle • $ORACLE_HOME/bin/oradism • $ORACLE_HOME/bin/dbsnmp	
OSVA ORCL 01.08 Oracle setuid/setgid File Check	Alerts if setuid or setgid permissions are assigned to files and directories under the Oracle Home directory specified on the Create/Modify Database Connection screen. Exempt from this check are: • $ORACLE_HOME/bin/oracle • $ORACLE_HOME/bin/oradism • $ORACLE_HOME/bin/dbsnmp	The SSH user needs other read and execute permissions on the $ORACLE_HOME directory. For example setup instructions, see see Using Minimally-Privileged User with an ACL.
OSVA ORCL 01.09 Oracle Database-Configuration-Change Check	This policy checks if these database configuration files change between the previous and current assessments: • init.ora • spfle.ora	• The SSH user needs execute permission on ls for the $ORACLE_HOME/dbs/ directory • The SSH user needs read permission on the $ORACLE_HOME/dbs/ directory
OSVA ORCL 01.10 Oracle Network-Configuration-Change Check	This policy check if network configuration files changed between between the previous and current assessments • listener.ora • tnsnames.ora • sqlnet.ora	• The SSH user needs execute permission for ls on the $ORACLE_HOME/network/admin/ directory • The SSH user needs read permission on the $ORACLE_HOME/network/admin/ directory
OSVA ORCL 01.11 Oracle Installed-Operating-System Info	Returns OS name and version	• The SSH user needs execute permission for cat on the /etc/release file • The SSH user needs read permission on the /etc/release file
OSVA ORCL 01.12 Oracle External-Procedure Processes Running Check	Alert if external-procedure process is running on target server.	The SSH user needs execute permission for ps and grep

OSVA ORCL 01.13 Oracle EXTPROC	Alerts if any EXTPROC settings are listed in listener.ora. For example: `(SID_NAME = PLSExtProc)`	• The SSH user needs execute permission for cat on the listener.ora file • The SSH user needs read permission on the listener.ora file
OSVA ORCL 01.14 Oracle Missing-Listener-Password Check	Alerts if a PASSWORD setting is missing in listener.ora.	• The SSH user needs execute permission for cat on the listener.ora file • The SSH user needs read permission on the listener.ora file
OSVA ORCL 01.15 Oracle Missing-Listener-ADMIN_RESTRICTIONS Check	Alerts if a ADMIN_RESTRICTIONS setting is missing in listener.ora.	• The SSH user needs execute permission for cat on the listener.ora file • The SSH user needs read permission on the listener.ora file
OSVA ORCL 01.16 Oracle Default-Listener Check	Alerts if default LISTENER is set in listener.ora.	• The SSH user needs execute permission for cat on the listener.ora file • The SSH user needs read permission on the listener.ora file
OSVA ORCL 01.17 Oracle Default-Port (1521) Check	Alerts if default PORT is set in listener.ora.	• The SSH user needs execute permission for cat on the listener.ora file • The SSH user needs read permission on the listener.ora file
OSVA ORCL 01.18 Oracle Advanced-Listener-Security Settings Check	Alerts if any Oracle Advanced Security settings are missing in sqlnet.ora. For example, the presence of the following would not cause an alert: `SQLNET.ENCRYPTION_SERVER = Requested`	• The SSH user needs execute permission for grep the sqlnet.ora file • The SSH user needs read permission on the sqlnet.ora file
OSVA ORCL 01.19 Oracle Configured Listener List	Display all listener names	• The SSH user needs execute permission for cat on the listener.ora file • The SSH user needs read permission on the listener.ora file

OSVA ORCL 01.20 Oracle Unencrypted Listener Password Check	Alerts if password in listener.ora is unencrypted. Encrypted passwords should be 16 characters long and consist only of upper-case letters from A to F or numbers. For example, the following is an acceptably encrypted password and would not generate an alert: `PASSWORDS_LISTENER = F56401ADBA6810DS`	• The SSH user needs execute permission for cat on the listener.ora file • The SSH user needs read permission on the listener.ora file

Note: You can use your known_hosts file in order to give access to only certain hosts.

Setting Access Control List (ACL) for Minimally-Privileged Users

The Access Control List (ACL) helps provide more secure target-database access. For example, an ACL enables a minimum-permission user to perform, via SSH, the OS-Level operations used by the FortiDB OS-level PDPs.

In general, you create a user, belonging to the `nobody` group, on your target-database machine. Then, using ACL, you give that user only the specific permissions necessary to execute the OS-level PDPs in which you are interested. Here are some examples you could use in order to grant, to the SSH user, the other users' read and execute permissions on the $ORACLE_HOME directory, required by some OSVA PDPs.

Example One: How to set ACL on an Oracle 10g or 11g target server for OSVA ORCL 01.01

This example describes how to set ACL on an Oracle 10g target server for OSVA ORCL 01.01.

1. Assume the SSH user is fortidb.

```
$setfacl -m user:fortidb:rwx,mask:rwx $ORACLE_HOME/cfgtoollogs/opatch/lsinv
```

2. In order to confirm permissions:

```
$getfacl $ORACLE_HOME/cfgtoollogs/opatch/lsinv
```

That will return something like:

```
# file: /export/home/ora1020/product/10.2.0/Db_1/cfgtoollogs/opatch/lsinv
# owner: ora1020
# group: oinstall
user::rwx
user:fortidb:rwx       #effective:rwx  <--- Please check it
group::r-x             #effective:r-x
mask:rwx
other:r-x
```

Example Two: How to set ACL on an Oracle 9, 10g, or 11g target server for OSVA ORCL 01.06, 01.07, and 01.08

This example describes how to set ACL on an Oracle 10g target server for OSVA ORCL 01.01.

1. In order to find the directories within $ORACLE_HOME for which the required permissions do not exist, execute the following, as the Oracle owner (see o_owner), on your target-database machine:

```
$ find $ORACLE_HOME \( -type d \) -a \( ! -perm -o+rx \)
   -ls|awk '{print $3,$11}'
```

which might return something like:

```
drwx------ /oracle/db1/Apache/Apache/conf/ssl.key
drwxr-x--- /oracle/db1/.patch_storage
```

2 .Using the File Access Control List program, grant the appropriate permissions to sshuser:

```
$ setfacl -m user:sshuser:r-x,mask:r-x /oracle/db1/Apache/Apache/conf/
ssl.key
$ setfacl -m user:sshuser:r-x,mask:r-x /oracle/db1/.patch_storage
```

3 .(Optionally) confirm that correct permissions were granted with:

```
$ getfacl /oracle/db1/Apache/Apache/conf/ssl.key
$ getfacl /oracle/db1/.patch_storage
```

which would return something like:

```
# file: /export/home/ora1020/product/10.2.0/Db_1/.patch_storage
# owner: ora1020
# group: oinstall
user::rwx
user:mitagaki:rwx               #effective:r--
group::r--              #effective:r--
mask:r--
other:---
```

4 .(Optionally) you can revoke permissions with:

```
$ setfacl -d user:sshuser:r-x,mask:r-x oracle/db1/Apache/conf/ssl.key
$ setfacl -d user:sshuser:r-x,mask:r-x /oracle/db1/.patch_storage
```

Note: If you can not give read(r)/exec(x) permission to the directory, FortiDB VA will produce a "Permission denied" error on the report which you can ignore.

VA User-Defined Policies (UDP)

On the **Policies** page, you can manage User-Defined Policies in the **User-Defined Policies** tab. To view only certain policies, you can use the **View** dropdown list at the top of the page. You can also import additional polices or updates to existing policies.

Columns	Descriptions
Status	• Enabled ( ) • Disabled ( ) • New and Enabled ( ) • New and Disabled ( ) • Modified and Enabled ( ) • Modified and Disabled ( )
Name	User-defined policy name
DB Type	Oracle, Sybase, DB2, MS SQL Server, or MySQL
Severity	User defined severity level. There are 5 levels of severity: • Informational (default)

Columns	Descriptions
	• Cautionary • Minor • Major • Critical
Classification	Unclassified, Configuration, Password, Privilege, Database server, Host System.

- The **View** dropdown enables you to limit the policies that you view to only those within a certain policy group
- The  button enables you to create a new policy group.
- The **Add** button enables you to create your own User-Defined policy.
- The **Delete** button enables you to delete the policies for which a checkbox has been checked.
- The **Enable** button enables you to activate the policies for which a checkbox has been checked.
- The **Disable** button enables you to deactivate the policies for which a checkbox has been checked.
- The **Import** button enables you to import new or updated policies into the FortiDB repository.
- The **Export** button enables you to export all policies on the screen as an XML file.

Adding User-Defined Policies (UDPs)

This topic describes the task of adding User-Defined Policies.

1. Go to **Policy**> **VA Policies** of the left-side tree menu.
2. Select the **User-Defined Policies** tab.
3. Select the **Add** button.
4. Fill in the appropriate fields. Some of the fields to note are:

Field Name	Description
ID	Enter a unique designator that can include any character, including alphanumerics, special characters, and white spaces.
SQL query	Enter the query that will be used when this User-Defined Policy is applied during an assessment.
Result Column Name(s)	Entries in this field are the column names referred to in the **SQL query** field. Multiple entries are delimited by semicolons. The names can either be actual column names in your query, like empno in '`SELECT empno FROM scott.emp`' or aliases like enumber in '`SELECT empno AS " enumber`[1]`"FROM scott.emp`' You can use the '*' column wild card in your queries; however, you must separately specify the name of each column for which you want report

	results. If, for example, you use 'SELECT * FROM scott.emp' against an Oracle target database, you must enter "empno;ename;job;mgr;hiredate;sal;comm;deptno in this field in order to get a report on all columns in scott.emp **Note:** Do not put spaces before or after the semicolons unless your aliased column names also have leading or trailing spaces, respectively.
Result Column Label(s)	Entries in this field are the column names that you would like to see in your reports. Multiple entries are delimited by semicolons. **Note:** If you don't populate this field, your report's column headers will be the entries used for the **Result Column Name(s)** field.
Keywords	Entries in this field can be used when using a filter to create policy groups.

5 .Select the **Save** button.

Here is an Oracle example, which assumes you have access to the SCOTT schema:[2]

1 .Create a new UDP with these entries:

- **ID**: unique designator
- **Name**: myOracleUDP1
- **Database type**: Oracle
- **SQL query**: SELECT empno, ename from scott.emp
- **Result Column Name(s)**: empno;ename
- **Result Column Label(s)**: Employee Number;Employee Name
- **Severity**: Informational
- **Classification**: Unclassified

2 .Select **Save** in order to save myOracleUDP1.

3 .Create a policy group, myUDPGroup, containing the new UDP

4 .Create an assessment that runs against an Oracle target-database group and which uses myUDPGroup.

5 .Run a Detailed (Pre-Defined) Report against your assessment and you should see several rows of **Scan Results** like this in the **Informational Vulnerabilities** section:

- ***Employee Number*** 7369 ***Employee Name***: SMITH

Here is another, slightly different, Oracle example, which uses column-name aliasing and, again, assumes you have access to the SCOTT schema:

1 .Create a new UDP with these entries:

- **ID**: can be any value
- **Name**: myOracleUDP2
- **Database type**: Oracle

- **SQL query**: `SELECT empno as "EmpID", ename as "Worker" from scott.emp`
- **Result Column Name(s)**: `EmpID;Worker`
- **Result Column Label(s)**: `Employee Number;Employee Name`
- **Severity**: `Informational`
- **Classification**: `Unclassified`

2. Select **Save** in order to save `myOracleUDP1`.
3. Create a policy group, `myUDPGroup`, containing the new UDP
4. Create an assessment that runs against an Oracle target-database group and which uses `myUDPGroup`.
5. Run a Detailed (Pre-Defined) Report against your assessment and you should see several rows of **Scan Results** like this in the **Informational Vulnerabilities** section:
   - ***Employee Number*** 7369 ***Employee Name****:* SMITH

Deleting User-Defined Policies (UDPs)

This topic describes how to delete User-Defined Policies.

1. Go to **Policy** > **VA Policies** of the left-side tree menu.
2. Select the **User-Defined Policies** tab.
3. Select the checkbox(es) corresponding to the user-defined policy you want to delete.
4. Select the **Delete** button.

Exporting User-Defined Policies

This topic describes how to export User-Defined Policies.

1. Go to **Policy** > **VA Policies** of the left-side tree menu.
2. Select the **User-Defined Policies** tab.
3. In the View dropdown list, select All or a policy group you want to export.

Note: The checkboxes next to the individual policies have no effect when exporting. No matter how many checkboxes you select, all policies on the screen will be exported

4. Select the **Export** button.
5. Save the XML file.

Importing User-Defined Policies

This topic describes how to import User-Defined Policies.

1. Go to **Policy** > **VA Policies** of the left-side tree menu.
2. Select the **User-Defined Policies** tab.
3. Select the **Import** button.
4. Enter the path to the XML file you want to import, or select the **Browse** button and select the XML file you want to import.
   To successfully import your policies, you need to increase the value of the version attribute (for example, you need to change from version="3" to version="4") which can be found in <VaPolicy> element.
5. Select or clear the **Deactivate new and modified rules after import** checkbox.
   - If you select this, the new and modified rules after import are deactivated.
   - If you clear this, the new and modified rules after import are activated.
6. Select or clear the **Identify new and modified rules with icons** checkbox.
   - If you select this, you can identify new and modified rules with icons.
   - If you clear this, you cannot identify new and modified rules with icons.
7. Select the **Import** button.

VA Policy Groups

The Policy Groups page displays all policy groups with groups names and descriptions.

In the VA Policy Groups page, you can:

- Add a new policy group by selecting **Add**. See *Adding a New Policy Group*
- Modify the policy group by selecting the group name. See *Modifying the Existing Policy Groups*
- Delete policy groups by selecting the group checkbox, and click **Delete**.

The following pre-defined policy groups are available:

Groups/Policies	Policies included
DB2 Policy Group	DB2 policies
MySQL Policy Group	MySQL policies
Oracle Policy Group	Oracle policies
SQL Server Policy Group	SQL Server policies
Sybase Policy Group	Sybase policies
Pen Test Policy Group	*Pen test policies*
CIS Policy Group	CIS benchmark policies

Adding VA Policy Groups

This topic describes the task of creating groups for Pre-, or User-, Defined) Policies by using filtering criteria.

1. Go to **Policy** > **VA Policy Groups** of the left-side tree menu.
2. Select the **Add** button.
3. On the subsequent **Policies** page, choose either the **Pre-Defined Policies** tab or the User-Defined Policies tab and then fill in the text boxes
   a) Use the **Policy Type** dropdown in order to create a group consisting of just Pre-Defined Policies, User-Defined Policies, or both (All).
   b) Use the **Group Name** text box to enter a name that will show up in the saved policy-group list. Use the optional **Description** text box to describe your filtering/grouping criteria.
   c) To create a filtering condition, enter an **Column** on which you would like to filter, an **Operator** that associates the **Column** with a **Value**, and a **Value** that the **Column** must match .
   d) You can add or subtract, respectively, filtering criteria rows by selecting the **+ (plus)** or **- (minus)** buttons.

Note: You cannot use the same **Column** in multiple rows. For example, you cannot establish a criteria that includes all the policies with a Severity of Minor and all the policies with a Severity of Major.

Note: In order to cancel creating a new policy-group filter and go back to the main **Policies** page, select the  icon.

Here are some examples of filtering criteria:

Table 5 : Filtering Criteria Examples

Attribute	Operator	Value	Return Possibilities
Severity	Equals	Minor	all policies with a Severity of Minor
Database Type	Equals	DB2	all policies associated with DB2 databases

4 .To test your filtering criteria, select the **Apply** button.

5 .
To save the group you created, select the  icon.

Note: In order to modify an existing group, select the **Name** of the group on the **Policy Groups** page.

Modifying the Existing VA Policy Groups

This topics describe modifying the existing policy group.

1 .Go to **Policy** > **VA Policy Groups** from the left-side tree menu.

2 .In the Policy Groups page, click the name of a policy group that you want to modify.

3 .Modify the policy name or description if necessary.

4 .Select the **Policy Type** from the dropdown list (All, Pre-efined, or User)

5 .To create a filtering condition, enter an **Column** on which you would like to filter, an **Operator** that associates the **Column** with a **Value**, and a **Value** that the **Column** must match .

6 .You can add or subtract, respectively, filtering criteria rows by selecting the **+ (plus)** or **- (minus)** buttons.

Note: You cannot use the same **Column** in multiple rows. For example, you cannot establish a criteria that includes all the policies with a Severity of Minor and all the policies with a Severity of Major.

Note: In order to cancel modifying the policy-group filter and go back to the main **Policies** page, select the  icon.

7 .To test your filtering criteria, select the **Apply** button.

8 .
Click  to save.

Deleting VA Policy Groups

This topic describes how to delete a policy group.

1 .Go to **Policy** > **VA Policy Groups** of the left-side tree menu.

2 .Check the checkbox(es) corresponding to the policy group(s) you want to delete.

3 .Click the **Delete** button.

About the Penetration Test

Penetration Tests (Pen Tests) allow you to run weak-password evaluations of your target databases.

For some database types, you can define whether they want to utilize hash-based method which is less destructive or login method which is more aggressive.

You can schedule Pen tests or run them immediately.

Managing Pen Tests

This topic describes how to configure and run Penetration Testing against target databases you specify.

1 .You can set the following properties in the **System Configuration** component of the FortiDB application.

Table 6 : Pen Test-related System Properties

Property	Purpose	Possible Values and Default Values
Enable Pen Test	When set to `true`, the Pen Test capability is enabled. When set to `false`, which is the default, the Pen Test capability is disabled.	`true` or `false`. The default value is `false`.
Enable Pen Test For All Users in Database (Standalone only)	When set to `false`, FortiDB uses the user names in <dbtype>user.txt, where dbtype represents the target-database type and is one of these strings: • ora for Oracle • sql for MS-SQL • db2 for DB2 UDB • syb for Sybase • mysql for MySQL When set to `true`, FortiDB ignores the user names in <dbtype>user.txt.	`true` or `false`. The default value is `true`.
Pen Test Method	The Login method actually logins in to your target databases. **Caution:**Be careful when using this method. Since its login attempts may be unsuccessful, it can result in preventing any, even approved, users from logging in to your target database. The Hash-based method is a safer, offline approach, but is available for only Oracle and MS SQL target databases. (A 'hash' is the value obtained after encrypting a clear-text string.) With the Hybrid method, FortiDB attempts the best	• 1=Login method • 2=Hash-based method • 3=Hybrid The default value is `Hybrid`. (If you select the Hash-based method for Sybase or DB2 targets, none of the Pen Test rules will be applied, your assessment result will be essentially empty, and no error will be signaled.)

Property	Purpose	Possible Values and Default Values
	available method. If the hash-based method is available, as will be the case with Oracle and MS-SQL targets, FortiDB uses it.	
Pen Test Password Dictionary	A file containing the passwords to be checked when executing the Dictionary Penetration test. The **Browse** button allows you to select your dictionary file. You need to select the **Save** button to complete your selection.	"Built-in Dictionary" indicates that the default dictionary is being used. "User Dictionary" indicates that you have uploaded your own dictionary file. The filename of the dictionary you upload will not appear here. **Note:**When you restore the default dictionary by checking the checkbox, and selecting **Restore Default(s)** and then **Save**, your dictionary file will be deleted from the system.

Note: After changing Pen Test properties, you must restart FortiDB to take your change into effect.

2 . Decide which of the following policies are suitable for your organization.

This table explains which files each Pen Test Policy uses:

Policy Name	File Used	Evaluate Content
Default Password	*<dbtype>default.txt*	All the username/password pairs in the file.
Username Reversed	*<dbtype>user.txt*	The pairing of usernames in the file with those same user names reversed as passwords.
Same as Username	*<dbtype>user.txt*	The pairing of usernames in the file with those same usernames as passwords.
Username Following Number	*<dbtype>user.txt*	The pairing of usernames in the file with those same usernames followed by one or more numbers as passwords.
Number Following Username	*<dbtype>user.txt*	The paring of usernames with those same usernames preceding one or more numbers as the passwords.
Dictionary	*<dbtype>user.txt, dictionary.txt*	The pairing of username in the <dbtype>user.txt

Policy Name	File Used	Evaluate Content
		file with every password in dictionary.txt file.

3 .(For standalone users) If you set `Enable Pen Test For All Users in Database` to `false`, you need to copy all of the files in the table below from *<FortiDB-install directory>/etc/conf/pentest* to *<FortiDB-install directory>/conf/pentest* and edit them.

The user name and password both have to be uppercase in the Oracle-related oradefault.txt and *orauser.txt* files.

Filename	Content
<dbtype>default.txt	A list of user name and password pairs that will be used for Default Password policy.
<dbtype>user.txt	A list of system or user accounts. The user names in this file will be used for all policies except for Default Password policy.
dictionary.txt	A list of passwords to use for Pen Test Dictionary policy. You can use your dictionary file by setting the Pen Test Password Dictionary property in the Assessment tab of the System Configuration page.  **Note:** When FortiDB executes the Pen Test Dictionary policy, the domain name automatically added in the password list.

 **Note:** The Enable Pen Test for All Users in Database property is not available for Appliance users.

4 .If you use Dictionary Policy, you can set your own dictionary file using Pen Test Password Dictionary property in the **Assessment** tab of the **System Configuration** page.

5 .You might also have to set proper privileges on your target database. For more information see *Target Privilege Matrix*.

6 .Select the **Policy Groups** link in the **Policy Management** section of the left-side tree-navigation menu.

7 .Select **Pen Test Policy Group**.

8 .Activate (or deactivate) Pen Test policies you want to run by checking the checkbox(es) next to each policy of interest and then clicking the **Enable** or (**Disable**) button.

9 .Optionally you can edit each policy by clicking on it and then modifying one or more of the following items. After you modify a policy, select the **Save** button on the Policy details page.

- Severity
- Classification
- Keywords
- Status

10Go to the **Assessments** link in the **Assessment Management** section of the left-side tree-navigation menu and create an assessment:

a) In the **Policies** tab of the **Assessment** page, select the **Pen Test Policy Group** within the **Available Policy Groups** list and then select the right arrow.
b) Save your Pen Test Assessment.
c) Run the Pen Test assessment.

d) Evaluate the results of your assessment.

Note: "Failed" means your passwords are weak and may not protect you from malicious login attempts.

Data Discovery Policies and Policy Groups

Data Discovery Policy is used by Sensitive Data Discovery and allows searching database for sensitive information located in tables/columns.

Manage Data Discovery Policies

Go to **Policy > Data Discovery Policies** to add/enable/disable/delete/import/export Data Discovery Policies.

The following table indicates columns and meanings in the Data Discovery Policies list.

Columns	Descriptions
Status	• Enabled ( ) • Disabled ( )
Policy Name	policy name
Policy Type	Built-in or User defined. The built-in policies cannot be deleted.
Match Rule	Match rule for searching data

Column Name Pattern	Pattern for matching table column's name.
	• Allow regular expression
	• Left blank for skipping column name match check
	• Data Discovery will check column name match first, and:
	  • if matched, continue to check sample data match
	  • if not matched, abort sample data match checking

Data Pattern	Pattern for matching sample data content. • Allow regular expression • Left blank(or regular expression ".+") for skipping sample data match check • If sample data matched with data pattern, will continue to check with Match Rule

Data Discovery Policy Groups

Data Discovery Policy Group will be assign to **Sensitive Data Discovery**, to search database for data discovery.

Go to **Policy > Data Discovery Policy Groups** to manage groups of Data Discovery Policy.

Click 'Group Name' to edit group, click 'Add' button to add new group, select group checkbox, and click 'Delete' button to delete group.

DAM Policy Management

Multiple Database Configuration from DAM Policy Management

DAM Policy Management enables you to configure policies for multiple databases. From the Monitoring Policy Management page, you can configure Metadata policies, Privilege Policies, and Compliance Policies. If you use the Policy Groups which consist of several policies, you can apply the policy group for the multiple target databases. You don't need to configure the same policy for each database.

To navigate to the Policies page, go to **Policy**> **DAM Policies** in the left-side tree menu.

Target based Configuration from Target Management

The target based configuration is useful when you configure a policy for a single target database. You can create or configure Data, Metadata, and Privilege policies from the Target Monitors page and Policies tab.

- FortiDB automatically creates a new data policy group, and
- FortiDB automatically associates the policy group to the target database

To configure a data policy for the individual target database, go to **Data Activity Monitoring** > Click on the target name > **Policies** tab.

Configuring Policies

The Monitoring Policy Management page displays all policies with Status, Policy Name, Severity, Supported Databases information.

This page allows you to:

- Configure Data policies: *Table Policy*, *Table and Column Policy*, *Session Policy*, and *User Policy*, by selecting the Data Policies dropdown list at the bottom of the page.
- Modify the pre-defined policies: *Privilege Policy*, *Metadata Policy*, and *Compliance Policy*, by clicking the policy name.
- Delete the user-defined policies (Data policies), by selecting the checkbox of the policy, and click Delete
- Filter the view by selecting a view from the View dropdown list.
- Navigate to the modifying the group page by clicking **Edit** button.
- Navigate to the searching and creating the group page by clicking **Search / New Group** button.

The following table indicates icons and meanings in the policy table list.

Columns	Descriptions
Type	Data Policy: •  **Table Policy** monitors suspicious reads and writes on specific tables •  **Table and Column Policy** monitors suspicious reads and writes on specific table columns •  **Session Policy** monitors suspicious session behavior

Columns	Descriptions
	•  **User Policy** monitors suspicious reads and writes by specific users Privilege policy is indicated as this icon  Metadata policy is indicated as this icon  Compliance policy is indicated as this icon 
Status	•  indicates the policy has a problem. •  indicates the policy is disabled. •  indicates the policy is enabled.
Policy Name	User defined policy name, or pre-defined name
Severity	User defined severity level. There are 5 levels of severity: • Informational (default) • Cautionary • Minor • Major • Critical
Supported Databases	All, or specify database type, or have fixed setting for each database

When add/edit a policy, set following base attributes in **Policy Info** field:

- Policy Name - enter unique name for policy, duplicate with exist policy name is not allowed.
- Description - enter a description if necessary.
- Enable - select **Enable** checkbox to enable policy
- Create new policy group for policy - For target-based configuration, Select the **Create new policy group for policy** checkbox (checked by default). If checked, the policy group will be automatically created and associated to the target database (This option is available for the target-based configuration: Data Access Monitoring > Monitors > click on the target name > Policies tab > Data Policies dropdown).
- Severity - select the severity
- Supported Database - For Data Policy, select supported database for the policy. Compliance Policy will be applied to All database. For Privilege and Metadata Policy, will have fixed settings for each database.

Data Policies

Data Policies monitor suspicious reads and writes on specific objects. They also monitor access to the database that takes place via your application server, location, or OS user.

To configure a data policy:

1. Go to **Data Activity Monitoring** > **Monitors** > click on the target name > **Policies** tab
2. Click on the target name for which you want to configure a policy.
3. Select a policy from the **Data Policies** dropdown.
4. Click **Add**, and set the policy base attributes, Audit Settings, and Alert Rule.

5 .Click **Save** to save policy.

Note: You can set **Supported Database** for Data Policy, with All or specified database. And if changed the **Supported Database** for a policy applied for a running monitoring target, you must **Stop Monitoring** and **Start Monitoring** to apply change, but not **Reconfigure**.

Configuring Table Policy

1 .In the **Data Policies** field, select **Table** from the Data Policies dropdown list.
2 .Select **Add**. The **Edit Policy** page displays.
3 .In the **Policy Info** field, set base attributes with Policy Name, Description, Enable, Severity, Supported Databases.
4 .To set Audit Settings, refer to *Setting or Modifying Audit Settings*
5 .To set Alert Rule, refer to:
- For Oracle, *Setting or Modifying Audit Rules*
- For MS SQL, *Setting or Modifying Alert Rules*
- For Sybase, *Setting or Modifying Alert Rules*
- For DB2, *Setting or Modifying Alert Rules*

6 .Select **Save**. The policy you created displays in the Data policy list.

Setting or Modifying Audit Settings (Table)

1 .Click the triangle icon of the **Audit Settings** section to expand.
2 .Select one of the following check boxes.
- **Manually Select Object:** You enter the specific object name.
- **Browse Object by Target**: You can select one from the dropdown list (default).

3 .Select a target from the **Target** dropdown list when you access from **Policy** > **DAM Policies** > **Data Policies** dropdown list.
4 .For Oracle and DB2, in the **Schema** field, select one from the dropdown list. For MS SQL Server and Sybase, select a database from the **Database** dropdown list, and then select a schema from the **Schema** dropdown list.
5 .From the **Tables** selection box, select one or more tables.
6 .Select the **Read** (Select)or **Write** (Insert/Update/Delete) checkbox or both in the **Audit Actions** field.
7 .Click the right arrow to move the selection to the **Selected Objects** table.

Note: If you want to remove the objects from the Selected Objects list, select the object you want to remove and click the left arrow.

8 .Configure Alerts Rules for each target database.

Setting or Modifying Alert Rules (Oracle)

1 .Click the triangle icon of the **Alert Rules** section to expand.
2 .In the **Combination Rule** field, select one from the dropdown list:

Options	Descriptions
Issue alert if ANY of the enabled rules are triggered	if you select this, each rule generates alerts individually.
Issue alert if ALL of the enabled rules are triggered	If you select this, the combination of selected policies generates alerts.

3 .Select the checkbox of your interests from the following rules:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.

Options	Descriptions
Suspicious OS User	Alert any successful access to selected object by certain OS users. You can specify one or more OS user names by typing the specific name or using a regular expression. 1 .Click **Add** 2 .Select an operator from the dropdown list. 3 .Enter OS user name depending on the operator you selected. • To generate alerts for the OS user(s) you specified in the list, check "Alert any successful access if the OS user is specified in the list " check box. • To generate alerts for the OS user(s) you didn't specified in the list, check " Alert any successful access if the OS user is not specified in the list " check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. 1 .Click **Add**. 2 .Select an operator from the dropdown list. 3 .Enter a location name depending on the operator you selected. 4 .Repeat 1 to 3 if necessary. • To generate alerts for any successful access from locations you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for any successful access from locations not in the list, check " Alert any successful access from locations in the list Alert any successful access from locations not in the list " check box.
Suspicious Database Users (Login Name)	Alert any successful access to selected object by certain database users. You can specify one or more users as follows: 1 .Select one or more users from the Users list. 2 .Click the right arrow to move the selections the Selected Users list. **Note:** If you want to remove the users from the selected users list, select the users you want to remove and click the left arrow. • To generate alerts for the database user(s) you specified in the list, check "Alert any successful access if the database user is in the list" check box.

Options	Descriptions
	• To generate alerts for the database user(s) you didn't specified in the list, check " Alert any successful access if the database user is not in the list " check box.
Suspicious Client Application (Client Id)	Alert any successful access to selected object by certain client applications. You can specify one or more client applications by typing the specific client application or using a regular expression. **1 .**Click Add. **2 .**Select an operator from the dropdown list. **3 .**Enter a client application depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for the client application you specified in the list, check "Alert any successful access if the client application is in the list " check box. • To generate alerts for the client application you didn't specified in the list, check " Alert any successful access if the client application is not in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. **1 .**Enter the number of accesses allowed. **2 .**Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 . Select Save or Cancel.

Setting or Modifying Alert Rules (MS SQL)

1 . Click the triangle icon of the **Alert Rules** section to expand.

2 . In the **Combination Rule** field, select one of the following options:

Options	Descriptions
Issue alert if ANY of the enabled rules are triggered	if you select this, each rule generates alerts individually.
Issue alert if ALL of the enabled rules are triggered	If you select this, the combination of selected policies generates alerts.

3 . Select the checkbox of your interests from the following rules and click the triangle icon of each section to expand:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious OS User	Alert any successful access to selected object by certain OS users (Windows authentication only). You can specify one or more OS user names by typing the specific name or using a regular expression. **1 .**Click **Add** **2 .**Select an operator from the dropdown list. **3 .**Enter OS user name depending on the operator you selected. **4 .**Check one of the following check boxes. • To generate alerts for the OS user(s) you specified in the list, check "Alert any successful access if the OS user is specified in the list " check box. • To generate alerts for the OS user(s) you didn't specified in the list, check " Alert any successful access if the OS user is not specified in the list " check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. **1 .**Click **Add** **2 .**Select an operator from the dropdown list. **3 .**Enter a location name depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for any successful access from locations you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for any successful access from locations not in the list, check " Alert any successful access from locations in the list Alert any successful access from locations not in the list " check box.
Suspicious Database Users	Alert any successful access to selected object by certain database users. You can specify one or more users as follows: **1 .**If you access from **DAM Policies Management**, the target you selected in the Audit Setting is displayed in the **Browse by targe**t dropdown list. **2 .**Select one or more users from the **Users** list. **3 .**Click the right arrow to move the selections the Selected Users list.

Options	Descriptions
	 **Note:** If you want to remove the users from the selected users list, select the users you want to remove and click the left arrow. • To generate alerts for the database user(s) you specified in the list, check "Alert any successful access if the database user is in the list" check box. • To generate alerts for the database user(s) you didn't specified in the list, check " Alert any successful access if the database user is not in the list " check box.
Suspicious Login Names	Alert any successful access to selected object by certain login users. You can specify one or more users as follows: **1 .**If you access from **DAM Policies Management**, the target you selected in the Audit Setting is displayed in the **Browse by targe**t dropdown list. **2 .**Select one or more users from the **Users** list. **3 .**Click the right arrow to move the selections the Selected Users list.  **Note:** If you want to remove the users from the selected users list, select the users you want to remove and click the left arrow. • To generate alerts for login user(s) you specified in the list, check "Alert any successful access if the login user is in the list " check box. • To generate alerts for login user(s) you didn't specified in the list, check " Alert any successful access if the login user is not in the list " check box.
Suspicious Client Application	Alert any successful access to selected object by certain client applications. You can specify one or more client applications by typing the specific client application or using a regular expression. **1 .**Click **Add** **2 .**Select an operator from the dropdown list. **3 .**Enter a client application depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for the client application(s) you specified in the list, check "Alert any successful access if the client application is in the list " check box. • To generate alerts for the client application(s) you didn't specified in the list, check " Alert any successful access if the client application is not in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot.

Options	Descriptions
	You can specify the maximum accesses allowed within a certain time period. 1 .Enter the number of accesses allowed in the **Threshold** field. 2 .Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 .Select **Save** or Cancel.

Setting or Modifying Alert Rules (Sybase)

1 .Click the triangle icon at **Alert Rules** to expand.

2 .In the **Combination Rule** field, select one from the following options:

Options	Descriptions
Issue alert if ANY of the enabled rules are triggered	if you select this, each rule generates alerts individually.
Issue alert if ALL of the enabled rules are triggered	If you select this, the combination of selected policies generates alerts.

3 .Select the checkbox of your interests from the following rules and click the triangle icon of each section to expand:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. 1 .Click **Add** 2 .Select an operator from the dropdown list. 3 .Enter a location name depending on the operator you selected. 4 .Repeat 1 to 3 if necessary. • To generate alerts for any successful access from locations you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for any successful access from locations not in the list, check " Alert any successful access from locations in the list Alert any successful access from locations not in the list " check box.

Options	Descriptions
Suspicious Login Names	Alert any successful access to selected object by certain login users. You can specify one or more users as follows: 1 .If you access from **DAM Policies Management**, the target you selected in the Audit Setting is displayed in the **Browse by targe**t dropdown list. 2 .Select one or more users from the **Users** list. 3 .Click the right arrow to move the selections the Selected Users list. **Note:** If you want to remove the users from the selected users list, select the users you want to remove and click the left arrow. • To generate alerts for login user(s) you specified in the list, check "Alert any successful access if the login user is in the list " check box. • To generate alerts for login user(s) you didn't specified in the list, check " Alert any successful access if the login user is not in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. 1 .Enter the number of accesses allowed in the **Threshold** field. 2 .Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by Location, Login User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 .Select **Save** or Cancel.

Setting or Modifying Alert Rules (DB2)

1 .Click the triangle icon at **Alert Rules** to expand.

2 .In the **Combination Rule** field, select one from the following options:

Options	Descriptions
Issue alert if ANY of the enabled rules are triggered	if you select this, each rule generates alerts individually.
Issue alert if ALL of the enabled rules are triggered	If you select this, the combination of selected policies generates alerts.

3 .Select the checkbox of your interests from the following rules and click the triangle icon of each section to expand:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. **1 .**Click **Add** **2 .**Select an operator from the dropdown list. **3 .**Enter a location name depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for any successful access from locations you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for any successful access from locations not in the list, check " Alert any successful access from locations in the list Alert any successful access from locations not in the list " check box.
Suspicious Database Users	Alert any successful access to selected object by certain database users. You can specify one or more users as follows: **1 .**If you access from **DAM Policies Management**, the target you selected in the Audit Setting is displayed in the **Browse by targe**t dropdown list. **2 .**Select one or more users from the **Users** list. **3 .**Click the right arrow to move the selections the Selected Users list. **Note:** If you want to remove the users from the selected users list, select the users you want to remove and click the left arrow. • To generate alerts for the database user(s) you specified in the list, check "Alert any successful access if the database user is in the list" check box. • To generate alerts for the database user(s) you didn't specified in the list, check " Alert any successful access if the database user is not in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. **1 .**Enter the number of accesses allowed in the **Threshold** field.

Options	Descriptions
	2 .Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 .Select **Save** or Cancel.

Setting or Modifying Alert Rules (MySQL)

1 .Click the triangle icon at **Alert Rules** to expand.

2 .In the **Combination Rule** field, select one from the following options:

Options	Descriptions
Issue alert if ANY of the enabled rules are triggered	if you select this, each rule generates alerts individually.
Issue alert if ALL of the enabled rules are triggered	If you select this, the combination of selected policies generates alerts.

3 .Select the checkbox of your interests from the following rules and click the triangle icon of each section to expand:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. 1 .Click **Add** 2 .Select an operator from the dropdown list. 3 .Enter a location name depending on the operator you selected. 4 .Repeat 1 to 3 if necessary. • To generate alerts for any successful access from locations you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for any successful access from locations not in the list, check " Alert any successful access from locations in the list Alert any successful access from locations not in the list " check box.
Suspicious Login Names	Alert any successful access to selected object by certain login users. You can specify one or more users as follows:

Options	Descriptions
	1 .If you access from **DAM Policies Management**, the target you selected in the Audit Setting is displayed in the **Browse by targe**t dropdown list. 2 .Select one or more users from the **Users** list. 3 .Click the right arrow to move the selections the Selected Users list.  **Note:** If you want to remove the users from the selected users list, select the users you want to remove and click the left arrow. • To generate alerts for login user(s) you specified in the list, check "Alert any successful access if the login user is in the list " check box. • To generate alerts for login user(s) you didn't specified in the list, check " Alert any successful access if the login user is not in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. 1 .Enter the number of accesses allowed in the **Threshold** field. 2 .Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by Location, Login User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 .Select **Save** or Cancel.

Configuring Table and Column Policy

1 .In the **Data Policies** field, select **Table and Column** from the Data Policies dropdown list.
2 .Select **Add**. The **Edit Policy** page displays.
3 .In the **Policy Info** field, set base attributes with Policy Name, Description, Enable, Severity, Supported Databases.
4 .To set Audit Settings, refer to *Setting or Modifying Audit Settings*
5 .To set Alert Rule, refer to:
- For Oracle, *Setting or Modifying Audit Rules*
- For MS SQL, *Setting or Modifying Alert Rules*
- For Sybase, *Setting or Modifying Alert Rules*
- For DB2, *Setting or Modifying Alert Rules*

6 .Select **Save**. The policy you created displays in the Data policy list.

Setting or Modifying Audit Settings (Table and column)

1 .Click the triangle icon at Audit Settings to expand.

2 .For Oracle and DB2, in the Schema field, select one from the pulldown list. For MS SQL Server and Sybase, select one from the pulldown list in the Database field, and then select one in the Owner field.
3 .From the Tables selection box, select one table.
4 .From the Column selection box, select one or more columns for the table you selected.
5 .Select the Read (Select)or Write (Insert/Update/Delete) checkbox or both in the Audit Actions field.
6 .Click the right arrow to move the selection to the Selected Objects table.

Note: If you want to remove the objects from the selected objects list, select the object you want to remove and click the left arrow.

7 .Configure Alert Rule for each target database.

Configuring Session Policy

1 .In the **Data Policies** field, select **Session** from the Data Policies dropdown list.
2 .Select **Add**. The **Edit Policy** page displays.
3 .In the **Policy Info** field, set base attributes with Policy Name, Description, Enable, Severity, Supported Databases.
4 .To set Audit Settings, refer to *Setting or Modifying Audit Settings*
5 .To set Alert Rule, refer to *Setting or Modifying Alert Rules*.
6 .Select **Save**. The policy you created displays in the Data policy list.

Setting or Modifying Audit Settings (Session)

1 .Click the triangle icon at Audit Settings to expand.
2 .From the Users selection box, select one or more users.
3 .Click the right arrow to move the selection to the Selected Objects table.

Note: If you want to remove the user from the selected users list, select the user you want to remove and click the left arrow.

4 .If you select the Apply alerts for all users checkbox, alerts will be generated for all users regardless of your users selection.
5 .Configure Alert Rule.

Setting or Modifying Alert Rules (all)

1 .Click the triangle icon at Alert Rules to expand.
2 .In the Combination Rule field, select one from the pulldown list:
- Issue alert if ANY of the enabled rules are triggered
- Issue alert if ALL of the enabled rules are triggered

3 .Select the checkbox of your interests from the following rules:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Login Failure	Failure to login due to invalid password.
Suspicious Login Time	Time of login is beyond specified normal hours. You can specify the time, entering numbers: 1 .In the From and To field, enter the starting and ending times you want to specify as suspicious login time. 2 .If necessary, click + sign to add more time range, or - sign to remove the time range. • To generate alerts for the login time you specified in the list, check "Alert if login time is within one of the time ranges in the list " check box.

Options	Descriptions
	• To generate alerts for the login time you didn't specified in the list, check " Alert if login time is NOT within one of the time ranges in the list" check box.
Extremely Long Session	Generate alerts when duration of session is abnormally long. You can specify the threshold by entering how many hours allowed for a session.
Excessive Read Activities	Generate alerts when number of logical page reads is abnormally high. You can specify the threshold by entering how many page reads are allowed for a session.
High Read Ratio	Generate alerts when number of logical reads/minute is abnormally high. You can specify the threshold by entering how many page reads are allowed for a session.
Suspicious Os User	Alert any successful access to selected object by certain OS users.  **Note:** For MS SQL Server, this rule is applicable for only Windows authentication. You can specify one or more OS user names by typing the specific name or using a regular expression. **1 .**Click Add **2 .**Select an operator from the pulldown list. **3 .**Enter OS user name depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for the OS user(s) you specified in the list, check "Alert any successful access if the OS user is specified in the list " check box. • To generate alerts for the OS user(s) you didn't specified in the list, check "Alert any successful access if the OS user is not specified in the list" check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. **1 .**Click Add **2 .**Select an operator from the pulldown list. **3 .**Enter a location name depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary.

Options	Descriptions
	• To generate alerts for location(s) you specified in the list, check "Alert any successful access from locations in the list" check box. • To generate alerts for location(s) you didn't specified in the list, check "Alert any successful access from locations not in the list" check box.

4 .Select Save or Cancel.

Configuring User Policy

1 .In the **Data Policies** field, select **User** from the Data Policies dropdown list.
2 .Select **Add**. The **Edit Policy** page displays.
3 .In the **Policy Info** field, set base attributes with Policy Name, Description, Enable, Severity, Supported Databases.
4 .To set Audit Settings, refer to *Setting or Modifying Audit Settings*
5 .To set Alert Rule, refer to:
- For Oracle, *Setting or Modifying Audit Rules*
- For MS SQL, *Setting or Modifying Alert Rules*
- For Sybase, *Setting or Modifying Alert Rules*
- For DB2, *Setting or Modifying Alert Rules*

6 .Select **Save**. The policy you created displays in the Data policy list.

Setting or Modifying Audit Settings (Users)

1 .Click the triangle icon of the **Audit Settings** section to expand.
2 .From the **Users** selection box, select one or more users.
3 .Click the right arrow to move the selection to the Selected Objects table.

Note: If you want to remove the user from the selected users list, select the user you want to remove and click the left arrow.

4 .Select the **Read (Select)**or **Write (Insert/Update/Delete)** checkbox or both in the **Audit Actions** field.
5 .If you select the **Apply alerts for all users** checkbox, alerts will be generated for all users regardless of your users selection.

Note: For DB2 target database, the **All alerts fro all users** checkbox is not available.

6 .Configure Alert Rule for each target database.

Setting or Modifying Alert Rules (User, Oracle)

1 .Click the triangle icon of the **Alert Rules** section to expand.
2 .In the **Combination Rule** field, select one from the dropdown list:

Options	Descriptions
Issue alert if ANY of the enabled rules are triggered	if you select this, each rule generates alerts individually.
Issue alert if ALL of the enabled rules are triggered	If you select this, the combination of selected policies generates alerts.

3 .Select the checkbox of your interests from the following rules:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.

Options	Descriptions
Suspicious OS User	Alert any successful access to selected object by certain OS users. You can specify one or more OS user names by typing the specific name or using a regular expression. 1 .Click **Add** 2 .Select an operator from the dropdown list. 3 .Enter OS user name depending on the operator you selected. • To generate alerts for the OS user(s) you specified in the list, check "Alert any successful access if the OS user is specified in the list " check box. • To generate alerts for the OS user(s) you didn't specified in the list, check " Alert any successful access if the OS user is not specified in the list " check box.
Suspicious Object Access	Alert any successful access to selected object(s). There are the following options to select objects: • Manually Select Object • Browse Object by Target (default) You can specify one or more objects as follows: 1 .Select a target from the Target dropdown list. 2 .Select a schema from the dropdown list. 3 .Select one or more tables from the Tables list. 4 .Select the Read (Select)or Write (Insert/Update/Delete) checkbox or both in the Audit Actions field. 5 .Click the right arrow to move the selections the Selected Objects list.  **Note:** If you want to remove the users from the selected objects list, select the objects you want to remove and click the left arrow. • To generate alerts for the object(s) you specified in the list, check "Issue alert if the accessed object is specified in the list " check box. • To generate alerts for the object(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. 1 .Click Add 2 .Select an operator from the dropdown list. 3 .Enter a location name depending on the operator you selected.

Options	Descriptions
	4 . Repeat 1 to 3 if necessary. • To generate alerts for the location(s) you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for the location(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Suspicious Client Application (Client Id)	Alert any successful access to selected object by certain client applications. You can specify one or more client applications by typing the specific client application or using a regular expression. **1 .**Click Add **2 .**Select an operator from the dropdown list. **3 .**Enter a client ID depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for the client application you specified in the list, check "Alert any successful access if the client application is in the list " check box. • To generate alerts for the client application you didn't specified in the list, check "Alert any successful access if the client application is not in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. **1 .**Enter the number of accesses allowed. **2 .**Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 . Select Save or Cancel.

Setting or Modifying Alert Rules (User, MS SQL)

1 . Click the triangle icon at Alert Rules to expand.

2 . In the Combination Rule field, select one from the pulldown list:

- Issue alert if ANY of the enabled rules are triggered
- Issue alert if ALL of the enabled rules are triggered

3 . Select the checkbox of your interests from the following rules:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious OS User	Alert any successful access to selected object by certain OS users (Windows authentication only). You can specify one or more OS user names by typing the specific name or using a regular expression. **1 .**Click Add **2 .**Select an operator from the pulldown list. **3 .**Enter OS user name depending on the operator you selected. • To generate alerts for the OS user(s) you specified in the list, check "Alert any successful access if the OS user is specified in the list " check box. • To generate alerts for the OS user(s) you didn't specified in the list, check " Alert any successful access if the OS user is not specified in the list " check box.
Suspicious Object Access	Alert any successful access to selected object(s). You can specify one or more objects as follows: **1 .**Select a schema from the pulldown list. **2 .**Select one or more tables from the Tables list. **3 .**Select the Read (Select)or Write (Insert/Update/Delete) checkbox or both in the Audit Actions field. **4 .**Click the right arrow to move the selections the Selected Objects list.  **Note:** If you want to remove the users from the selected objects list, select the objects you want to remove and click the left arrow. • To generate alerts for the object(s) you specified in the list, check "Issue alert if the accessed object is specified in the list " check box. • To generate alerts for the object(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. **1 .**Click Add **2 .**Select an operator from the pulldown list. **3 .**Enter a location name depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary.

Options	Descriptions
	• To generate alerts for the location(s) you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for the location(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Suspicious Client Application	Alert any successful access to selected object by certain client applications. You can specify one or more client applications by typing the specific client application or using a regular expression. **1 .**Click Add **2 .**Select an operator from the pulldown list. **3 .**Enter a client application depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for the client application(s) you specified in the list, check "Alert any successful access if the client application is in the list" check box. • To generate alerts for the client application(s) you didn't specified in the list, check "Alert any successful access if the client application is not in the list" check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. **1 .**Enter the number of accesses allowed. **2 .**Enter the number of hours, days, minutes, or seconds after selecting one from the pulldown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 . Select Save or Cancel.

Setting or Modifying Alert Rules (User, Sybase)

1 . Click the triangle icon at Alert Rules to expand.

2 . In the Combination Rule field, select one from the dropdown list:

- Issue alert if ANY of the enabled rules are triggered
- Issue alert if ALL of the enabled rules are triggered

3 . Select the checkbox of your interests from the following rules:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious OS User	Alert any successful access to selected object by certain OS users. You can specify one or more OS user names by typing the specific name or using a regular expression. **1 .**Click Add **2 .**Select an operator from the dropdown list. **3 .**Enter OS user name depending on the operator you selected. • To generate alerts for the OS user(s) you specified in the list, check "Alert any successful access if the OS user is specified in the list " check box. • To generate alerts for the OS user(s) you didn't specified in the list, check " Alert any successful access if the OS user is not specified in the list " check box.
Suspicious Object Access	Alert any successful access to selected object(s). You can specify one or more objects as follows: **1 .**Select a schema from the dropdown list. **2 .**Select one or more tables from the Tables list. **3 .**Select the Read (Select)or Write (Insert/Update/Delete) checkbox or both in the Audit Actions field. **4 .**Click the right arrow to move the selections the Selected Objects list.  **Note:** If you want to remove the users from the selected objects list, select the objects you want to remove and click the left arrow. • To generate alerts for the object(s) you specified in the list, check "Issue alert if the accessed object is specified in the list " check box. • To generate alerts for the object(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. **1 .**Click Add **2 .**Select an operator from the dropdown list. **3 .**Enter a location name depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary.

Options	Descriptions
	• To generate alerts for the location(s) you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for the location(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. **1 .**Enter the number of accesses allowed. **2 .**Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 . Select Save or Cancel.

Setting or Modifying Alert Rules (User, DB2)

1 . Click the triangle icon at Alert Rules to expand.
2 . In the Combination Rule field, select one from the pulldown list:
- Issue alert if ANY of the enabled rules are triggered
- Issue alert if ALL of the enabled rules are triggered

3 . Select the checkbox of your interests from the following rules:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious OS User	Alert any successful access to selected object by certain OS users. You can specify one or more OS user names by typing the specific name or using a regular expression. **1 .**Click Add **2 .**Select an operator from the pulldown list. **3 .**Enter OS user name depending on the operator you selected. • To generate alerts for the OS user(s) you specified in the list, check "Alert any successful access if the OS user is specified in the list " check box. • To generate alerts for the OS user(s) you didn't specified in the list, check " Alert any successful access if the OS user is not specified in the list " check box.

Options	Descriptions
Suspicious Object Access	Alert any successful access to selected object(s). You can specify one or more objects as follows: **1 .**Select a schema from the pulldown list. **2 .**Select one or more tables from the Tables list. **3 .**Select the Read (Select)or Write (Insert/Update/Delete) checkbox or both in the Audit Actions field. **4 .**Click the right arrow to move the selections the Selected Objects list.  **Note:** If you want to remove the users from the selected objects list, select the objects you want to remove and click the left arrow. • To generate alerts for the object(s) you specified in the list, check "Issue alert if the accessed object is specified in the list " check box. • To generate alerts for the object(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. **1 .**Click Add **2 .**Select an operator from the pulldown list. **3 .**Enter a location name depending on the operator you selected. **4 .**Repeat 1 to 3 if necessary. • To generate alerts for the location(s) you specified in the list, check "Alert any successful access from locations in the list " check box. • To generate alerts for the location(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. **1 .**Enter the number of accesses allowed. **2 .**Enter the number of hours, days, minutes, or seconds after selecting one from the pulldown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User

Options	Descriptions
	separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 .Select Save to save the settings, or Cancel to cancel your entry.

Setting or Modifying Alert Rules (User, MySQL)

1 .Click the triangle icon at Alert Rules to expand.

2 .In the Combination Rule field, select one from the dropdown list:

- Issue alert if ANY of the enabled rules are triggered
- Issue alert if ALL of the enabled rules are triggered

3 .Select the checkbox of your interests from the following rules:

Options	Descriptions
Security Violation	Alert any failed attempt to access selected object without proper permission.
Suspicious Object Access	Alert any successful access to selected object(s). You can specify one or more objects as follows: 1 .Select a schema from the dropdown list. 2 .Select one or more tables from the Tables list. 3 .Select the Read (Select)or Write (Insert/Update/Delete) checkbox or both in the Audit Actions field. 4 .Click the right arrow to move the selections the Selected Objects list.  **Note:** If you want to remove the users from the selected objects list, select the objects you want to remove and click the left arrow. • To generate alerts for the object(s) you specified in the list, check "Issue alert if the accessed object is specified in the list " check box. • To generate alerts for the object(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Suspicious Location	Alert any successful access to selected object from certain locations. You can specify one or more locations by typing the specific location or using a regular expression. 1 .Click Add 2 .Select an operator from the dropdown list. 3 .Enter a location name depending on the operator you selected. 4 .Repeat 1 to 3 if necessary. • To generate alerts for the location(s) you specified in the list, check "Alert any successful access from locations in the list " check box.

Options	Descriptions
	• To generate alerts for the location(s) you didn't specified in the list, check " Issue alert if the accessed object is not specified in the list " check box.
Time Violation	Alert excessive access to selected object within the specified time slot. You can specify the maximum accesses allowed within a certain time period. **1 .**Enter the number of accesses allowed. **2 .**Enter the number of hours, days, minutes, or seconds after selecting one from the dropdown list.
Tracking Strategy	Tracking rule selection for time violation. The threshold you set for time violation can be incremented by OS User, Location, Client Application, or Database User separately, depending on your selection. If you don't select any rule, any access to the selected audit settings will be counted.

4 . Select Save or Cancel.

Privilege Policies

Privilege Policies monitor changes of privilege settings in selected databases. If you select Privilege from the View dropdown list, you can see predefined privilege policies.

To configure a privilege policy:

- From DAM Policy Management

  Policy > DAM Policies
- From Data Activity Monitoring

  Data Activity Monitoring > Monitors > Click on the target name > Policies tab

Configuring Privilege Policy

You can choose global configuration or target based configuration for privilege policies. After creating a target database connection, take the following steps:

1 . For global configuration, go to **Policy** > **DAM Policies**. For target based configuration, go to **Data Activity Monitoring** > **Monitors** > click a target name > **Policies**.

2 .(For global configuration) Select **Privilege Policies** from the View dropdown list.

Note: The default Privilege Policies groups include privilege policies of all database types. If you want to view privilege policies of a certain database type, you can modify the filter of the Privilege policies group or create a new policy group. For details about modifying a policy group, see *DAM Policy Groups* .

3 . Click on the policy name you want to configure. The Edit Policy:<policy name> page displays.

4 . In the **Policy Info** field:

a) Enter a description if necessary.

b) Select the **Enable** checkbox. If checked, the policy will be enabled.

5 . Select one of the following severity options from the dropdown list.

- Informational (default, lowest severity level)

- Cautionary
- Minor
- Major
- Critical (highest severity level)

6 .Select **Save**.

Oracle Privilege Policies

This topic describes Oracle Privilege policies.

Privilege policies consist of the following policies:

Policy Names	Contents	Description
Column Privileges	Column-level privilege granting	This policy generates alerts when the column privileges are modified. For example, user SCOTT can grant SELECT privileges on a column of a table to a user, without letting that user SELECT on other columns in the same table.
Profiles	Resources (I/O, etc.) assigned to users	This policy generates alerts when the profiles are modified. Changes to any profile setting could have wide-reaching effects.
Role Privileges	Roles granted to users and other roles	This policy generates alerts when the role privileges are modified. It also contains information about which role has been assigned to other roles. Change of user's role means changes in user's access privileges. Role changes should be closely monitored in order to ensure data security.
Roles	Database roles	This policy generates alerts when the roles are modified. Contains information about all existing roles in the database.
System Privileges	All granted system privileges	This policy generates alerts when the system privileges are created, deleted, or modified. Contains all granted system privileges to all users or roles. System privileges are powerful privileges and should be granted with great cautions. Monitoring system-privilege changes should be mandatory.
Table Privileges	All granted schema-object privileges	This policy generates alerts when the table privileges are modified. Lists all granted privileges on schema objects. These include privileges on tables, views, sequences, procedures, functions and packages.

Policy Names	Contents	Description
User Privileges	Database users	This policy generates alerts when the users privileges are modified. Contains information about users in the database. Although this view has no privilege information, it contains the users to whom privileges may be assigned or changed.

MS SQL Server Privilege Policies

This topic describes MS SQL Server Privilege policies.

Privilege policies consist of the following policies:

Policy Names	Privileges involved	Description
Column Privileges	Column-level privilege	This policy generates alerts when the column privileges are modified.
Member Privileges	Role- and group-membership assignments	This policy generates alerts when the members are modified.
Object Privileges	Column- and table- and other object-level privileges	This policy generates alerts when the object privileges are modified.
Roles	All objects that are accessible by the current user	This policy generates alerts when the roles are modified. Contains information about all existing roles in the database.
Server Roles	Default server roles assigned to users.	This policy generates alerts when the server roles are modified.
User Privileges	Lists valid database users and the groups to which they belong	This policy generates alerts when the user privileges are modified.

Sybase Privilege Policies

This topic describes Sybase Privilege policies.

Privilege policies consist of the following policies:

Policy Names	Privileges involved	Description
Column Privileges	Column-level privilege	This policy generates alerts when the column privileges are modified.
Member Privileges	Role- and group-membership assignments	This policy generates alerts when the members privileges are modified.

Policy Names	Privileges involved	Description
Object Privileges	Column- and table- and other object-level privileges	This policy generates alerts when the object privileges are modified.
Procedures	Procedure privilege	This policy generates alerts when the procedures are modified.
Roles	All role groups as the server level.	This policy generates alerts when the role groups are modified.
Roles and Groups	All roles and groups. A group is a user group as the database level.	This policy generates alerts when the roles and groups are modified.
System Privileges	All granted system privileges	This policy generates alerts when the system privileges are modified.
User Privileges	Lists valid database users and the groups to which they belong	This policy generates alerts when the user privileges are modified.

DB2 Privilege Policies

This topic describes DB2 Privilege policies.

Privilege policies consist of the following policies:

Policy Names	Contents	Description
Column Privileges	column privileges	
Database Privileges	database system privileges	
Index Privileges	Index privileges	This view contains the right to DROP the index. The creator of an index automatically has this CONTROL privilege.
Package Privileges	A package is a database object grouping related procedures, functions, associated cursors, and variables together.	CONTROL: Provides the ability to rebind, drop, execute, and extend these package privileges to others. Only SYSADM and DBADM authorities can grant CONTROL privilege. BIND: Provides the privilege to rebind an existing package. EXECUTE: Provides the privilege to execute a package.
Schema Privileges	Objects within a schema : tables, views, indexes, packages, data types, functions, triggers, procedures, and aliases	CREATEIN: Provides the privilege to create objects within the schema. ALTERIN: Provides the privilege to alter objects within the schema. DROPIN: Provides the privilege to drop objects within the schema

Policy Names	Contents	Description
Table and View Privileges	Tables and view privileges	CONTROL: Provides the privilege to DROP the table or view and GRANT table or view privileges to somebody else. ALTER: Provides the privilege to add columns, comments, primary key or unique constraint, in order to create triggers, and create or drop check constraints DELETE: Provides the privilege to delete rows INDEX: Provides the privilege to CREATE INDEX INSERT: Provides the privilege to INSERT rows. REFERENCES: Provides the privilege to CREATE or DROP a foreign key. SELECT: Provides the privilege to retrieve data. UPDATE: Provides the privilege to change existing entries.
Tablespace Privileges	tablespace privileges	A SYSADM or SYSCTRL authority can create Tablespace and grant USE privilege to others

MySQL Privilege Policies

This topic describes MySQL Privilege policies.

Privilege policies consist of the following policies:

Policy Names	Privileges involved	Description
Column Privileges	Column-level privilege	This policy generates alerts when the column privileges are modified.
Object Privileges	Column- and table- and other object-level privileges	This policy generates alerts when the object privileges are modified.
Procedures	Procedure privilege	This policy generates alerts when the procedures are modified.

Metadata Policies

Metadata Policies monitor changes of metadata in selected databases. If you select Metadata from the View dropdown list, you can see predefined metadata policies.

To configure a metadata policy:

- From DAM Policy Management

  Policy > DAM Policies

- From Data Activity Monitoring

  Data Activity Monitoring > Monitors > Click on the target name > Policies tab

Configuring Metadata Policy

You can choose global configuration or target based configuration for metadata policies. After creating a target database connection, take the following steps:

1 .For global configuration, go to **Policy** > **DAM Policies**. For target based configuration, go to **Data Activity Monitoring** > **Monitors** > click a target name > **Policies**.

2 .(For global configuration) Select **Metadata Policies** from the View dropdown list.

Note: The default Metadata Policies groups include metadata policies of all database types. If you want to view metadata policies of a certain database type, you can modify the filter of the Metadata policies group or create a new policy group. For details about modifying a policy group, see *DAM Policy Groups* .

3 .Click on the policy name you want to configure. The Edit Policy:<policy name> page displays.

4 .In the **Policy Info** field:

a) Enter a description if necessary.

b) Select the **Enable** checkbox. If checked, the policy will be enabled.

5 .Select one of the following severity options from the dropdown list.

- Informational (default, lowest severity level)
- Cautionary
- Minor
- Major
- Critical (highest severity level)

6 .Select **Save**.

Oracle Metadata Policies

This topic describes Oracle Metadata policies.

Metadata policies consist of the following policies:

Policy Names	Contents	Description
Packages	packages	This policy generates alerts when database packages are modified.
Synonyms	synonyms	This policy generates alerts when database synonyms are modified.
Tables	tables, columns and indexes	This policy generates alerts when tables, columns, or indexes are modified.
Tablespaces	tablespaces	This policy generates alerts when table spaces are modified.
Triggers	triggers	This policy generates alerts when triggers are modified.
Views	views	This policy generates alerts when views are modified.

MS SQL Server Metadata Policies

This topic describes MS SQL Server Metadata policies.

Metadata policies consist of the following policies:

Policy Names	Contents	Description
Routines	routines	This policy generates alerts when database packages are modified.
Tables	tables, columns and indexes	This policy generates alerts when tables, columns, or indexes are modified.
Triggers	triggers	This policy generates alerts when triggers are modified.
Views	views	This policy generates alerts when views are modified.

Sybase Metadata Policies

This topic describes Sybase Metadata policies.

Metadata policies consist of the following policies:

Policy Names	Contents	Description
Indexes	indexes	This policy generates alerts when indexes are modified.
Stored Procedures	stored procedures	This policy generates alerts when stored procedures are modified.
Tables	tables, columns and indexes	This policy generates alerts when tables, columns, or indexes are modified.
Triggers	triggers	This policy generates alerts when triggers are modified.
Views	views	This policy generates alerts when views are modified.

DB2 Metadata Policies

This topic describes Oracle Metadata policies.

Metadata policies consist of the following policies:

Policy Names	Contents	Description
Aliases	aliases	This policy generates alerts when aliases are modified
Indexes	indexes	This policy generates alerts when indexes are modified
Packages	packages	This policy generates alerts when database packages are modified.
Tables	tables	This policy generates alerts when tables and columns are modified.
Tablespaces	tablespaces	This policy generates alerts when table spaces are modified.
Triggers	triggers	This policy generates alerts when triggers are modified.

Policy Names	Contents	Description
Views	views	This policy generates alerts when views are modified.

MySQL Metadata Policies

This topic describes MySQL Metadata policies.

Metadata policies consist of the following policies:

Policy Names	Contents	Description
Events	events	This policy generates alerts when events are modified.
Indexes	indexes	This policy generates alerts when indexes are modified.
Stored Procedures	stored procedures	This policy generates alerts when stored procedures are modified.
Tables	tables	This policy generates alerts when tables and columns are modified.
Triggers	triggers	This policy generates alerts when triggers are modified.
Views	views	This policy generates alerts when views are modified.

Compliance Policies

Compliance Policies capture all types of database activities and store the data in the internal repository. This policy can be used for generating the SOX compliance reports. For details about compliance reports, see *Compliance Reports*

To configure a compliance policy:

1. Go to **Policy** > **DAM Policies**
2. Select **Compliance Policies** from the **View** dropdown.
3. Click on **Compliance** in the Policy Name column.

Configuring Compliance Policy

In order to generate Compliance reports (except History of Privilege Changes), you need to set either Object audit options or User audit option. "History of Privilege Changes" report doesn't require objects or users settings. To configure the compliance policy, take the following steps:

1. Go to **Policy** > **DAM Policies**.
2. In the **View** field, select **Compliance Policies** from the View dropdown list.
3. Click on the policy name ("Compliance" by default).
   The **Edit Policy: Compliance** page will display.
4. Enter the following information if necessary.
   a) Enter a description.
   b) Select the **Enable** checkbox. If checked, the policy will be enabled.
5. Select one of the following severity options from the dropdown list.

- Informational (default, lowest severity level)
- Cautionary
- Minor
- Major
- Critical (highest severity level)

6 .For generating reports (except for History of Privilege Changes), set Object Audit Options or User Audit Options. For details about setting Object Audit Options and User Audit Options, *Setting or Modifying Audit Settings (Object Audit Options)* and *Setting or Modifying Audit Settings (User Audit Options)*

The Compliance report "History of Privilege Changes" does not require to set Audit Settings section.

7 .Select **Save**. The Target Monitor page displays.

Setting or Modifying Audit Settings (Object Audit Options)

This action is required for generating the following SOX reports: Abnormal or Unauthorized Changes to Data, Abnormal Use of Service Accounts, Abnormal Termination of Database Activity, and End of Period Adjustments.

1 .Click the triangle icon of the **Audit Settings** section to expand.

2 .In the **Select Objects to Audit** section, Select one of the check boxes. The following steps are based on the default setting of this field.

- **Manually Select Object:** You enter the specific object name.
- **Browse Object by Target**: You can select one from the dropdown list (default).

3 .In the **Target** field, select a target from the dropdown list.

4 .For Oracle and DB2, in the **Schema** field, select one from the dropdown list. For MS SQL Server and Sybase, select one from the dropdown list in the **Database** field, and then select one in the **Schema** field.

5 .From the **Tables** selection box, select one or more tables.

6 .Select the **Read** (Select)or **Write** (Insert/Update/Delete) checkbox or both in the **Audit Actions** field.

7 .Click the right arrow to move the selection to the Selected Objects table.

Note: If you want to remove the objects from the Selected Objects list, select the object you want to remove and click the left arrow.

8 .Click **Save**.

9 .Configure the User Audit Options for SOX reports "Abnormal Use of Service Accounts" and "Abnormal Termination of Database Activity". For details about setting the User Audit Options, go to "Setting or Modifying User Audit Options".

Setting or Modifying Audit Settings (User Audit Options)

This action is required for generating the following SOX reports: Abnormal Use of Service Accounts and Abnormal Termination of Database Activity.

1 .Click the triangle icon of the **Audit Settings** section to expand.

2 .In the **User Audit Options** section, select a target from the **Browse by target** dropdown list. You can enter a user name in the **Enter user** field.

3 .Click the right arrow to move the selection to the Selected Objects table.

Note: If you want to remove the objects from the Selected Objects list, select the object you want to remove and click the left arrow.

4 .Click **Save**.

DAM Policy Groups

The Policy Groups page displays all policy groups with groups names and descriptions.

In this page you can:

- Add a new policy group by selecting **Add**. See *Adding a New Policy Group*
- Modify the policy group by selecting the group name. See *Modifying the Existing Policy Groups*
- Delete the user-defined policy groups by selecting the group and click **Delete**.

This table shows which policies are included in the DAM per-defined policy groups.

Groups/ Policies	Complia	Table/ Columns	User	Session	Privilege	Metadata
Compliance Policies	X					
Data Policies		X	X	X		
Metadata Policies						X
Privilege Policies					X	

Adding a New Policy Group

This topics describe adding a new policy group.

1. Go to **Policy** > **DAM Policy Groups**
2. In the Policy Groups page, click **Add**.
3. Enter a policy group name in the Group Name field (required).
4. (optional) Enter descriptions in the Description field to describe your filtering/grouping criteria.
5. Create a filtering condition by taking the following steps:
   a) Select a column on the **Column** dropdown on which you would like to filter.
   b) Select an operator from the **Operator** dropdown that associates the column you selected.
   c) Select a value from the **Value** dropdown that the **Column** must match, and click the right arrow to move the selection to the right box.
   d) You can add or subtract, respectively, filtering criteria rows by selecting the **+ (plus)** or **- (minus)** buttons.

   Note: In order to cancel creating a new policy-group filter and go back to the main **Policies** page, select the  icon.

   Here are some examples of filtering criteria:

   Table 7 : Filtering Criteria Examples

Column	Operator	Value	Return Possibilities
Database Type	Equals	DB2	All policies associated with DB2 databases
Policy Type	Equals	Metadata Policies	Metadata policies associated with DB2 databases

6. To test your filtering criteria, select the **Apply** button.

7 .
To save the group you created, select the  icon.

Note: In order to modify an existing group, select the **Name** of the group on the **Policy Groups** page.

8 .Associate the policy group to a target database.

a) Select the Targets tab.
b) Select the targets to be associated with the policy group, and click the right arrow to move the selection to the right box.

9 .Click **Save**.

Modifying the Existing Policy Groups

This topics describe modifying the existing policy group.

1 .Go to **Policy** > **DAM Policy Groups**
2 .In the Policy Groups page, click on the name of the policy group you want to modify.
3 .Modify the filtering condition by taking the following steps:

a) Select a column on the **Column** dropdown on which you would like to filter.
b) Select an operator from the **Operator** dropdown that associates the column you selected.
c) Select a value from the **Value** dropdown that the condition must match, and click the right arrow to move the selection to the right box.
d) You can add or subtract, respectively, filtering criteria rows by selecting the **+ (plus)** or **- (minus)** buttons.

Note: In order to cancel creating policy-group filter and go back to the main **Policies** page, select the  icon.

4 .To test your filtering criteria, select the **Apply** button.
5 .
To save the group you created, select the  icon.
6 .Modify the target databases associated to the policy group.

a) Select the **Targets** tab.
b) Modify the selected target databases by selecting the target name first and either the right arrow or the left arrow to move the selection.

7 .Click **Save**.

Deleting the Policy Group

This topics describe deleting the existing user-defined policy groups. Pre-defined policy groups cannot be deleted.

1 .Go to **Policy** > **DAM Policy Groups**
2 .In the Policy Groups page, select the checkbox(es) of user-defined policies.

Note: The pre-defined policy groups will not be deleted.

3 .Click **Delete**.
The policy will be deleted from the list.

Assessment Management

Adding (or Modifying) Assessments

This topic describes the task of adding (or modifying) FortiDB assessments. For a successful assessment, you must:

- Create, or use an existing, target-base group which contains at least one valid target database
- Create, or use an existing, policy group which contains at least one working policy

Note: FortiDB does not perform an automatic session timeout after a certain period of time has elapsed. For example, if you leave assessment results on your screen while at lunch, unauthorized individuals could see this information. Therefore, you should logout or close your browser if you expect to leave your machine unattended.

Note: Items marked with an asterisk (*) on data-entry forms are mandatory.

1. Go to the **Assessments** page by selecting the **Assessments** link in the **Assessment Management** section on the left-side tree-navigation menu.
2. Select the **Add** button. (or, to modify a user, select the **Name** of the assessment you would like to change.)
3. On the subsequent **Assessment** page (**General** tab) , enter the requested items: an **Assessment Name** so that you can reuse it later and (optionally) a **Description** of your assessment. Then configure your assessment using the tabs on the web page.
4. In the **Targets** tab, specify which target-database groups you want to assess.
   a) Select one or more target-database groups from the **Available Target Groups** list on the left and add them to the **Assigned Target Groups** list by selecting the  button.
   In order to remove a target-database group from **Assigned Target Groups** list on the right, select the  button.
5. In the **Policies** tab, specify which target-database groups you want to assess.
   a) Select one or more target-database groups from the **Available Policy Groups** list on the left and add them to the **Assigned Policy Groups** list by selecting the right-arrow button. (In order to remove a policy group from the **Assigned Policy Groups** list , select the left-arrow button.)
   b) In order to see the policies associated with a policy group, select the group of interest in either the **Available Policy Groups** list or the **Assigned Policy Groups** list. The list of policies should then show up in the **Active Policies** list on the right.

Running Assessments

This topic explains how to run an assessment immediately and via a schedule.

On the **Scheduling** tab of the **Assessment** page, select either the **Run once** radio button, which enables you to specify the time and date for a single assessment run, or the **Recurring** radio button, which enables you to schedule a series of assessments.

Running an Assessment Immediately

This topic explains how to run an assessment immediately.

1. Go to the **Assessments** page.
2. Select the assessment of interest.

3 .Select the **Run** button.

Running an Assessment At a Specified Date and Time

This topic explains how to run an assessment at a specified date and time.

1 .After you select the **Run once** radio button:
   a) In the **Starts at** field group, specify a starting date directly, use the default, or alternatively, select the calendar icon, and then select a date.
2 .Select the **Enable Schedule** checkbox if you want to activate your schedule. (By default, your assessment schedule is disabled so that you can configure it without activating it.)
3 .Select the **Save** button to save your schedule.

Running Scheduled Assessments

This topic explains how to schedule an assessment.

1 .After you select the **Recurring** radio button:
   a) In the **Starts at** field group, specify a starting date directly, use the default, or alternatively, select the calendar icon, and then select a date.
2 .Select one of the radio buttons in the **Recurrence pattern** field group.
   - If you choose the **Hourly** radio button, you can then specify the hourly interval in the **Every __ hours** field.
   - If you choose the **Daily** radio button, you can then specify the daily interval in the **Every __ days** field.
   - If you choose the **Weekly** radio button, you can then specify the day(s) of the week on which you want your weekly assessments to run.
   - If you choose the **Monthly** radio button, you can then specify which day(s) during which month(s) you want your assessment to run. The **Day** radio button and adjacent dropdown list allows you to specify the numeric day for your assessment to run in each specified month. Alternatively, you may specify the day in each month, such as the 'first Monday', using the two provided dropdown lists.

   a) In the **Starts at** field group, specify a starting time or use the default.
   b) In the **Recurrence pattern** field group, select the **Hourly** , **Daily** , **Weekly** , or **Monthly** radio button.
   c) In the **Ends by** field group, you can leave the default **No end date** radio button selected or select the **End by** radio button and then specify a particular date at which you want your schedule to end by selecting on the calendar icon.
3 .Select the **Enable Schedule** checkbox if you want to activate your schedule. (By default, your assessment schedule is disabled so that you can configure it without activating it.)
4 .In the Administrative Domains section, you can select which users this scheduled task will be applicable for. Remember that users may only manage specific targets, so this section provides a way to perform assessments on particular targets. If one or more of the selected users manages all targets, then assessments will be performed on all applicable targets for this VA scan.
5 .Select the **Save** button to save your schedule.

Assessment Notifications

This topic describes the task of configuring how and to whom assessment notifications will be sent. You can choose email and/or SNMP-trap notifications of these issues.

1 .In the **Desired Notification format(s)** section of the **Notifications** tab, select the **Target Level** (default) and/or the **Rule Level** checkbox(es).
   - Target-level notifications contain a target-database-level summary of issues discovered during the assessment.
   - Rule-level notifications contain detail for every discovered issue.
2 .Select the **Enable Email** and/or the **Enable SNMP Trap** checkbox(es) in order to enable email and/or SNMP notifications, respectively, of assessment-discovered issues.

a) For email notifications, you must designate one or more email receivers. Select one or more of the entries in the **Available Receivers** list box and add them to the **Selected Receivers** list on the right by selecting on the right-arrow button.

Note: When the email receiver cannot be reached, it is your email server's responsibility to retry sending the email.

Note: In order to remove receiver(s), select them in the **Selected Receivers** list and select the left-arrow button.

Note: In order to see the details associated with any receiver, select the name of a receiver in either the **Available Receivers** or **Selected Receivers** lists and those details will appear in **Receiver Details** list on the right.

b) For SNMP notifications, you should set the **Notification** properties in the **System Configuration** component of the FortiDB application.

Note: The non-appliance version of FortiDB ships with MIB files in the *$FortiDB_HOME/etc/snmp* directory.

3 .(Optional) If you want to attach reports to the e-mail notification, go to the **Reports** tab and select the **Attach reports to selected e-mail receivers** checkbox, and make sure to select one or more report(s) and format(s). Note that the **Enable Report Generation to Disk** option is not required to be selected to use this capability.

Notification OIDs for Target-Level Assessments

Here are OIDs, and their descriptions, for target-level assessment notifications.

Here is an example of a trap for a target-database-level SNMP notification:

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.12356.104.0.6
SNMPv2-SMI::enterprises.12356.104.0.105 = STRING: "Tue Dec 04
 17:38:15 PST 2007"
SNMPv2-SMI::enterprises.12356.104.0.107 = STRING: "Test Target"
SNMPv2-SMI::enterprises.12356.104.0.123 = STRING: "Test
 Assessment"
SNMPv2-SMI::enterprises.12356.104.0.124 = STRING: "jdoe.fdb.com"
SNMPv2-SMI::enterprises.12356.104.0.125 = STRING: "158"
SNMPv2-SMI::enterprises.12356.104.0.126 = STRING: "36"
SNMPv2-SMI::enterprises.12356.104.0.127 = STRING: "10"
SNMPv2-SMI::enterprises.12356.104.0.128 = STRING: "0"
SNMPv2-SMI::enterprises.12356.104.0.129 = STRING: "2"
SNMPv2-SMI::enterprises.12356.104.0.130 = STRING: "4"
SNMPv2-SMI::enterprises.12356.104.0.131 = STRING: "20"
```

Here are the OID descriptions:

Table 8 : OID Description Table

OID	Meaning
SNMPv2-SMI::enterprises.12356	Fortinet enterprise ID
SNMPv2-SMI::enterprises.12356.104	FortiDB product ID
SNMPv2-SMI::enterprises.12356.104.0.6	VA Alert Trap/Notification
SNMPv2-SMI::enterprises.12356.104.0.105	assessment Time
SNMPv2-SMI::enterprises.12356.104.0.107	Target Name

SNMPv2-SMI::enterprises.12356.104.0.123	Assessment Name
SNMPv2-SMI::enterprises.12356.104.0.124	FortiDB host name
SNMPv2-SMI::enterprises.12356.104.0.125	Policy count
SNMPv2-SMI::enterprises.12356.104.0.126	Total Failed Count
SNMPv2-SMI::enterprises.12356.104.0.127	Critical failure count
SNMPv2-SMI::enterprises.12356.104.0.128	Major failure count
SNMPv2-SMI::enterprises.12356.104.0.129	Minor failure count
SNMPv2-SMI::enterprises.12356.104.0.130	Caution failure count
SNMPv2-SMI::enterprises.12356.104.0.131	Informational count

Notification OIDs for Rule-Level Assessments

Here are OIDs, and their descriptions, for rule-level assessment notifications.

Here is an example of formatted traps for a rule-level SNMP notification. Here is the trap with the target-database information:

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (73) 0:00:00.73
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.12356.104.0.8
SNMPv2-SMI::enterprises.12356.104.0.123 = STRING: "Test
 Assessment"
SNMPv2-SMI::enterprises.12356.104.0.107 = STRING: "Test Target"
SNMPv2-SMI::enterprises.12356.104.0.124 = STRING: "jdoe.fdb.com"
SNMPv2-SMI::enterprises.12356.104.0.105 = STRING: "Thu Dec 06
 16:26:26 PST 2007"
SNMPv2-SMI::enterprises.12356.104.0.125 = STRING: "158"
SNMPv2-SMI::enterprises.12356.104.0.126 = STRING: "36"
SNMPv2-SMI::enterprises.12356.104.0.127 = STRING: "10"
SNMPv2-SMI::enterprises.12356.104.0.128 = STRING: "0"
SNMPv2-SMI::enterprises.12356.104.0.129 = STRING: "2"
SNMPv2-SMI::enterprises.12356.104.0.130 = STRING: "4"
SNMPv2-SMI::enterprises.12356.104.0.131 = STRING: "20"
```

Next is the trap with the rule information:

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (84) 0:00:00.84
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.12356.104.0.6
SNMPv2-SMI::enterprises.12356.104.0.132 = STRING: "6501"
SNMPv2-SMI::enterprises.12356.104.0.102 = STRING: "MINOR"
SNMPv2-SMI::enterprises.12356.104.0.103 = STRING: "DVA ORCL 01.01
 Lock and Expire
Unused Default Accounts"
SNMPv2-SMI::enterprises.12356.104.0.106 = STRING:
 "VA@jdoe.fdb.com"
SNMPv2-SMI::enterprises.12356.104.0.107 = STRING: "Test Target"
SNMPv2-SMI::enterprises.12356.104.0.123 = STRING: "Test
 Assessment"
SNMPv2-SMI::enterprises.12356.104.0.105 = STRING: "Thu Dec 06
 16:26:26 PST 2007"
```

And here are the OID descriptions:

Table 9 : OID Description Table

OID	Meaning
SNMPv2-SMI::enterprises.12356	Fortinet enterprise ID
SNMPv2-SMI::enterprises.12356.104	FortiDB product ID
SNMPv2-SMI::enterprises.12356.104.0.6	VA Alert Trap/Notification
SNMPv2-SMI::enterprises.12356.104.0.8	VA Target Level Alert Trap/Notification
SNMPv2-SMI::enterprises.12356.104.0.102	Severity
SNMPv2-SMI::enterprises.12356.104.0.103	Policy Name
SNMPv2-SMI::enterprises.12356.104.0.105	Assessment Time
SNMPv2-SMI::enterprises.12356.104.0.106	Application name@ server name
SNMPv2-SMI::enterprises.12356.104.0.107	Target Name
SNMPv2-SMI::enterprises.12356.104.0.123	Assessment Name
SNMPv2-SMI::enterprises.12356.104.0.107	Target Name
SNMPv2-SMI::enterprises.12356.104.0.124	FortiDB host name
SNMPv2-SMI::enterprises.12356.104.0.125	Policy count
SNMPv2-SMI::enterprises.12356.104.0.126	Total Failed Count
SNMPv2-SMI::enterprises.12356.104.0.127	Critical failure count
SNMPv2-SMI::enterprises.12356.104.0.128	Major failure count
SNMPv2-SMI::enterprises.12356.104.0.129	Minor failure count
SNMPv2-SMI::enterprises.12356.104.0.130	Caution failure count
SNMPv2-SMI::enterprises.12356.104.0.131	Informational count
SNMPv2-SMI::enterprises.12356.104.0.132	Policy ID

Assessment Reports

This topic describes the task by which you choose which reports you want for your assessment. For example, you might want just a Summary Report, just a Detailed Report, or both.

1. Go to **Assessment Management** > **Assessment**
2. Select one of the Assessment name.
3. Click the **Reports** tab.
4. Specify which report you want for your assessment.
   a) Select one or more report groups from the **Available Reports**: list on the left and add them to the **Selected Reports** list box by clicking on the right-arrow button. (In order to remove a report from the **Selected Reports** list, select the left-arrow button.)

   Note: In order to see a report description, select the report of interest in the **Selected Reports** list box and then the description should show up in the **Report Description** list box on the right.

   b) Check the **Enable Report** checkbox.
5. In the **Report formats** field group:
   a) Enable one or more of the following checkboxes: **PDF (.pdf)** (the default), **Excel (.xls)**, **Comma Delimited (.csv)**, and/or **Tab Delimited (.txt)**.

6 .Select the **Save** button

Evaluating Assessment Results and Aborting Assessments

The **Results** tab of the **Assessment** page allows you to review assessment results and to abort assessments.

1 .Select an assessment's **Start Time** (in the top table) in order to view the target databases involved.
2 .To see target-specific results, select a name in the **Target** column in the bottom table.
3 .You can abort an entire assessment or the assessment of a particular target on this tab.

- In order to abort an entire assessment, check the row of interest in the top table and then select the **Abort** button below that table.
- In order to abort the assessment of a particular target database within an assessment, after clicking on an assessment's **Start Time** in the top table, check the row of interest in the bottom table and then select the **Abort** button below the bottom table.

Assessment Results

The **Results** tab shows you the status and other information about your assessments, completed or not.

Column Descriptions

The Results tab shows the following columns:

Table 10 : Assessment Results Columns

Column Name	Description
Status	The current status of the assessment
DB Type	The type of your target database
Failed (Cri,Maj,Min,Cau)	The number of failed policies by Severity type where: • **Cri** is Critical • **Maj** is Major • **Min** is Minor • **Cau** is Cautionary
Passed	The number of passed policies
Informational	The number of Informational policies
Errors	The number of policies for which errors were returned
Total	The total number of policies incorporated by the assessment

Status Icons

Assessments can be in any one of the following states:

Table 11 : Assessment Status Icons

Status-Column Icon	Description
	Running
	Idle
	Queued

Status-Column Icon	Description
	Completed
	Error
	Aborted

Deleting Assessments

This topic describes how to delete previously run assessments.

1. Go to the **Assessments** page.
2. Select the checkbox(es) corresponding to the assessment(s) you want to delete.
3. Select the **Delete** button.

Assessment History

The Assessment History page displays the run assessments and scheduled reports in disk.

Assessment History

Display all run assessment in this list page.

Click the link of **Target** to view the Detailed Report of this assessment.

Select the assessment reocrd(s), click the **Delete** button to delete.

Scheduled Reports

When enable the option **"Save Scheduled Assessment Report to Disk File"** in **Assessment** -> **Report** tab, the selected report files will be saved in disk after running the scheduled assessment.

Go to **Scheduled Reports** tab page, to download report files, or delete.

VA Privilege Summary

This topic describes how to display and export the Privilege Summary.

In order to view the Privilege Summary, you must have the Operations Manager role.

The Privilege Summary shows who has access to what in your target databases. As such, it can:

- Help you establish a baseline for your security system
- Show you if any users have more privileges than they need in order to do their jobs
- Show you if any roles (or, for DB2, groups) include more privileges than necessary
- Provide a common place to review privilege assignments for all FortiDB-supported target DB types
- Eliminate the need to execute the SQL statements to get privilege-assignment information

1. In order to display the **Privilege Summary** page, select the **Privilege Summary** link in the **Assessment Management** section of the left-side tree-navigation menu.
2. From the **Target Group** dropdown list, select the target-database group containing the target database for which you want to see a Privilege Summary.

3 .From the **Target** dropdown list , select the target database for which you want to see a Privilege Summary.

Note: MS SQL Server and Sybase targets may be accessed individually via database-level connections or, as a group, via server-level connections

4 .From the **Database Name** dropdown list , select the name of the database for which you want to see a Privilege Summary.

5 .Select the **Users** tab in order to see a list of users, or the **Roles** tab in order to see a list of roles, for the database whose name you selected .

Note: MySQL does not support roles or groups of privileges. There is no role tab for MySQL target databases.

Note: In MySQL a user is identified by a combination of a user name and host name, such as `root@localhost', or 'navicat@172.21.12.3'. Therefore two users with the same name but at different hosts, can have different privileges.

a) Once you have selected a user or role, you can then use the **Privilege Type** or **Classification** dropdown lists in order to filter the displayed information.
The subsequently available privilege information depends on:

- FortiDB-user access having already been given to certain target-database system tables, catalogs, and/or views. (See the **Target Privilege Matrix** for a list of the appropriate tables.)
- The particular combination of Privilege Type and Classification choices you make. (See the **DB-Type Distinctions** link below for more information on these choices.)

b) Optionally, you may export most of the information displayed when viewing a Privilege Summary. You may choose among these file formats:

- PDF (**Portrait** (the default) or **Landscape** orientation)
- Tab-delimited (.txt)
- Comma-separated-values (.csv)

DB-Type Distinctions

The Privilege Summary varies slightly by the DB type of the target database.

General Differences

There are differences by RDBMS type:

- The **Users** tabs are used for all RDBMS types.
- The **Roles** tab are used for all RDBMS types, except for MySQL which does not support roles. For DB2 target database, **Roles** means Groups.

Filtering Differences

After selecting a specific user name on the **Users** tab, or a specific role on the **Roles** tab, you can filter the displayed privilege information via:

- For Oracle, DB2, MS SQL Server, and Sybase, the **Privilege Type** dropdown offers these choices:
  - **Direct** which refers to privileges that have been directly assigned (i.e., not via roles) to the selected user name
  - **Indirect** which refers to privileges that have been assigned via roles to the selected user name

  Note: MySQL applies the **Direct** type only.
- For Oracle, the **Classification** dropdown offers these choices:
  - **Object Privileges** which refers to privileges that pertain to a specific schema or object

    - **System Privileges** which refers to privileges that do not pertain to a specific schema or object
- For DB2, the **Classification** dropdown offers these choices:
    - **Column Auth** which refers to privilege information on certain columns
    - **DB Auth**which refers to privilege information on certain databases
    - **Index Auth** which refers to privilege information on certain indexes
    - **Package Auth** which refers to privilege information on certain packages
    - **Schema Auth** which refers to privilege information on certain schemas
    - **Table Auth** which refers to privilege information on certain tables
    - **Tablespace Auth** which refers to privilege information on certain tablespaces
- For MySQL, the **Classification** dropdown offers these choices:
    - **Column Level** which refers to privilege information on certain columns. Granting/Revoking grant option is applied for all privileges within the same table only.
    - **Schema Level** which refers to privilege information on certain databases. Granting/Revoking grant option is applied for all privileges.
    - **Table Level** which refers to privilege information on certain tables. Granting/Revoking grant option is applied for all privileges within the same table only.
    - **User Level** which refers to privilege information applied to all databases on the database server. Granting/Revoking grant option is applied for all privileges.

Column and Column-Value Differences

The column names and values used by the Privilege Summary vary by the DB type of your target database. For more information, see the documentation provided by your database vendor for system tables, views, and/or catalogs.

VA Global Summary

The Global Summary page displays the summary information for all targets.

The summary information includes statistics of assessments, and vulnerabilities found by assessment.

If you run more than once assessments to same target, this global summary only summarizes the latest one assessment.

For found vulnerabilities (failed checking items in assessment scan), this page also displays category statistics, includes by severity, classification, and by database type.

Sensitive Data Discovery

This topic describes the sensitive data discovery.

Note:

This feature is only working with Oracle and MSSQL target database.

And you need define target database before using this feature.

Manage Sensitive Data Discovery

Before starting define/run sensitive data discovery, you must define and enable **Data Discovery Policy** first, and add policies to group(s).

See *Data Discovery Policies and Policy Groups* for data discovery policy management.

Go to **Vulnerability Assessment > Sensitive Data Discovery** to manage data discovery.

In the list page:

- Status: indicates discovery is running (active) or not(inactive).
- Data Discovery Policy Group: which policy groups are assigned to this discovery.
- Last Discovery: Last discovery time and found result, click to view detail report.

Click 'Target Name' in list to add/modify data discovery:

- Target tab: select database metadata as discovery object(s).
- Policy Group tab: select discovery policy group to assign to this discovery.
- Result tab: after run discovery, check this tab for result summary.

And click 'Save' button to save discovery definition.

Run Sensitive Data Discovery

In discovery add/modify page, click 'Save & Start Scan' button to save and start discovery.

In discovery list page, select one or more discovery with checkbox(es), click 'Start Scan' button to start discovery, click 'Stop Scan' button to stop.

Sensitive Data Discovery Report

There are two pre-defined data discovery reports - detailed and summary report.

In discovery list page, click result link in 'Last Discovery' column, to view detailed report.

Go to **Report > Pre-Defined VA Reports**, click 'Sensitive Data Discovery Detailed Report', or 'Sensitive Data Discovery Summary Report', to view or export report.

Data Activity Monitoring

Target Monitors

The Target Monitors page provides a centralized management for monitoring target databases. You can view monitoring status, policies you configures, start and stop monitoring. You can also associate policy groups to your target databases and view generated alerts.

When you click on each target name, the following tabs and functionalities are available:

Tabs	Purposes
General	Settings of audit configuration for each target database. You can start and stop monitoring and auditing in this page. It also shows monitoring and auditing status.
Policies	Shows the available policies with information, such as policy type, status, name, and severity. You can create Data policies from this page. You can also associate policy groups to the selected target database.
Policy Groups	Associate the policy group to your target database
Alerts	Shows all alerts with policy information. You can filter alerts by policies. The Advanced option allows you to filter by date range, policy names, or severity.
Logs	History of activities for a selected target.
Audit Management	For Oracle, this page shows the issued audit command and all audit commands for each object. For MS SQL Server, this page shows audited events and audited filters used by FortiDB. This page is not applicable for Sybase.

The following buttons and icons are available:

Buttons and icons	Description
Start Monitoring	This button starts monitoring for the target database. You must select the target first.
Stop Monitoring	This button stops monitoring. You must select the target first.
Reconfigure	This button is only available when the target needs to be reconfigured.
Batch Edit	This button is useful when you want to apply the **Same policy groups** against multiple targets.  **Note:** A previously-applied mapping set will be replaced with the new mapping set on the multiple targets you selected. As a result, you might lose the policy groups that were previously mapped to some of the selected target.

Choosing a Collection Method

This topic describes monitoring and auditing options to choose a collection method for your target database.

Oracle Audit Configuration

FortiDB can collect audit information using several methods. Select the type of agent you have configured your target with. The **Test** button will confirm that FortiDB can monitor your system with the type you select. For details, see *Configuring the Oracle Target Database*

Fields	Descriptions
Collection Method	You can select one of the following options: • DB,EXTENDED • XML File Agent • SGA Agent (for Oracle 10gR2 on Solaris only) • Net Agent • TCP/IP Sniffer(available with FortiDB appliance only) Click the **Test** button to confirm the connection with the method you selected (not for 'TCP/IP Sniffer').
Polling Frequency (ms)	Polling frequency for audit collection. This field applies only DB,EXTENDED collection methods. **Note:** When you change the value of Polling frequency, you must stop and start monitoring.
TCP/IP Sniffer Settings	Specify: • Target database version • FortiDB port connecting to network switch's SPAN port • Enable/Disable to save sniffer audit log See *Configuring Monitoring with TCP/IP Sniffer* for detail

MS SQL Server Audit Configuration

FortiDB uses SQL Trace for collecting audit information. Select SQL Trace as the Collection Method. You must specify the folder where your server writes the trace information. For details, see *Configuring the MS SQL Server Target Database*

Fields	Descriptions
Collection Method	• SQL Trace - Click the **Test** button to confirm the connection with the method you selected. • Net Agent • TCP/IP Sniffer(available with FortiDB appliance only)
Trace Folder	Enter the full path of the audit trace folder here.
Polling Frequency (ms)	Polling frequency for audit collection. This field applies only SQL Trace collection methods. **Note:** When you change the value of Polling frequency, you must stop and start monitoring.

Fields	Descriptions
TCP/IP Sniffer Settings	Specify: • Target database version • SSL Certification Private Key file and Key Password, for encrypted connection • FortiDB port connecting to network switch's SPAN port • Enable/Disable to save sniffer audit log See *Configuring Monitoring with TCP/IP Sniffer* for detail

DB2 Audit Configuration

FortiDB uses the DB2 agent for collecting audit information. You must configure your DB2 system for auditing. In addition you must install and start the FortiDB DB2 audit agent. For details, see *Configuring the DB2 Target Database*

Fields	Descriptions
Collection Method	• DB2 Agent Click the **Test** button to confirm the connection with the method you selected. • TCP/IP Sniffer(available with FortiDB appliance only)
TCP/IP Sniffer Settings	Specify: • Target database version • FortiDB port connecting to network switch's SPAN port • Enable/Disable to save sniffer audit log See *Configuring Monitoring with TCP/IP Sniffer* for detail

Sybase Audit Configuration

FortiDB uses the Sybase Monitoring and Data Access (MDA) tables for collecting audit information. You must configure your server to enable MDA. For details, see *Configuring the Sybase Target Database*

Fields	Descriptions
Collection Method	• MDA Click the **Test** button to confirm the connection with the method you selected. • TCP/IP Sniffer(available with FortiDB appliance only)
Polling Frequency (ms)	Polling frequency for MDA audit collection method. **Note:** When you change the value of Polling frequency, you must stop and start monitoring.
TCP/IP Sniffer Settings	Specify: • Target database version • FortiDB port connecting to network switch's SPAN port • Enable/Disable to save sniffer audit log See *Configuring Monitoring with TCP/IP Sniffer* for detail

MySQL Audit Configuration

FortiDB uses the MySQL general log for collecting audit information. You must configure your server to enable MySQL genneral log. For details, see *Setting MySQL General Log*

Fields	Descriptions
Collection Method	General Log Click the **Test** button to confirm the connection with the method you selected.

Start or Stop Monitoring from Target Monitors

This topic describes starting monitoring a target database. This task assumes you already have a target database connection, and at least one policy group mapped to the target. There are several ways to start or stop monitoring.

1. Go to Data Activity Monitoring > Monitors
2. Select the checkbox(es) of your target database(s).
3. Click the Start Monitoring button to start, or the Stop Monitoring button to stop.

Start or Stop Monitoring from Individual Target

This topic describes starting monitoring a target database. This task assumes you already have a target database connection, and at least one policy group mapped to the target. There are several ways to start or stop monitoring.

1. Go to Data Activity Monitoring > Monitors
2. Click on the name of a target database.
3. In the General tab, click the Start Monitoring button to start, or the Stop Monitoring button to stop.

General tab

The General tab shows Audit configuration information and monitoring status for each target database.

Audit Configuration

For choosing a collection method, see *Choosing a Collection Method*

Start/Stop Monitoring

This field allows you to start or stop monitoring. The following buttons and information are available:

Fields	Description
Start Monitoring or Stop Monitoring	If you click this button, monitoring starts or stops.
Start monitoring when FortiDB starts	If you select this checkbox, monitoring automatically starts when FortiDB starts.
Monitoring Status	Indicates the following monitoring status: • Running • NEEDS_RECONFIGURE: you need to go to the Policies tab, and click the Reconfigure button. • Idle • Terminating • Terminated • INIT (Initializing)

Fields	Description
Status Message	Indicates information related to the status of monitoring or auditing

Policies tab

In the policies tab, you can configure data policies, which will be automatically belong to a new policy group and associated to the target you selected.

The following table explains columns, icons and meanings in the policy table list.

Fields and Columns	Descriptions
Type	This column shows the following policy icons: • Compliance policy:  • Data policy:  Table,  Table column,  Session,  User • Metadata policy:  • Privilege policy: 
Status	This column shows the following status icons: •  indicates the policy has a problem. •  indicates the policy is disabled. •  indicates the policy is enabled.
Policy Name	This column shows a user-defined policy name.
Severity	This column shows a user-defined severity level. There are 5 levels of severity: • Informational (default) • Cautionary • Minor • Major • Critical
Reconfigure	When you change the policy configuration, this button becomes available. You need to click this button to allow FortiDB reconfigure the selected policy.
Data Policies	From this field, you can add data policies.

Associating Policy Groups to your Target Database

Data, Metadata, and Privilege policies are automatically associated to your target databases. When you configure policies, you do not need to manually associate. However, Compliance policies are not automatically associated to your targets. You need to take the following steps to associate the compliance policy to your target databases.

1 .Create a target database connection.

2 .Go to **Data Activity Monitoring** > **Monitors**.

3 .Click on the target name. The Target Monitor:<target name> page will display.
4 .Select the **Policy Groups** tab.
5 .Select the policy groups you want to associate to the target from the **Available Policy Groups** box..
6 .Click the right arrow to move the selection to the **Selected Policy Groups** box.
If you select each group name, the policies contained in selected policy group are shown in the right box.
7 .Select **Save**.

Notification tab

The Notification tab allow setup notification configurations for new alert.

The notification will be sent once FortiDB receives the monitoring alert. If you want to filter the alerts in batch and send the notification email, go to the Alert Grouping Notification section.

Email Notification

Enable this option to send notification email for alert.

For email notifications, you must designate one or more email receivers. Select one or more of the entries in the Available Receivers list box and add them to the Selected Receivers list on the right by selecting on the right-arrow button.

You need to set the following properties in the System Configuration.

- Email Server Host Name: enter your email server host name in the Value text box.
- Email Server Port: enter the email server port associated with the email server host property. The default is 25.

For details about the System Configuration, go to the System Configuration section.

SNMP Trap

Enable this option to send SNMP notification.

For SNMP notifications, you should set the following properties in the System Configuration.

- SNMP Receiver Host: enter the SNMP receiver host.
- SNMP Receiver Port : enter the SNMP receiver port number: the default is 162.

Syslog

Enable this option to send syslog packet to syslog server.

For Syslog notifications, you should set the following properties in the System Configuration.

- Syslog Receiver Host: enter the Syslog receiver host.
- Syslog Receiver Port : enter the Syslog receiver port number: the default is 514.

Alerts tab

The alerts page displays all alerts that were generated for the database you selected.

Columns	Descriptions
ID	Alert ID. This number is set sequentially
Type	•  indicates that the alert is generated by Data-table policies •  indicates that the alert is generated by Data-table and columns policies

Columns	Descriptions
	•  indicates that the alert is generated by Data-session policies •  indicates that the alert is generated by Data-user policies •  indicates that the alert is generated by Privilege policies •  indicates that the alert is generated by Metadata policies
Status	Three types of alert status: Unacknowledged, Acknowledged, or Error_corrected. You can change the alert status from the Alert Summary page. • indicates that the alert is not acknowledged • indicates that the alert has been acknowledged •  indicates that the error has been corrected
Policy Name	Name of the policy which the alert was generated from
Severity	Severity of the policy which the alert was generated from
Date	Date and time when the alert was generated

Filtering by Alert Group

You can filter the alert display by selecting one from the following Alert groups from the View dropdown.

- Major and Critical Alerts
- Metadata Changes
- Privilege Changes
- Security Violations
- Table Changes
- Unacknowledged Alerts
- All

You can modify the alert groups definition from the Alert Groups page. You can also add a user-defined alert group. For details about the Alert Groups, see the Alert Groups section.

Filtering by Date

You also can filter the alert display by selected date range that specified in the From field and To field. The date indicate the midnight of the date. For example, if you specify 6/16/09 in the From field, and 6/17/09 in the To field. The alert generated from 6/16/09 0:00 to 6/17/09 00:00 will be displayed.

Alert Details

The Alert Details field displays the detail information about alerts including SQL Statement executed in the target database. Each target database type contains different fields.

Logs tab

The logs tab displays history of activities for the specific target database you selected.

Columns	Descriptions
Date	Date and time that the activity occurred

Columns	Descriptions
Policy Name	Policy name which the activity is associated.
Type	Activity types
Severity	Severity of the policy which the alert was generated from
Description	Description of the activity

Audit Management Tab

The Audit Management page displays the issued audit command history. Each target databases has a different style of Audit management.

- *Oracle Audit Management*
- *MS SQL Server Audit Management*
- *DB2 Audit Management*
- Sybase MDA is not applicable for audit management

Oracle Audit Management

The Audit Management page for Oracle target databases displays the issued audit command history.

Statement Options

The Statement options section displays:

- Database User
- Audit Option
- Success
- Failure

Object Options

The Object options section displays all the audit commands, success or failure, for each object with:

- Object owner
- Object name
- Object type
- Access or Session on SELECT/INSERT/UPDATE/DELETE/EXECUTE/ALTER

The Refresh button is available to update the list.

Clear Audit Settings

FortiDB modifies the Oracle auditing system for monitoring the policies defined by the FortiDB user. These audit settings affect what is audited and affect how fast the SYS.AUD$ table will fill. Under normal operating conditions FortiDB removes its settings when monitoring is stopped.

However is not uncommon for the AUDIT system to get cluttered with settings from other users that were not properly removed and are no longer needed - thus needlessly filling the SYS.AUD$ table. FortiDB's clear audit setting feature removes all the audit settings. These are the settings are described above.

If FortiDB is the only client of the audit system then it is safe to use this feature to clear all audit settings. If other users need the audit settings you should not use the clear audit settings feature. To clear audit settings monitoring must be stopped. After clearing the settings the audit statement and audit options tables described above will be empty. If you then start FortiDB monitoring you will see only FortiDB's audit settings neccessary for the enabled policies.

Audit Management

When using the Audit-based collection methods for Oracle, users may want to clear the audit settings that were set from previous operations if FortiDB is used as the exclusive auditing mechanism for that target

database. Also, for the DB,EXTENDED collection method, users may want to delete all previous log entries in the Oracle target database. Both of these options are available in the **Audit Settings Management** section of the Audit Management tab. Furthermore, these options are selected by default, so users must make sure to un-select these options if FortiDB is not the only service that is using Oracle's auditing mechanism.

In addition, for the DB,EXTENDED collection mechanism, the audit log table may periodically grow larger than the file system capacity for that table. There is a scheduled deletion option in the **Scheduled Maintenance** section, where users can setup FortiDB to periodically delete audit log entries.

WARNING: Using FortiDB to manage the contents of the SYS.AUD$ should be compliant with the best practices of your organization.

MS SQL Server Audit Management

The Audit Management page for MS SQL Server target databases displays a list of MS SQL Server event, and filters used by FortiDB for auditing purposes.

You select Monitoring or Auditing from the Trace Type dropdown list and click the Refresh button, the general information will be displayed.

Audited Events

The MS SQL Server Audited Events section displays a list of MS SQL Server events used by FortiDB for auditing purposes with the following information:

- Column
- Event

Audited Filters

The MS SQL Server Audited Filters section displays a list of MS SQL Server filters used by FortiDB for auditing purposes with the following information:

- Column
- Comparison Operator
- Logical Operator
- Value

The Refresh button is available to update the list.

DB2 Audit Management

The Audit Management page for Oracle target databases displays the issued audit command history.

DB2 Audit Settings with syscat.auditpolicies

The DB2 Audit Settings section displays DB2 syscat.auditpolicies view contents with the following information:

- Policy Name
- Policy ID
- Create Time
- Alter Time
- Audit Status
- Context Status
- Validate Status
- Checking Status
- SecMaint Status
- ObjMaint Status

- SysAdmin Status
- Execute Status
- Execute with Data
- Error Type

DB2 Audit Settings with syscat.audituse

The DB2 Audit Settings section also displays DB2 syscat.audituse view contents with the following information:

- Policy Name
- Policy ID
- Schema
- Object Name
- Object Type
- Sub Object Type

The Refresh button is available to update the list.

Alerts

The Alerts page is a comprehensive alerts list with alert details. All alerts generated from all databases are displayed in this page. You can filter the alerts based on groups, pre-defined alert groups or alert groups you created.

The alert list displayed in this page can be exported to several different formats as a report.

The Alerts list is displayed in the following columns:

Columns	Descriptions
Type	•  indicates that the alert is generated by **Table Policy** •  indicates that the alert is generated by **Table and Column Policy** •  indicates that the alert is generated by **Session Policy** •  indicates that the alert is generated by **User Policy** •  indicates that the alert is generated by **Privilege Policy** •  indicates that the alert is generated by **Metadata Policy**
Status	Three types of alert status: Unacknowledged, Acknowledged, or Error_corrected. You can change the alert status from the Alert Summary page. • indicates that the alert is not acknowledged • indicates that the alert has been acknowledged •  indicates that the error has been corrected •  indicates that the alert has user-input annotation

Columns	Descriptions
ID	Alert ID. This number is set sequentially
Severity	Severity of the policy which the alert was generated from. There are Informational, Cautionary, Minor, Major, and Critical.
Date	The system date and time when the alert was generated
Target	User defined target database name. This name comes from the Name field of the General tab on the Targets page.
Policy & Rule Viloation	User defined name of the policy which the alert was generated from, and action of rule violation

Note: The Refresh button refreshes the page to display new alerts.

Filtering

Alert display can be filtered by the following criteria:

- **View**: filters alerts based on the alert group, per-defined or user-defined. Click **Search / New Group** button to add a new group. Click **Edit** button to modify your selected group.
- **Date Range**: filters alerts based on the date range
- **Status**: filters alerts based on the status (Unacknowledged, Acknowledged, Error_Corrected)

Report

The alert list displayed in this page can be exported as several different formats as reports.

- PDF (.pdf)
- Excel (.xls)
- Tab (.txt)
- CSV (.csv)

Changing Status and Annotate

This topic describes how to change the alert status, and annotate alert.

1. Go to **Data Activity Monitoring > Alerts** in the left-side tree.
2. To display alerts you want to include in the report, select a view from one of the following filtering:
   - **View**: select one from the dropdown list
   - **Date Range:** enter a start date and end date
   - **Limit To**: enter a value for the number of alerts displayed
3. Click the **Refresh** button to show the filtered alerts.
4. Select the checkbox at the left column for the alerts you want to change the status.
5. Click the three **Set Status** to change the status:
   - Unacknowledged
   - Acknowledged
   - Error_corrected
6. Click the **Annotate** button to add/edit the annotation, and click **Save** button to save.

Filtering Alerts

This topic describes the task of filtering alerts for a display or reports.

1. Go to **Data Activity Monitoring > Alerts** in the left-side tree.
2. To display alerts you want to include in the report, use one or more of the following filtering criteria:

a) To filter based on the alert group, select one of the alert group from the **View** dropdown. The alert display is immediately refreshed.
b) To filter based on the date range, enter the date range in the **From** and **To** fields when alerts were generated, or select a date by clicking the calendar icon.
c) To filter based on the alert status, select a status among Unacknowledged, Acknowledged, Error_corrected from the **Status** dropdown.

3 . Click **Apply** to apply filters you specified.

Exporting Alert Report

This topic describes the task of exporting alert reports from the Alerts page.

1 . Go to **Data Activity Monitoring > Alerts** in the left-side tree.
2 . To display alerts you want to include in the report, use one or more of the following filtering criteria:

Options	Description
View:	Select an alert group from the **View** dropdown
Date Range:	Enter the date range in the **From** and **To** fields when alerts were generated
Status:	Select a status among Unacknowledged, Acknowledged, Error_corrected from the **Status** dropdown

3 . Click **Apply** to apply the filtering criteria you specified.
4 . Select a format of the file you want to export a report from the **Export as** dropdown.

- PDF
- Excel
- Tab
- CSV

5 . Click **Export**.
6 . Save or open the file. The exported report is the summary report. It does not contain alert details.

Note: If you want to export the detail report, use the Pre-Defined DAM Reports feature. For details about Pre-Defined DAM Reports, go to *Pre-Defined DAM Reports*

Alert Details

The Alert Details section shows details information about the alerts.

Information contained in the Alert Details

The Alert details section shows the following information:

Field Name	Description
Policy Name	Policy name that generated the alert. For example, Tables, Column Privileges, tablePolicy1, etc.
Rule Violations	Alert rules that generated the alert. For example, Suspicious location, Suspicious Login Name, etc.
Severity	Severity level to which the policy is configured, such as Informational, Cautionary, Major, Minor, or Critical.
OS User or Auth Id (DB2)	OS user (for Oracle, MS SQL Server), Auth Id (for DB2) that accessed to the target database

Field Name	Description
DB User	DB user who took an action
Login Name	Login name that logged into the target database
Object	Object that was accessed and caused the alert
Action	Action that was taken and caused the alert
Return Code	Return code from the target database
SQL Statement	SQL Statements that were executed and caused the alert
Location	Location that originated the action
Timestamp	Target machine's date and time that the action was executed.
Application	Application that originated the actions and caused alerts

Note: For Sybase target databases, the OS User field shows as "not available". For MS SQL Server, the OS User is available only when you use the Windows authentication. For Sybase, and MS SQL Server, the Object field may not be available for Privilege Policies: Roles and System Privileges.

Alert Grouping

The Alert Grouping page allows you to categorize the alerts into the specific groups. Based on the group you select, you can generate alert reports, or send the email notification. The grouping can be run once, or scheduled recurring. The columns and icons of the Alerts Groups table are as follows:

Columns	Descriptions
Status	• indicates that email notification is enabled. • indicates that report generation and notifications are disabled.
Name	Name of the alert group
Description	Description of the alert group
Actions	To view the generated report, click

Pre-defined alert groups

FortiDB provides the following pre-defined alert groups. Based on these pre-defined alert groups, you can add and modify filtering criteria.

Pre-defined alert groups	Descriptions
Major and Critical Alerts	Alerts that have major and critical severities
Metadata Changes	Alerts generated by triggering metadata policies.
Privilege Changes	Alerts generated by triggering privilege policies
Security Violations	Alerts that are triggered by security violations

Pre-defined alert groups	Descriptions
Table changes	Alerts that are triggered by inserts, updates, or deletes on tables
Unacknowledged Alerts	Alerts that have a status of 'Unacknowledged'

Adding or Modifying Alert Groups

This topic describes the task of creating or modifying alert groups by using your filtering criteria.

1. Go to **Data Activity Monitoring** > **Alert Groups**
2. In the Alert Groups page, click **Add**. If you want to modify the specific alert group, click on the name of the group.
3. Enter an alert group name in the **Name** field (required).
4. (optional) Enter descriptions in the **Description** field to describe your filtering/grouping criteria.
5. Select the **Filters** tab and create a filtering condition by taking the following steps:
   a) Select a column from the **Column** dropdown on which you would like to filter.
   b) Select an operator from the **Operator** dropdown that associates the column you selected.
   c) Select a value from the **Value** dropdown or enter a value that the **Column** must match, and click the right arrow to move the selection to the right box.

   Note: The value you enter should be case-sensitive.

   d) You can add or subtract, respectively, filtering criteria rows by selecting the **+ (plus)** or **- (minus)** buttons.

   Here are some examples of filtering criteria:

Column	Operator	Value	Return Possibilities
Database Type	Equals	Oracle	Alerts associated with Oracle databases
Policy Type	Equals	Metadata Policies	Alerts associated with Metadata policies

6. Click **Save**.

Deleting the Alert Group

This topics describe deleting the existing user-defined alert groups. Pre-defined alert groups cannot be deleted.

1. Go to **Data Activity Monitoring** > **Alerts Groups**
2. In the Alert Groups page, select the checkbox(es) of user-defined alert groups.

   Note: The pre-defined alert groups will not be deleted.

3. Click **Delete**.
   The alert group will be deleted from the list.

Generating Alert Reports

This topic describes how to generate alert reports at the scheduled time.

1. Go to **Data Activity Monitoring > Alert Groups** in the left-side tree.
2. Click on the name of the alert group that you want to generate a report.

3 .Go to the **Reports** tab.
   a) Select the **Save Scheduled Alert Report to Disk File** checkbox.
   b) Specify the report type you want to generate.
      - Detailed
      - Statistical
      - Summary
   c) Specify the report format you want to generate.
      - PDF (.pdf)
      - Excel (.xls)
      - Comma Delimited (.csv)
      - Tab Delimited (.txt)
   d) (Optional) If you want to attach reports to the e-mail notification, select the **Attach reports to selected e-mail receivers** checkbox, and make sure that the **Enable e-mail Notification** checkbox in the Notifications tab is selected. Note that the **Save Scheduled Alert Report to Disk File** option is not required to be selected to use this capability.
4 .To schedule a report once or recurring, go to the **Schedule** tab. For details about selecting the schedule of alert reports, go to *Scheduling Notification and Alert Reports*
5 .Click **Save** .
6 .
To view the report, click the Report icon  in the **Action** column.

Scheduling Alert Reports

This topic describes the task to schedule alert reports for any alert group at scheduled times.

The Alert Group scheduler allows you to set up when to start report generation, how often to generate reports, and when to stop. There are two ways that you can set up the scheduler.

Scheduled Type	Description	Alert Date Range
Run Once	Alert notification and report generation will occur once at the specific time you set in the **Start at** field.	The alert date range used to execute the selected tasks will be the date range that is specified in the **Alert Date Range** field.
Recurring	Alert notification and report generation will occur starting from the time set in the **Start at** field, and continue until the **End by**.	The alerts used will be alerts generated between the last scheduled time and the current time. When the scheduler first triggers, the recurrence interval will be used to determine the start time of alerts used.

Setting the Run Once Option

1 .Go to **Data Activity Monitoring > Alert Groups** in the left-side tree.
2 .Click on the name of the alert group that you want to schedule.
3 .Select the **Schedule** tab.
4 .Select the **Run Once** option in the **Schedule type** section.
5 .In the **Starts at** section, enter a starting time.
6 .In the **Alert Date Range** section, enter a start date and end date of generated alerts that you want to schedule tasks against.

7 .In the **Limit To** section, enter the number of alerts you want to include in the report.
8 .Click **Save.**

Setting the Recurring Option

1 .Go to **Data Activity Monitoring > Alert Groups** in the left-side tree.
2 .Click on the name of the alert group that you want to schedule.
3 .Go to the **Schedule** tab.
4 .Select the **Recurring** option in the **Schedule type** section.
5 .In the **Starts at** section, enter a starting time.
6 .Set the **Recurrence pattern**. You can select one of the following recurring patterns.

Recurrence Pattern	Interval	Example
Hourly	Specify the hourly interval in the **Every __ hours** field.	If you specify '1' in the Every __ hours field, the recurrence pattern starts from the Start time, the schedule will trigger every 1 hour to perform selected actions.
Daily	Specify the daily interval in the **Every __ days** field.	If you specify '1' in the Every __ days field, the recurrence pattern starts from the Start time, the schedule will trigger every 24 hours to perform selected actions.
Weekly	Select the days of the week.	If you select 'Monday' and 'Friday', then on Mondays and Fridays, at the time specified in the Start time section, the schedule will be triggered to perform selected actions.
Monthly	Select the day of selected months.	If you select Day, and choose '2', and select all the months, then the schedule will be triggered to perform selected actions on the 2nd day of every month at the time specified in the Start time section. If you select The, and choose **first** and **Monday** in the adjacent drop-down lists, and select all the months, then the schedule will be triggered to perform selected actions on the first Monday of every month at the time specified in the Start time section.

7 .In the **Ends by** section,select the date on which to stop the scheduler. You can choose **No end date** if you do not want to specify an end date.
8 .In the **Limit To** section, enter the number of alerts you want to include in the report.
9 .Click **Save**.

Notification of Alert Reports

You can setup the notification email or SNMP trap to notify alert generation to specific users. To enable alert report notification to specific users, take the following steps:

1 .Go to **Data Activity Monitoring** > **Alert Groups** in the left-side tree.
2 .Click on the name of the alert group that you want to set the report notification.
3 .Go to the **Notification** tab.
4 .Select the **Enable Email** to enable email notification respectively.
   a) For email notifications, you must designate one or more email receivers. Select one or more of the entries in the Available Receivers list box and add them to the Selected Receivers list on the right by selecting on the right-arrow button.

Note: You need to set the following properties in the System Configuration.

- Email Server Host Name: enter your email server host name in the Value text box.
- Email Server Port: enter the email server port associated with the email server host property. The default is 25.

   For details about the System Configuration, go to the System Configuration section.
   b) (Optional) If you want to attach reports to the e-mail notification, go to the **Reports** tab and select the **Attach reports to selected e-mail receivers** checkbox, and make sure to select one or more report(s) and format(s). Note that the **Save Scheduled Alert Report to Disk File** option is not required to be selected to use this capability.
5 .To confirm the email address for the receiver, select the name of a receiver in either the Available Receivers or Selected Receivers lists and those details will appear in Receiver Details list on the right.
6 .Click **Save** .

Browse Sniffer Audit Logs

When monitoring the target database with collection method **TCP/IP Sniffer**, and enabling the **Save Sniffer Audit Log** option, FortiDB will save the sniffer audit logs accordingly.

Note: TCP/IP Sniffer and **Sniffer Audit** browsing are available with FortiDB appliance only.

FortiDB will keep sniffer log for a period of date (30 days by default), and will remove old logs out of duration limit. To change this setting, go to **Administration > Global Configuration > Monitor**, change value of **Sniffer Audit Log Keep Duration**.

Go to **Data Activity Monitoring > Sniffer Audit** to browse the audit log from sniffer.

Select the **Target Database** and **Data Activity Action** in the dropdown listbox, enter the from/to date, click the **Refresh** button to filter the audit logs.

Click **Search** button, to input criteria and search logs.

Browse Compliance Audit Logs

When monitor the target database with **Compliance Policy**, FortiDB will save the compliance audit logs accordingly.

This page displays the compliance audit logs.

Select the **Target Database** in the dropdown listbox, enter the from/to date, click the **Refresh** button to filter the audit logs.

Local Monitor Logs

The Monitor Logs page lists all errors based on the severity levels you select for a view. Target monitor logs include information: Date, Policy name, Target, Type, Severity.

In the Target Monitor Logs page, you can:

- Display error logs filtered by the database type that you select from the **Database Type** dropdown list.
- Display error logs filtered by the severity level that you select from the **Severity Level** dropdown list.
- Display error logs filtered by the date range you select from the **From** and **To** fields.
- Display Date, Policy name, Target, Type, Severity, and description for each error.
- Export the error view you selected based on the severity level by selecting **Export**
- Delete all error logs by selecting **Delete All**
- Schedule error checks. You can select check schedules as:
  - *Run Once*: Error checks will occur once at the specific time you set in the Start at field.
  - *Recurring*: Error checks will occur starting from the time set in the Start at field, and continue until the End by.

Scheduling Error Checks: Run Once

This topic describes scheduling error checks with the Run once option.

1. Go to **Data Activity Monitoring** > **Log** in the left-side tree.
2. Click the triangle icon at **Schedule Error Checks** to expand.
3. Select **Run Once**.
4. In the **Starts at** section, enter a starting time and date.
5. In the **Days** filed, specify the number of days after which to delete error log entries.
6. Click **Save**.

Scheduling Error Checks: Run Recurring

1. Go to **Data Activity Monitoring** > **Log** in the left-side tree.
2. Click the triangle icon at **Schedule Error Checks** to expand.
3. Select the **Recurring** option in the **Schedule type** section.
4. In the **Starts at** section, enter a starting time.
5. Set the **Recurrence pattern**. You can select one of the following recurring patterns.

Recurrence Pattern	Interval	Example
Hourly	Specify the hourly interval in the **Every __ hours** field.	If you specify ‘1’ in the Every __ hours field, the recurrence pattern starts from the Start time, the schedule will trigger every 1 hour to perform selected actions.
Daily	Specify the daily interval in the **Every __ days** field.	If you specify ‘1’ in the Every __ days field, the recurrence pattern starts from the Start time, the schedule will trigger every 24 hours to perform selected actions.

Recurrence Pattern	Interval	Example
Weekly	Select the days of the week.	If you select ‘Monday’ and ‘Friday’, then on Mondays and Fridays, at the time specified in the Start time section, the schedule will be triggered to perform selected actions.
Monthly	Select the day of selected months.	If you select Day, and choose ‘2’, and select all the months, then the schedule will be triggered to perform selected actions on the 2nd day of every month at the time specified in the Start time section. If you select The, and choose **first** and **Monday** in the adjacent drop-down lists, and select all the months, then the schedule will be triggered to perform selected actions on the first Monday of every month at the time specified in the Start time section.

6 .In the **Ends by** section,select the date on which to stop the scheduler. You can choose **No end date** if you do not want to specify an end date.

7 .In the **Days** filed, specify the number of days after which to delete error log entries.

8 .Click **Save**.

Report Management

Pre-Defined VA Reports

The following report templates are available for Pre-defined Vulnerability Assessment Reports.

Note: In order to generate reports, users are required to have the Report manager role.

Assessment Reports

- Global Detailed Report: this report gives the number and types of passed and failed policies and their details for all targets in the assessment
- Target Detailed Report: this report gives the number and types of passed and failed policies and their details
- Target Detailed Failed Report: this report gives the number and types of failed policies and their details
- Target Summary Report: this report summarizes the number and types of passed and failed policies
- Target Summary Failed Report: this report summarizes the number and types of failed policies
- Target Score Report: this report displays the scan results in graphical form
- Target Trend Report: this report displays the database policy progress over time
- Sensitive Data Discovery Detailed Report: this report gives the detailed information about the sensitive data discovery.
- Sensitive Data Discovery Summary Report: this report gives the summary information about the sensitive data discovery.

Policy Reports

- Policy Summary Report: this report gives the detailed information about the current vulnerability assessment policies in the system
- Policy Detailed Report: this report summarizes the most current vulnerability assessment policies in the system

Generating Assessment Reports

This topic describes how to manage pre-defined assessment reports. To generate an assessment report, take the following steps:

1. Select **Pre-Defined VA Reports** under Report Management.
2. Select a report. The Generate Audit Compliance Report page displays.
3. If you want a file-based report, select an output-format type from the **Export as** drop down and then select the **Export** button. (You will then see another preview and can then save that to your file system.)

Note: The available output-format types are:

- PDF (.pdf)
- Excel (.xls)
- Tab-delimited (.txt)
- Comma-delimited (.csv)

Note: Some output-format types may not available for all report types.

Preview Assessment Report

This topics describes the Assessment Report Preview page. You can sort the report table by clicking each title in the reports.

Statistic Tables

All report templates (except for Trend report and Global report) contain the following two statistic tables:

- Severity: Summary of numbers of each state by policy-severity type.
- Classification: Summary of numbers of each state by policy-classification type

Summary Report

The pre-defined Summary Report template provides a summary of the number and type of all policies used by an assessment.

Table 12 : Statistic Table of Summary Report

Section	Description
Critical Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Critical.' (Select the plus (+) sign to expand the list.)
Major Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Major.' (Select the plus (+) sign to expand the list.)
Minor Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Minor.' (Select the plus (+) sign to expand the list.)
Cautionary Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Cautionary.' (Select the plus (+) sign to expand the list.)
Informational Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Informational.' (Select the plus (+) sign to expand the list.)

Summary Failed Report

The pre-defined Summary Failed Report template provides you a summary for just those policies that failed during an assessment.

Table 13 : Summary Failed Report Sections

Section	Description
Classification	Summary by policy-classification type for just failed assessment results
Critical Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of 'Critical.' (Select the plus (+) sign to expand the list.)
Major Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of

	'Major.' (Select the plus (+) sign to expand the list.)
Minor Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of 'Minor.' (Select the plus (+) sign to expand the list.)
Cautionary Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of 'Cautionary.' (Select the plus (+) sign to expand the list.)
Informational Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of 'Informational.' (Click on the plus (+) sign to expand the list.)

Detailed Report

The pre-defined Detailed Report template provides you detail and fix recommendations for all of the policies used by an assessment.

Table 14 : Detailed Report Sections

Section	Description
Classification	Details by policy-classification type
Critical Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Critical.' (Select on the plus (+) sign to expand the list.)
Major Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Major.' (Select the plus (+) sign to expand the list.)
Minor Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Minor.' (Select on the plus (+) sign to expand the list.)
Cautionary Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Cautionary.' (Select the plus (+) sign to expand the list.)
Informational Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Informational.' (Select the plus (+) sign to expand the list.)

Detailed Failed Report

The pre-defined Detailed Failed Report template provides you detail all policies that failed during an assessment.

Table 15 : Detailed Failed Report Sections

Section	Description
Critical Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Critical.' (Select the plus (+) sign to expand the list.)

Major Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Major.' (Select on the plus (+) sign to expand the list.)
Minor Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Minor.' (Select the plus (+) sign to expand the list.)
Cautionary Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Cautionary.' (Select the plus (+) sign to expand the list.)
Informational Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Informational.' (Select on the plus (+) sign to expand the list.)

Score Report

The pre-defined Score Report Vulnerability template provides you a way to see vulnerability results in graphical form for all target databases used in an assessment. It also shows results by the RDBMS type of the assessed targets.

Table 16 : Score Report Sections

Section	Description
Severity	Graphical chart by policy-severity type for the assessed database
Classification	Graphical chart by policy-classification type for the assessed database
Vulnerability	Bubble chart that plots both the severity and classification types for the assessed database

Trend Report

The pre-defined Trend Report template provides you a way to see assessment results over time to assist your vulnerability planning and remediation efforts.

Table 17 : Trend Report Sections

Section	Description
Trend Chart of Policy-Severity Type	Line chart of policy-severity results for specified assessments
Trend Chart by Policy-Classification Type	Line chart of policy-classification results for specified assessments
Table of Policy-Severity Type by Scan Time	Table of policy-severity results for specified assessments
Table of Policy-Classification Type by Scan Time	Table of policy-classification results for specified assessments

Generating Policy Reports

This topic describes how to generate a report for policies currently used in the FortiDB system.

You can filter contents of the reports by selecting the following parameters:

- Database types: DB2, Microsoft SQL Server, MySQL, Oracle, Sybase, or All.

  Note: Pen Test policies are included in "All". If you want to include Pen Test policies in the report, you need to select "All".
- Classification: Pre-defined vulnerability categories from which you can filter by Configuration, Database Server, Host System, Password, Privilege, Unclassified, or All.
- Severity: Severity levels from which you can filter by Cautionary, Critical, Informational, Major, Minor, or All.

To create a policy report filtered with your selections, take the following steps:

1. Select **Pre-Defined Reports** under Report Management.
2. Select either Policy Detailed Report or Policy Summary Report.
3. In the **Report Parameters** section of the **Policy Detailed Report** or **Policy Summary Report** page, select a database type from the dropdown list in the **Database Type** field.
4. In the **Classification** field, select one you want to filter from the dropdown list.
5. In the **Severity** field, select one you want to filter from the dropdown list.
6. Select the **Apply** button. You should see the filtered policy-report information with the number of policies shows up in the **Report Information** tab.
7. Select the **Preview Report** tab in order to see your report including the statistic tables based on Severity, and Classification, and the summary table or detailed table filtered by your selection. For descriptions of table columns, see *Preview Policy Report*
8. If you want to export a report as a file, select an output-format type from the **Export as** dropdown list and select the **Export** button. (You will see another preview and can save that to your file system.)

   Note: The available output-format types are:

   - PDF (.pdf)
   - Excel (.xls)
   - Tab-delimited (.txt)
   - Comma-delimited (.csv)

Preview Policy Report

This topics describes the Policy Report Preview page. You can sort the table columns by clicking each column title of the reports.

Summary Report

The Summary Report template provides two statistic tables, and the policy summary report. The descriptions of the tables are as follows:

Table 18 : Statistic Tables

Tables	Description
Severity	Summary of all database types (and Pen Test when "All" is selected in the Database Type field) counted by severity
Classification	Summary of all database types (and Pen Test when "All" is selected in the Database Type field) counted by classification

Table 19 : Summary Report

Columns	Description
DB Type	Database type that you selected in the Database Type field. For Pen Test policies, the DB Type column is a blank. Pen Test policies are included

	in the report only when you select "All" in the Database Type field.
Ver. (Policy Version)	Version number of the policy.
Severity	Policy severity type that you selected in the Severity field.
Classification	Policy classification type that you selected in the Classification field.
PolicyName	Pre-defined policy name of the database you selected.

Detailed Report

The Detailed Report template provides two statistic tables, and policy detailed report. The descriptions of the tables are as follows:

Table 20 : Statistic Tables

Tables	Description
Severity	Summary of all database types (and Pen Test when "All" is selected in the Database Type field) counted by severity
Classification	Summary of all database types (and Pen Test when "All" is selected in the Database Type field) counted by classification

Table 21 : Detailed Report

Columns	Description
DB Type	Database type that you selected in the Database Type field. For Pen Test policies, the DB Type column is a blank. Pen Test policies are included in the report only when you select "All" in the Database Type field.
Ver. (Policy Version)	Version number of the policy.
Severity	Policy severity type that you selected in the Severity field.
Classification	Policy classification type that you selected in the Classification field.
PolicyName	Pre-defined policy name of the database you selected.
Description	Description of the policy.

Pre-Defined DAM Reports

The following report templates are available for Pre-defined DAM reports. Pre-defined DAM reports display alerts data, which you can filter unnecessary alerts to exclude from the report data.

The following DAM reports templates are available:

- Detailed report: this report shows the details for all alerts generated within the alert group filter criteria.

- Summary report: this report summarizes the alerts generated within the alert group filter criteria.
- Statistical report: this report summarizes statistical information about alerts generated based on rules-violations, policies, and severities.

Generating DAM Alerts Reports

This topic describes how to manage pre-defined DAM reports. To generate an DAM report, take the following steps:

1. Select **Pre-Defined DAM Reports** under Report Management.
2. Select a report name among Detailed, Summary, or Statistical. Alert Report page displays.
3. Select a view you want to include in the report from the View dropdown.
4. Select the date range of the alerts generated, by entering a starting date at the From field, and ending date at the To field, or selecting dates using the Calendar icon.
5. To preview the report, click the Preview Report tab.
6. If you want a file-based report, select an output-format type from the **Export as** drop down and then select the **Export** button.

Note: The available output-format types are:

- PDF (.pdf)
- Excel (.xls)
- Tab-delimited (.txt)
- Comma-delimited (.csv)

Preview Alerts Report

This topics describes Alert Report Preview. The preview reports are displayed according to your filtering settings. You can sort the table columns by clicking each column title of the reports.

Summary Report

The Summary Report provides your filter settings, and alert summary information as follows:

Table 22 : Summary Report

Columns	Description
ID	Alert ID.
Status	Acknowledged, Unacknowledged, Error corrected
Severity	INF (Informational), CAU (Cautionary), MAJ (Major), MIN (Minor), CRI (Critical)
Policy	User defined or predefined policy name
Action	Action that triggered the alert. SELCT, LOGON, etc
Rule Violations	Rule violations of the policy that triggered the alert
Timestamp	Date and time the alert was generated.

Detailed Report

The Detailed Report provides your filter settings, and alert detailed information as follows:

Table 23 : Detailed Report

Columns	Description
ID	Alert ID.

Severity	INF (Informational), CAU (Cautionary), MAJ (Major), MIN (Minor), CRI (Critical)
Policy Name	User defined or predefined policy name
Object	Object that triggered the alert. orcl.SCOTT.EMP, etc
Timestamp	Date and time the alert was generated.
Description	Other available information in Alert Details field

Statistical Report

The Statistical Report provides alert counts by severities generated based on policies, actions, rules-violations, and status.

Table 24 : Statistical Report

Statistical reports	Description
Alerts grouped by policy	Alert counts by severities based on policies
Alerts grouped by action	Alert counts by severities based on actions
Alerts grouped by rule-violation	Alert counts by severities based on rules-violations
Alerts grouped by status	Alert counts by severities based on status

User-Defined Reports (VA and DAM)

You can customize your report template with selected columns and data from the User-Defined VA and DAM Reports page.

Note: In order to generate reports, users are required to have the Report manager role.

Columns and Buttons	Description
Name	User defined name
Description	User defined description
Last Modified	Date and time of the report you modified last
Created By	User who created the report
Add	This button adds a report
Delete	This button deletes the report you checked in the checkbox

Managing VA and DAM User-Defined Reports

This topic explains how to configure and run User-Defined Reports and exposes the report fields that can be populated for your reports.

For VA Reports, you should run an assessment before running reports. For DAM Reports, you should start monitoring and generate alerts before running reports.

Here are the User-Defined report operations:

- Naming and describing your reports
- Specifying which columns you want to include in your reports
- Specifying grouping criteria
- Specifying filtering criteria
- Exporting your report in a certain output format, PDF or tab-delimited.
- Deleting reports

In order to create your own report:

1. Go to **Report Management** > **User-Defined VA Reports** or **User-Defined DAM Reports** of the left-side tree menu.
2. Select the **Add** button.

   Note: If you are modifying an existing User-Defined report, select its name in the **Name** column
3. On the the **General** tab of the **User-Defined Report** page, enter a **Name** and (optionally) a **Description** for your report.
4. On the the **Columns** tab of the **VA (or DAM) User-Defined Report** page, select the name(s) of the columns you want to appear in your report from the **Available Columns** list box and then select the **Right** arrow to move them to the **Columns in Report** list box. (You can remove columns from your report by selecting them in the **Columns in Report** list box and then select the **Left** arrow.)

   Note: Your report must contain at least one display column. So , once you have selected at least one column for your report, you may select the **Export** button to see a report sample.

   Note: By selecting the **First**  , **Up**  , **Down**  , or **Last**  button(s), you can change the subsequent (left-to-right) order of the columns in your report. The first and last columns will be the leftmost and rightmost columns, respectively, in your resulting report.
5. (Optional) Select the **Grouping** tab. In the **Group Data By** dropdown, enter the column name(s) by which you want to group report results. Optionally, specify a sort order in the **Order** dropdown. Specify a **Day**, **Week**, **Month, Quarter**, or **Year** value by which to group date-related report results in the **Group date values by** dropdown.

   Note: For VA reports, you cannot group by **Policy Description.**

   Note: You can specify two additional grouping levels, in the same way, by using the **and then by** and the **and lastly by** drop down lists.
6. (Optional, VA only) In the **Filtering** tab, enter the criteria by which you would like to filter or limit the data that shows up in your report.
   a) Enter the criteria by which you would like to filter or limit the data that shows up in your report.
      - Select a column from the **Column** dropdown on which you want to filter.
      - Select an operator from the **Operator** dropdown that associates the column you selected.
      - Enter a value that the column must match (the value you enter should be case-sensitive).
      - You can add or subtract, respectively, filtering criteria rows by selecting the + (plus) or - (minus) buttons.

   b) In order to limit the number of rows you would like to display, check the **Enter number** radio button and then specify, as your row limit, any positive number less than 1000.
7. Select **Save**.
8. In order to export your report:
   a) For DAM: Click on the **Export report** action icon for the report you want to export. This will take you to a new page where you can select the Alert Group filter and specify the row limit to narrow down the number of alerts to export.
   b) For VA: Click on the report you want to export to open the report template.

c) Specifying an output format in the **Export as** drop down list.
d) Assuming you want a PDF output, specifying your page orientation by enabling either the **Portrait** (the default) or the **Landscape** radio button.

Note: For a PDF output, you will need to limit the number of display columns in order to get a legible report. You may have to experiment to derive the limit, which may be dependent on your PDF rendering application.

e) Select the **Export** button.
f) View the result, make setting changes if necessary, and regenerate the report. Once you are satisfied with the result, select the **Save** button.

Deleting VA and DAM User-Defined Reports

This topic describes how to delete VA (or DAM) User-Defined reports.

1 .Go to **Report Management** > **VA (or DAM) User-defined Reports** of the left-side tree menu.
2 .Select the checkbox(es) corresponding to the **Name**(s) of the report templates you want to delete.
3 .Select the **Delete** button.

Compliance Reports

FortiDB Compliance reports contain data that are most necessary for IT internal controls. These reports can help achieve compliance with both internal and external requirements.

Some compliance reports need to be generated weekly, monthly, or quarterly.

Name	Description	Required option settings
Abnormal or Unauthorized Changes to Data	This report tracks all changes made to data by any account other than the application user account.	Object Audit Options
Abnormal Termination of Database Activity	This report identifies failed database processes (i.e. Financial transactions or failed login attempts) originating from an application server.	Object Audit Options or User Audit Options
Abnormal Use of Service Accounts	This report identifies service accounts and the associated or related transaction origins. For example, the use of service account from an origin other than the application server would be identified.	Object Audit Options or User Audit Options
End of Period Adjustments	This report tracks changes to the general ledger at month, quarter, year end.	Object Audit Options
History Of Privilege Changes	This report tracks changes to user access rights that are elevated or lessened in the database over time.	Not required
Verification of Audit Settings	This report tracks changes to configurable audit parameters.	Not required

Note: The Compliance reports do not support monitoring column-level policies.

General Steps for Generating Compliance Reports

1. Configure your target databases. See *Required Settings of Target Databases*
2. Connect FortiDB to your target databases. See *Managing Target Databases*
3. Configure FortiDB Compliance policies. See *Configuring Compliance Policy*
4. Go to the General tab, and click Start Monitoring. For details, see *General tab*
5. Assuming that several violations occurred in your target database, go to Compliance Reports under Report Management.
6. Select one of the reports and export reports. For generating the Compliance reports, go to *Generating Compliance Reports*

Generating Compliance Reports

This topic describes how to manage compliance reports. To generate a compliance report, take the following steps:

1. Select **Compliance Reports** under Report Management.
2. Select a report name.
3. In the **Export as** field, select the format type you want to generate a report from the dropdown list: PDF, Excel, or CSV.
4. (Optional) Enter W/P reference and/or Customer name in each field.
5. In the **Date Range** field, enter the starting date of the data retrieval in the From field, and ending date of data retrieval from the To field. Alternatively you can select a date by clicking the calendar icon.

   Note: The date entered in these fields means 00:00 (midnight) of the day. For example, 9/23/09 means 00:00AM of 9/23/09
6. In the **Targets** section, select one or more databases, and click the right arrow to move your selection to the right box. If you want to select all databases, select the All Databases checkbox.
7. (Optional) You can set filters to display the specific data in the report. To set filters:
   a) Select a column from the **Column** dropdown by which to filter the list of the items.
   b) Select an operator from the **Operator** dropdown by which to associate your chose column and value.
   c) Enter a column value for filtering.
   d) Click + sign to add more criteria, or - sign to delete the criteria you entered.
8. Select **Export.** The File Download dialog displays.
9. Select **Open** to open the PDF file, or **Save** to save the report file in your local hard drive.

Report: Abnormal Termination of Database Activity

This report identifies failed database processes (i.e. Financial transactions) originating from the application server. This should be reviewed on a daily basis by IT Management.

COBIT Objectives

Objective Number	Description
DS10.1	Routine transactions and processes between the application and the database are reviewed on a daily basis for successful completion by IT Management.

Setup Requirements

Compliance Policy: Object Audit Options and/or User Audit Options

Report Columns

The following columns are displayed in the report body.

Columns	Description
User ID	The ID of the database user that conducted the flagged activity
Object	The name and owner of the database object that was directly manipulated by the flagged activity
Timestamp	The exact time the flagged activity was conducted
Terminal	The terminal IP address or name
Origin Application	The name, or other identifier, for the originating application, if the activity originated from an external application or from an application server
Action Type	The type of action successfully enacted by the User ID.
Error Code	The proprietary error code generated by the originating application.

Report: Abnormal or Unauthorized Changes to Data

This report tracks all changes made to data by any account other than the application user account. The report should be reviewed and commented on by appropriate management on a quarterly basis.

COBIT Objectives

Objective Number	Description
AI2.3	Unauthorized changes to data by non-application[13] accounts are tracked and reviewed by IT Management on a quarterly basis.

Setup Requirements

Compliance Policy: Object Audit Options

Report Columns

Columns	Description
User ID	The ID of the database user that conducted the flagged activity
Object	The name and owner of the database object that was directly manipulated by the flagged activity
Timestamp	The exact time the flagged activity was conducted
Terminal	The terminal IP address or name
Origin Application	The name, or other identifier, for the originating application, if the activity originated from an external application or from an application server

Columns	Description
Action Type	The type of action successfully enacted by the User ID.

Note: By default, all actions are considered unauthorized. If you want, for example, to only mark UPDATEs as unauthorized actions, use Filters section in order to filter out the other action types.

Report: Abnormal Use of Service Accounts

This report identifies the use of service accounts and the associated transaction origins. For example: The use of a service account from an origin other than the application server would be identified. The report should be reviewed and commented on by IT Management on a weekly basis.

COBIT Objectives

Objective Number	Description
DS5.3	Database transactions from unauthorized sources are tracked and reviewed by IT Management on a weekly basis

Setup Requirements

Compliance Policy: Object Audit Options and/or User Audit Options

Report Columns

The following columns are displayed in the report body.

Columns	Description
User ID	The ID of the database user that conducted the flagged activity
Terminal	The terminal IP address or name
Originating Application	The name, or other identifier, for the originating application, if the activity originated from an external application or from an application server
Number of Actions	The number of actions attempted by the account associated with the User ID
Timestamp	The exact time the flagged activity was conducted

Report: End of Period Adjustments

This report tracks changes to the general ledger at month/quarter/year end. The report should be reviewed and commented on by appropriate management on a monthly basis.

COBIT Objectives

Objective Number	Description
AI2.3	End of period adjustments to the general ledger are tracked and reviewed by Business Management on a monthly basis.

Setup Requirements

Compliance Policy: Object Audit Options

Report Columns

The following columns are displayed in the report body.

Columns	Description
User ID	The ID of the database user that conducted the flagged activity
Object	The name and owner of the database object that was directly manipulated by the flagged activity
Timestamp	The exact time the flagged activity was conducted
Terminal	The terminal IP address or name
Origin Application	The name, or other identifier, for the originating application, if the activity originated from an external application or from an application server
Action	The type of action successfully completed by the User ID.

Report: History of Privilege Changes

This report tracks privileged changes to database user access rights (i.e. granting of privileged or escalated access rights). The report identifies the database account that was changed, the type of privilege that was granted, the date of the change, and the account that initiated the change. The report should be reviewed by both IT and Business Management on a quarterly basis.

COBIT Objectives

Objective Number	Description
AI2.4, DS3.5, DS5.3, DS5.4	Changes to escalate database user access privileges are tracked for review on a quarterly basis by the IT manager and the application business manager

Setup Requirements

Compliance Policy: Just enable the policy. No settings of Object Audit or User Audit Options required.

Report Columns

The following columns are displayed in the report body.

Columns	Description
User ID	The ID of the database user that conducted the flagged activity
Grantee	The name of the user for whom privileges were changed
Action	The type of action successfully enacted by a non-application user account. Actions include UPDATE, INSERT, and GRANT

Columns	Description
Target	The object on which the privileges were changed
Privilege Details	The type of object privilege granted to, or revoked from, the grantee.
Timestamp	The exact time the flagged activity was conducted.

Report: Verification of Audit Settings

This report identifies any changes that have been made to the audit reporting and tracking capability of the database.

COBIT Objectives

Objective Number	Description
DS3.5, DS5.5, DS13.3	Audit tracking is configured on all financial databases, changes to audit functionality is reviewed by IT Management on a quarterly basis.

Setup Requirements

There are two requirement:

1. At least one of the auditing policies must be run in order to collect audit data:
   - Data Policies
   - Privilege Policies: using the audit data retrieval method
   - Metadata Policies: using the audit data retrieval method
2. For tracking audit activity with the Data policies, run the following commands

   ```
   audit system audit; audit audit system; audit audit any;
   ```

   and then Close and Open your database connection in Data policies.

Report Columns

The following columns are displayed in the report body.

Columns	Description
User ID	The ID of the database user that conducted the flagged activity
OS User	The OS User that conducted the flagged activity
Object	The name and owner of the database object that was directly manipulated by the flagged activity
Timestamp	The exact time the flagged activity was conducted
Terminal	The terminal IP address or name
Origin Application	The name, or other identifier, for the originating application, if the activity originated from an external application or from an application server
Action	The type of action successfully enacted by the User ID.

Appliance - Command Line Interface (CLI)

Using the FortiDB CLI

This topic describes the basics of using the CLI (Command Line Interface). You can use CLI commands to view all system information and to change all system configuration settings.

To use the FortiDB CLI:

1. Logon to the FortiDB appliance as the `admin` user or as a user with the FortiDB System Administrator role via the following methods:
   - SSH (Secure Shell)
   - Telnet
2. Enter the CLI command of interest.

Basic CLI Information

This topic provides basic information for using the FortiDB CLI.

This section includes information about:

- Command help
- Command completion
- Recalling commands
- Editing commands
- Line continuation
- Command abbreviation
- Encrypted password support
- File names and locations
- Entering spaces in strings
- Entering quotation marks in strings
- Entering a question mark (?) in a string
- Special characters
- IP address formats
- DNS for Hostname Recognition
- FTP-directory abbreviations

Command help

You can press the question mark (?) key to display command help.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Type a command followed by an option and press the question mark (?) key to display a list of additional options available for that command-option combination and a description of each option.

Command completion

You can use the tab key or the question mark (?) key to complete commands.

- You can press the tab key at any prompt to scroll through the options available for that prompt.
- You can type the first characters of any command and press the tab key or the question mark (?) key to complete the command or to scroll through the options that are available at the current cursor position.
- After completing the first word of a command, you can press the space bar and then the tab key to scroll through the options available at the current cursor position.

Recalling commands

You can recall previously entered commands by using the Up and Down arrow keys to scroll through commands you have entered.

Editing commands

Use the **Left** and **Right** arrow keys to move the cursor back and forth in a recalled command. You can also use the **Backspace** and **Delete** keys and the control keys listed in the following table in order to edit the command.

Function	Key combination
Beginning of line	CTRL+A
End of line	CTRL+E
Back one character	CTRL+B
Forward one character	CTRL+F
Delete current character	CTRL+D
Previous command	CTRL+P
Next command	CTRL+N
Abort the command	CTRL+C
If used at the root prompt, exit the CLI	CTRL+C

Line continuation

To break a long command over multiple lines, use a \ at the end of each line.

Command abbreviation

You can abbreviate commands and command options to the smallest number of non-ambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st`.

File names and locations

Filenames and locations should consist only of letters, numbers, hyphens, and underscores. Do not use spaces or special characters. For example, *my_file* is an acceptable name; *my&file* is not.

Entering spaces in strings

Note: Spaces are not allowed in strings that represent filenames or file locations.

When a string value, for other than a filename or locations, contains a space, do one of the following:

- Enclose the string in quotation marks; `"Security Administrator"`, for example.
- Enclose the string in single quotes; `'Security Administrator'`, for example.

- Use a backslash (“\”) preceding the space; `Security\ Administrator`, for example.

Entering quotation marks in strings

If you want to include a quotation mark, single quote or apostrophe in a string, you must precede the character with a backslash character. To include a backslash, enter two backslashes.

Entering a question mark (?) in a string

If you want to include a question mark (?) in a string, you must precede the question mark with **CTRL-V**. Entering a question mark without first entering **CTRL-V** causes the CLI to display possible command completions, terminating the string.

Special characters

The characters <, >, (,), #, ’, and ” are not permitted in most FortiDB CLI fields nor are they permitted in the passwords used to protect configuration-file backups.

IP address formats

You can enter an IP address and subnet using either dotted decimal or slash-bit format. For example you can type either:

```
set ip 192.168.1.1 255
```

or

```
set ip 192.168.1.1/24
```

The IP address is displayed in the configuration file in dotted decimal format.

DNS for hostname recognition

A Domain Name Service (DNS) will enable you to use machine names as well as IP addresses in your CLI commands.

You can setup DNS via:

- The FortiDB GUI
- The FortiDB CLI console (using SSH or *telnet*)

In order to setup DNS using the FortiDB GUI:

1. Go to the **Appliance** section of the left-side tree navigator and select **Network**
2. On the **Network Configuration** page, select the **DNS** tab.
3. Enter the IP addresses for your **Primary DNS Server** and **Secondary DNS Server**.
4. Select the **Apply** button.

In order to setup DNS using the FortiDB CLI:

1. Logon as the `admin` user in your SSH or telnet console window.
2. Enter the following:

```
config system dns
    set primary <dns-server-ip>
    set secondary <dns-server-ip>
end
```

where:

- `<dns-server-ip>` represents the IP address for your primary and secondary DNS-server machines

FTP-directory abbreviations

When specifying file locations on your FTP server, you can use these abbreviations:

- `.` which refer to the currently logged-in user's home directory on the FTP server. For example:

```
diagnose system export va_log <your_ftp_server> <your_ftp_username>
 <your_ftp_password> . myDiagnose.tar
```

- `./<subdirectory>` which refer to an existing subdirectory of the currently logged-in user's home directory on the FTP server. For example:

```
diagnose system export va_log <your_ftp_server> <your_ftp_username>
 <your_ftp_password> ./diagnostics myDiagnose.tar
```

CLI Command Syntax

This topic provides general CLI-syntax information.

This guide uses the following conventions to describe command syntax:

- Angle brackets < > indicate variables.

  For example:

  ```
  execute restore config <filename_str>
  ```

  You enter:

  ```
  execute restore config myfile.bak
  ```

- Vertical bar and curly brackets `{|}` separate alternative, mutually exclusive required keywords.

  For example:

  ```
  set protocol {ftp | sftp}
  ```

  You can enter:

  ```
    set protocol ftp or set protocol sftp
  ```

- Square brackets `[ ]` indicate that a keyword or variable is optional.

  For example:

  ```
  show system interface [<name_str>]
  ```

  To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the `Port1` interface, you can enter `show system interface port1`.

- A space separates options that can be entered in any order and in any combination and that must be separated by spaces.

  For example:

  ```
  set allowaccess {https ping ssh}
  ```

  You can enter any of the following:

  ```
  - set allowaccess ping
  - set allowaccess https ping
  - set allowaccess ssh
  - set allowaccess https ssh
  - set allowaccess https ping ssh
  ```

  In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.

- Special characters:
  - The `\` is supported to escape spaces or as a line continuation character

- The single quotation mark ' and the double quotation mark " are supported, but must be used in pairs.
- If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Administration Commands

This topic lists the system-administration commands that are available to the FortiDB user.

Note: For general CLI usage information, see the *Basic CLI Information* section of this document.

The following commands are available for the FortiDB CLI:

Command branch	Supported commands	Description
config	• system admin setting • system backup all-settings • system dns • system interface • system ntp • system route	Use *config* to configure objects of FortiDB functionality. Top-level objects are not configurable; they are containers for more specific lower-level objects. For example, the *system* object contains DNS addresses, interfaces, routes and so on. When these objects are multiple, such as routes, they are organized in the form of a table. You can add, delete or edit the entries in the table. Table entries each consist of keywords that you can set to particular values. Simpler objects, such as system DNS, are a single set of keywords.
execute	• backup all-settings • backup-remove fd-archive • backup-remove fd-report • date • format disk • ping • reboot • reset • restart • restore all-settings • restore fd-archive • shutdown • time • top • traceroute • raid rebuild	Use *execute* to run static commands, to reset the FortiDB unit to factory defaults, or to back up or restore the FortiDB configuration. The execute commands are available only from the root prompt.
show	• system admin setting • system backup all-settings	Use *show* to display the FortiDB unit configuration. Only changes to the default configuration are displayed.

Command branch	Supported commands	Description
	• system dns • global • system interface • system ntp • system route • system raid	You can use *show* within a *config* shell to display the configuration of that shell, or you can use *show* with a full path to display the configuration of the specified shell.
diagnose	• system export fd_log • system raid list • network interface list • network interface detail [port-name]	Use *diagnose* commands to view the detail information of ethernet interfaces, or send the diagnostic information to an FTP serve.

config command

This topic contains the information about the *config* commands that are available to the FortiDB user.

You can use the FortiDB CLI in order to perform the following *config* tasks.

config system admin setting

The *config system admin setting* command allows you to configure web administration settings.

Syntax:

```
config system admin setting
 set http_port <integer>
 set https_port <integer>
 set idle_timeout <integer>
end
```

where:

Variables	Description	Default
`http_port`	The HTTP port number for web administration.	80
`https_port`	The HTTPS port number for web administration.	443
`idle_timeout`	The idle-timeout value which ranges from 1 to 480 minutes	5

Sample command: (This example sets an idle-timeout value of 2 minutes and port 444 for HTTPS web administration.)

```
config system admin setting
 set idle_timeout 2
 set https_port 444
end
```

config system backup all-setting

The *config system backup all-settings* command allows you to set or check the settings for scheduled backups.

Syntax:

```
config system backup all-settings
 set crptpasswd <passwd>
```

```
 set directory <dir_name>
 set passwd <pwd>
 set protocol {ftp | sftp}
 set server <string>
 set status {enable | disable}
 set time <hh:mm:ss>
 set user <user_name>
 set week_days {monday tuesday wednesday thursday friday}
end
```

where:

Keywords and variables	Description	Default
`crptpasswd <passwd>`	Optional password to protect backup content	None
`directory <dir_name>`	The directory on the backup server in which to save the backup file.	None
`passwd <pwd>`	The password for the backup server.	None
`protocol {ftp | sftp}`	The backup protocol.	`sftp`
`server <string>`	The IP address or DNS-resolvable host name for the backup server.	None
`status {enable | disable}`	Enable or disable scheduled backups.	disable
`time <hh:mm:ss>`	The time of day to perform the backup. Time is required in the form `<hh:mm:ss>`.	None
`user <user_name>`	The user account name for the backup server.	None
`week_days {monday tuesday wednesday thursday friday}`	The day(s) of the week on which to perform backups. You may select multiple days.	None

Sample command:

The backup server is at 172.20.120.11 using the admin account with no password and saving the backup in the /usr/local/backups directory. Backups will be done on Mondays at 1:00pm using ftp.

```
config system backup all-settings
  set status enable
  set server 172.20.120.11
  set user admin
  set directory /usr/local/backups
  set week_days monday
  set time 13:00:00
  set protocol ftp
end
```

config system dns

The *config system dns* command allows you to set the DNS server addresses.

Syntax:

```
config system dns
 set primary <dns_ip>
 set secondary <dns_ip>
end
```

where:

Keywords and variables	Description	Default
primary <dns_ip>	Enter the primary DNS server IP address.	172.30.62.6
secondary <dns_ip>	Enter the secondary DNS IP server address.	65.39.139.63

Sample Command:

```
config system dns
  set primary 65.39.139.53
  set secondary 65.39.139.63
end
```

config system global

The *config system global* command allows you to configure global settings that affect miscellaneous FortiDB features.

Syntax:

```
config system global
  set console-output {more | standard}
  set daylightsavetime {enable | disable}
  set hostname <unithostname>
  set ssl-low-encryption {enable disable}
  set swapmem {enable | disable}
  set timezone <timezone_number>
end
```

Where:

Keywords and variables	Description	Default
console-output {more | standard}	Select how the output is displayed on the console. Select more to pause the output at each full screen until keypress. Select standard for continuous output without pauses.	standard
daylightsavetime {enable | disable}	Enable or disable daylight saving time. If you enable daylight saving time, the FortiDB system automatically adjusts the system time when the time zone changes to or from daylight saving time.	enable
hostname <unithostname>	Enter a name for this FortiDB system.	FD-XXX. The default hostname varies depending on the appliances.
ssl-low-encryption {enable disable}	Enable or disable low-grade (40-bit) encryption.	disable
swapmem {enable | disable}	Enable or disable virtual memory.	enable

Keywords and variables	Description	Default
timezone <timezone_number>	The number corresponding to your time zone. Press ? to list time zones and their numbers. Choose the time zone for the FortiDB system from the list and enter the correct number.	00

Sample Command:

The following command turns on daylight saving time, sets the FortiDB system name to FDB1K, and chooses the Eastern timezone for US & Canada.

```
config system global
  set daylightsavetime enable
  set hostname FDB1k
  set timezone 12
end
```

config system interface

The *config system interface* command allows you to edit the configuration of a FortiDB network interface.

Syntax:

```
config system interface
 edit <port>
 set allowaccess {http https ping ssh telnet}
 set ip <ipmask>
 set status {up | down}
end
```

Variable	Description	Default
<port>	<port> can be one of port1, port2, port3, port4.	No default.
allowaccess {http https ping ssh telnet}	Enter the types of management access permitted on this interface. Valid types are: http https ping ssh telnet. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.	Varies for each interface.
ip <ipmask>	Enter the interface IP address and netmask. The IP address cannot be on the same subnet as any other interface.	No default
status {up | down}	Start or stop the interface. If the interface is stopped it does not accept or send packets. If you stop a physical interface, VLAN interfaces associated with it also stop.	up

Sample Command:

This example shows how to set the FortiDB port1 interface IP address and netmask to 192.168.100.159 255.255.255.0, and the management access to ping, https, and ssh.

```
config system interface
 edit port1
 set allowaccess ping https ssh
 set ip 192.168.100.159 255.255.255.0
 set status up
end
```

config system ntp

The *config system ntp* command allows you to configure automatic time setting using a network time protocol (NTP) server.

Syntax:

```
config system ntp
 set server <server_ip>
 set status {enable | disable}
 set sync_interval <minutes>
end
```

Variable	Description	Default
server <server_ip>	Enter the IP address or fully qualified domain name of the NTP server.	No default.
status {enable | disable}	Enable or disable NTP time setting.	disable
sync_interval <minutes>	Enter how often, in minutes, the FortiDB system synchronizes its time with the NTP server.	60

config system route

The *config system route* command allows you to view or configure static routing table entries.

Syntax:

```
config system route
 edit <seq_num>
 set device <port>
 set dst <dst_ip_mask>
 set gateway <gw_ip>
end
```

Variable	Description	Default
<seq_num>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.	No default.
device <port>	Enter the port used for this route.	No default.
dst <dst_ip_mask>	Enter the IP address and mask for the destination network.	0.0.0.0 0.0.0.0
gateway <gw_ip>	Enter the default gateway IP address for this network.	0.0.0.0

config system raid

The *config system raid* command allows you to view or configure hard disk raid.

Syntax:

```
config system raid
 set level raid1
end
```

Variable	Description	Default
level	Set raid level. Use this command to create harddisk raid.	must be "raid1"

Note:

- Create raid will remove all exist data in hard disks.
- Only 'raid1' is supported in this version of fortidb appliance. And please check your hardware specification to see if your appliance supports raid.
- To create raid, you must have 2 hard disks in appliance disk bays.
- Once create raid, the hard disk cannot go back with original partitions.
- Use CLI "diagnose system raid list" to check current raid status.

execute command

This topic explains the *execute* administration commands that are available to the FortiDB user.

Note: For general CLI usage information, see the *Basic CLI Information* section of this document.

You can use the FortiDB CLI in order to perform the following *execute* tasks:

execute backup all-settings

The FortiDB CLI allows you to back up your local database to a FTP server.

Note: Please press <enter> to get back to the original prompt after the backup has completed with the message saying "Transfer Finished.

Syntax:

```
execute backup all-settings <ftp server> <filepath> <username> <password>
 [cryptpasswd]
```

where:

Keywords and variables	Description
<ftp server>	IP address or hostname of FTP server.
<filepath>	Location on FTP server where you want the settings file to be placed. note: If you don't specify a name, you will get a default file called fdb_allbackup.dat.
<username>	User name of account that logs on to the FTP server.
<password>	Password of account that logs on to the FTP server.
[crptpasswd]	Optional password for protecting the settings file on the FTP server.

Sample command:

```
execute backup all-settings <your_ftp_server> . <your_ftp_username>
 <your_ftp_password> myCrptpasswd
```

execute backup-remove fd-archive

This FortiDB CLI allows you to backup and then remove archives to a FTP server.

Note: Please press <enter> to get back to the original prompt after the backup has completed with the message saying "Transfer Finished.

Syntax:

```
execute backup-remove fd-archive <before-date> <ftp server> <username>
 <password> [directory][filename]
```

where:

Keywords and variables	Description
<before-date>	Date of the last archive you want included in your backup. For example, if you specify 2008-12-31, the backup will include archives for up to this date. The format is YYYY-MM-DD (MM(1-12), DD(1-31)). YYYY is a 4-digit number representing the year. MM is a 2-digit number from 1 to 12 representing the month. DD is a 2-digit number from 1 to 31 representing the day of the month.
<ftp server>	IP address or hostname of FTP server.
<username>	User name of account that logs on to the FTP server.
<password>	Password of account that logs on to the FTP server.
[directory]	Location on FTP server where you want the tar file to be placed.
[filename]	Name for the tar file on the FTP server where you want the archives to be placed. The default file name is FD-ARCHIVE-<before-date>.tar.

Sample command:

```
execute backup-remove fd-archive 2008-07-30 <your_ftp_server>
 <your_ftp_username> <your_ftp_password> . myArchives.tar
```

execute backup-remove fd-report

This FortiDB CLI allows you to backup and then remove reports to a FTP server.

Note: Please press <enter> to get back to the original prompt after the backup has completed with the message saying "Transfer Finished.

Syntax:

```
execute backup-remove fd-report <before-date> <ftp server> <username>
 <password> [directory][filename]
```

where:

Keywords and variables	Description
<before-date>	Date of the last archive you want included in your backup. For example, if you specify 2008-12-31, the backup will include reports for up to this date. The format is YYYY-MM-DD

Keywords and variables	Description
	(MM(1-12), DD(1-31)). YYYY is a 4-digit number representing the year. MM is a 2-digit number from 1 to 12 representing the month. DD is a 2-digit number from 1 to 31 representing the day of the month.
<ftp server>	IP address or hostname of FTP server.
<username>	User name of account that logs on to the FTP server.
<password>	Password of account that logs on to the FTP server.
[directory]	Location on FTP server where you want the tar file to be placed.
[filename]	Name for the tar file on the FTP server where you want the reports to be placed. The default file name is FD-REPORT-<before-date>.tar.

Sample command:

```
execute backup-remove fd-report 2008-07-30 <your_ftp_server>
 <your_ftp_username> <your_ftp_password> . myReports.tar
```

execute date

The *execute date* command allows you to get or set the system date. If you do not specify a date, the command returns the current system date.

Syntax:

```
execute date [<date_str>]
```

where:

Variable	Description
<date_str>	This variable has the form mm/dd/yyyy. • mm is the month and can be 01 to 12 • dd is the day of the month and can be 01 to 31 • yyyy is the year and can be 2001 to 2100 Dates entered will be validated - mm and dd require 2 digits, and yyyy requires 4 digits.

Sample command(This example sets the date to 17 September 2008):

```
execute date 09/17/2008
```

execute format disk

The *execute format disk* command allows you to format the hard disk on the FortiDB system. Executing this command will erase all device settings/images, VPN & Update Manager databases, and log data on the FortiDB system's hard drive. FortiDB's IP address and routing information will be preserved.

Syntax:

```
execute format disk
```

When you run this command, you will be prompted to confirm the request.

Warning: If you use this command without executing `backup all settings` command, you may not be able to view assessments or reports after you archive and restore your data. When you want to archive

and format disk, make sure that you execute `config system backup all-settings` command before archiving.

execute ping

The *execute ping* command allows you to send an ICMP echo request (ping) to test the network connection between the FortiDB system and another network device.

Syntax:

```
execute ping {<ip> | <hostname>}
```

where:

Variable	Description
<ip>	IP address of network device to contact
<hostname>	DNS resolvable hostname of network device to contact

Sample command(This example shows how to ping a host with the IP address 192.168.1.23):

```
execute ping 192.168.1.23
```

execute reboot

The *execute reboot* command allows you to restart the FortiDB system. This command will disconnect all sessions on the FortiDB system.

Syntax:

```
execute reboot
```

execute reset

The *execute reset* command allows you to reset the FortiDB system to factory defaults. This command will disconnect all sessions and restart the FortiDB system.

Syntax:

```
execute reset {admin-password | all-settings | data}
```

where:

commands	Description
admin-password	Reset admin's password to default password.
all-settings	Reset the all settings.
data	Reset the database.

Sample command:

```
execute reset all-settings
```

execute restart

This FortiDB CLI allows you to restart the application server under which both FortiDB-VA (Vulnerability Assessment) and FortiDB-DAM (Data Activity Monitoring) are running.

Syntax:

```
execute restart appserver
```

execute restore all-settings

This FortiDB CLI allows you to restore previously backed up your local database, FortiDB system-configuration settings, archives and reports.

Syntax:

```
execute restore all-settings <ftp server> <filepath> <username> <password>
 [crptpasswd]
```

where:

Variable	Description
<ftp server>	IP address or hostname of FTP server.
<filepath>	Location of, and filename for, the settings file on the FTP server.
<username>	User name of account that logs on to the FTP server.
<password>	Password of account that logs on to the FTP server.
[crptpasswd]	Optional password for protecting the settings file on the FTP server.

Note: This operation will replace your current settings and necessitate a reboot.

Sample command:

```
execute restore all-settings <your_ftp_server> ./fdb_allbackup.dat
 <your_ftp_username> <your_ftp_password> myCrptpasswd
```

execute restore fd-archive

This FortiDB CLI allows you to restore previously backed up your archives.

Syntax:

```
execute restore fd-archive <ftp server> <filepath> <username> <password>
```

where:

Variable	Description
<ftp server>	IP address or hostname of FTP server.
<filepath>	Location of, and filename for, the settings file on the FTP server.
<username>	User name of account that logs on to the FTP server.
<password>	Password of account that logs on to the FTP server.

Note: This operation will replace your current settings and necessitate a reboot.

Sample command:

```
execute restore fd-archive <your_ftp_server> ./fdb_allbackup.dat
 <your_ftp_username> <your_ftp_password>
```

execute shutdown

The *execute shutdown* command allows you to shut down the FortiDB system. This command will disconnect all sessions.

Syntax:

```
execute shutdown
```

execute time

The *execute time* command allows you to get or set the system time.

Syntax:

```
execute time [<time_str>]
```

where:

Variable	Description
<time _str>	This variable has the form hh:mm:ss. • hh is the hour and can be 00 to 23 • mm is the minutes and can be 00 to 59 • ss is the seconds and can be 00 to 59 All parts of the time are required. Single digits are allowed for each of hh, mm, and ss.

If you do not specify a time, the command returns the current system time.

Sample command (This example set the system time to 15:31:03):

```
execute time 15:31:03
```

execute top

The *execute top* command allows you to view the processes running on the FortiDB system.

Syntax:

```
execute top
```

To exit the display, type q. Other interactive commands are available while running top. For help on them, type h.

The execute top command displays the following information:

```
15:28:03 up 2 days, 0 users, load average: 0.06, 0.04, 0.01
Tasks: 82 total, 2 running, 80 sleeping, 0 stopped, 0 zombie
CPU(s): 0.0% us, 0.0% sy, 0.0% ni, 100.0% id, 0.0% wa, 0.0% hi, 0.0% si
Mem: 2069772K total, 485764K used,  1584008K free, 40124K buffers
Swap: 2069764K total,     0K used,  2069764K free,  7275k cached

PID   USER   PR   NI  VIRT  RES  SHR  S  %CPU %MEM  TIME+ COMMAND
  1   root   18    0  3232  1012 720  S     0  0.0  0:07.12 init
  2   root   RT    0     0     0   0  S     0  0.0  0:00.00 migration/0
  3   root   34   19     0     0   0  S     0  0.0  0:00.00 ksoftirqd/0
  4   root   RT    0     0     0   0  S     0  0.0  0:00.00 migration/1
  5   root   39   19     0     0   0  S     0  0.0  0:00.00 ksoftirqd/1
  6   root   RT    0     0     0   0  S     0  0.0  0:00.00 migration/2
  7   root   33   19     0     0   0  S     0  0.0  0:00.00 ksoftirqd/2
  8   root   RT    0     0     0   0  S     0  0.0  0:00.00 migration/3
  9   root   34   19     0     0   0  S     0  0.0  0:00.00 ksoftirqd/3
 10   root   10   -5     0     0   0  S     0  0.0  0:00.00 events/0
 11   root   10   -5     0     0   0  S     0  0.0  0:00.00 events/1
 12   root   10   -5     0     0   0  S     0  0.0  0:00.00 events/2
 13   root   10   -5     0     0   0  S     0  0.0  0:00.00 events/3
 14   root   10   -5     0     0   0  S     0  0.0  0:00.00 khelper
 15   root   10   -5     0     0   0  S     0  0.0  0:00.00 kthread
 21   root   10   -5     0     0   0  S     0  0.0  0:00.00 kblockd/0
```

execute traceroute

The *execute traceroute* command allows you to test the connection between the FortiDB system and another network device, and display information about the network hops between the device and the FortiDB system.

Syntax:

```
execute traceroute {<address_ipv4> | <host-name>}
```

where:

Variable	Description
<address_ipv4>	IP address of network device.
<host-name>	FQDN hostname of network device.

Sample command:

```
execute traceroute <your_IPaddress>
```

execute raid rebuild

The *execute raid rebuild* command allows you to rebuild the hard disk raid when the raid is corrupted.

Syntax:

```
execute raid rebuild
```

Note:

- Rebuild raid will clean all exist data in 2nd hard disk.
- If you just replace the 2nd disk from exist raid, the new inserted disk will get raid synchronizing automatically and does not need rebuild raid. But if the 2nd disks was part of raid volume before, usually need rebuild it.

show commands

This topic contains the information about the *show system* commands that are available to the FortiDB user. Only changes to the default configuration are displayed.

You can use the *show* command within a config shell to display the configuration of that shell, or you can use the *show* command with a full path to display the configuration of the specified shell. To display the configuration of all config shells, you can use the *show* command from the root prompt.

show system admin setting

The *show system admin setting* command allows you to display the change of system-administration settings.

Syntax:

```
show system admin setting
```

show system backup all-settings

The *show system backup all-setting*s command allows you to display the change of system backup settings.

Syntax:

```
show system backup all-settings
```

show system dns

The *show system dns* command allows you to display the change of the DNS server addresses.

Syntax:

```
show system dns
```

Sample Result:

```
FD-XXX # show system dns
config system dns
    set primary 65.39.139.53
    set secondary 65.39.139.63
end
```

show system global

The *show system global* command allows you to display the change of global settings.

Syntax:

```
show system global
```

show system interface

The *show system interface* command allows you to display the change of a FortiDB network interface.

Syntax:

```
show system interface
```

Sample Result:

```
FD-XXX # show system interface
config system interface
    edit "port1"
        set ip 172.30.62.80 255.255.255.0
        set allowaccess ping https ssh telnet http
    end
```

show system ntp

The *show system ntp* command allows you to display the change of the automatic time setting using a network time protocol (NTP) server.

Syntax:

```
show system ntp
```

Sample Result:

```
FD-XXX # show system ntp
config system ntp
    set server "132.246.168.147"
    set status enable
    set sync_interval 120
end
```

show system route

The *show system route* command allows you to display the change of the static routing table entries.

Syntax:

show system route

Sample Result:

```
FD-XXX # show system route
config system route
 edit 1
        set device "port1"
        set gateway 172.30.62.254
```

```
end
```

get and set commands

This topic describes some examples to use get command and set command.

get command

The *get* command allows you to retrieve system settings.

Here is an example which retrieves the current system-administration settings:

```
get system admin setting <Enter>
http_port           : 80
https_port          : 443
idle_timeout        : 2
```

set command

The *set* command allows you to set specific properties within a settings category.

Here is an example which uses *set* to change a default value for a property within the system-administration settings category:

```
show system admin setting <Enter>

config system admin setting <Enter>
(setting)# set idle_timeout 2
end

show system admin setting <Enter>
config system admin setting
    set idle_timeout 2
end
```

diagnose command

diagnose command display diagnostic information that helps you to troubleshoot problems.

You can use the FortiDB CLI in order to perform the following *config* tasks.

diagnose system export fd_log

This FortiDB CLI allows you to export debug log files to an FTP server

Syntax:

```
diagnose system export fd_log <ftp server> <user> <password> [directory]
 [filename]
```

where:

Keywords and variables	Description
<ftp server>	IP address or hostname of FTP server.
<username>	User name of account that logs on to the FTP server.
<password>	Password of account that logs on to the FTP server.
[directory]	Location on FTP server where you want the diagnostic file to be placed.
[filename]	Name of the zip file that contains several log files that will be put on the FTP server. If you don't specify a filename, you will get a default file called fortidb.zip.

Sample command:

```
diagnose system export fd_log <your_ftp_server> <your_ftp_username>
 <your_ftp_password> . myDiagnose.zipd
```

diagnose system raid list

This FortiDB CLI allows you to check hard disk raid status

Syntax:

```
diagnose system raid list
```

diagnose network interface list

This FortiDB CLI allows you to view status of ethernet interfaces

Syntax:

```
diagnose network interface list
```

diagnose network interface detail

This FortiDB CLI allows you to view detail information of ethernet interface

Syntax:

```
diagnose network interface detail <port name>
```

where:

Variable	Description
<port name>	Ethernet interface name, such as 'port1'.

Sample command:

```
diagnose network interface detail port1
```

Contact Information

Getting Fortinet Contact Information

Please go to following Fortinet main website or Customer Service & Support website for contact information:

- http://www.fortinet.com/
- http://support.fortinet.com/

Or, after login FortiDB, click the 'Support' link at right top of any page, to goto the support website.