

LED	State	Description
Power	Green	The device is connected to a power source and on.
Hard Disk	Flashing Green	Activity on the hard disk.
Alarm	Red	Hard disk failure.
Ports 1 to 4 Right LED	Green	The correct cable is connected to the interface and the connected equipment has power.
	Flashing	Network activity at this interface.
Ports 1 to 4 Left LED	Green	The interface is connected at 1000 Mbps.
	Amber	The interface is connected at 100 Mbps.
	Off	The interface is connected at 10 Mbps.



Visit these links for more information and documentation for your Fortinet product.

- Technical Documentation - <http://docs.forticare.com>
- Fortinet Knowledge Center - <http://kc.forticare.com>
- Fortinet Technical Support - <http://support.fortinet.com>

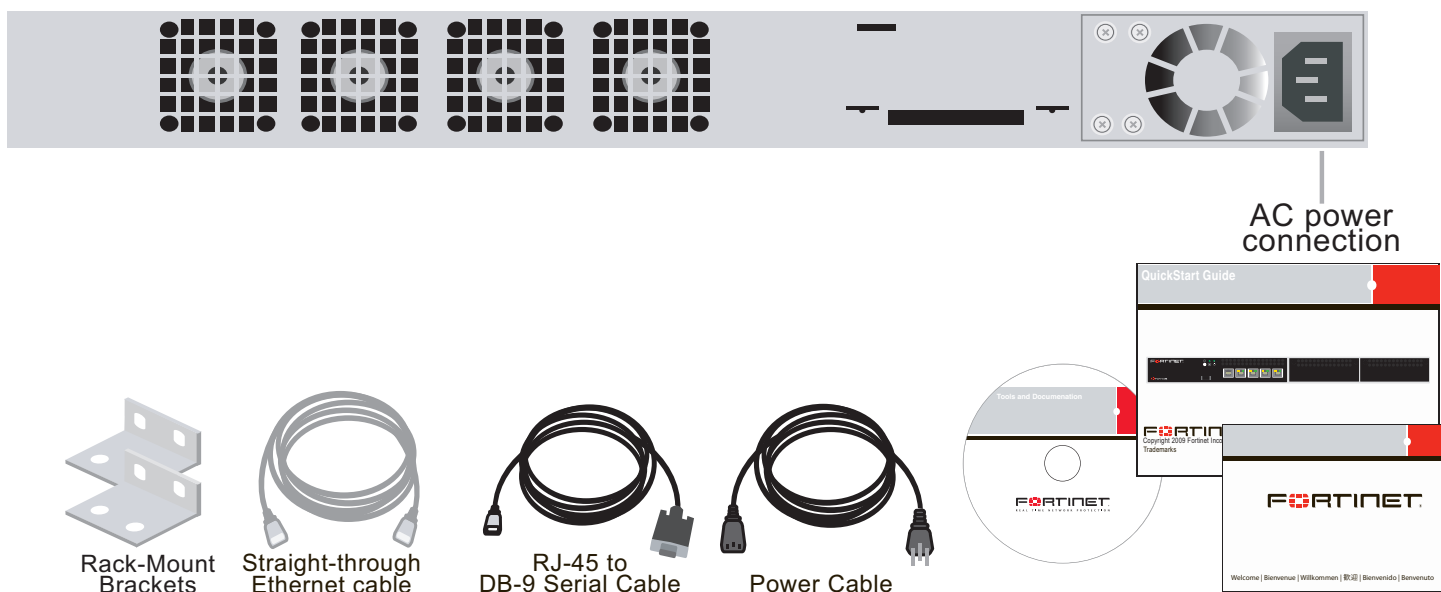
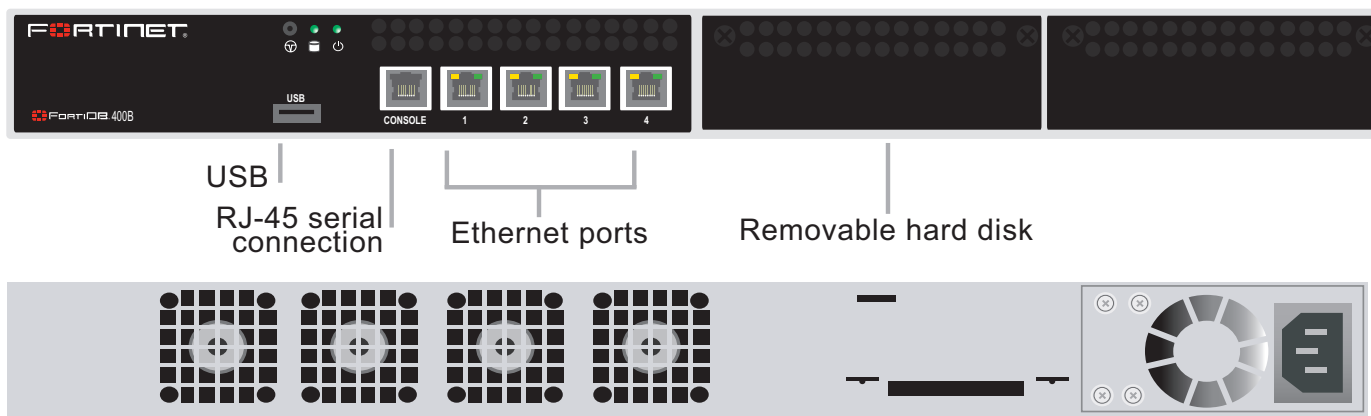


© Copyright 2009 Fortinet Incorporated. All rights reserved.
 Products mentioned in this document are trademarks or registered trademarks of their respective holders.
 Regulatory Compliance
 FCC Class A Part 15 CSA/CUS
 7 January 2009

15-32000-86800-20090107

Package Contents

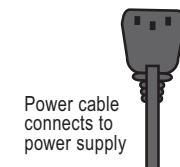
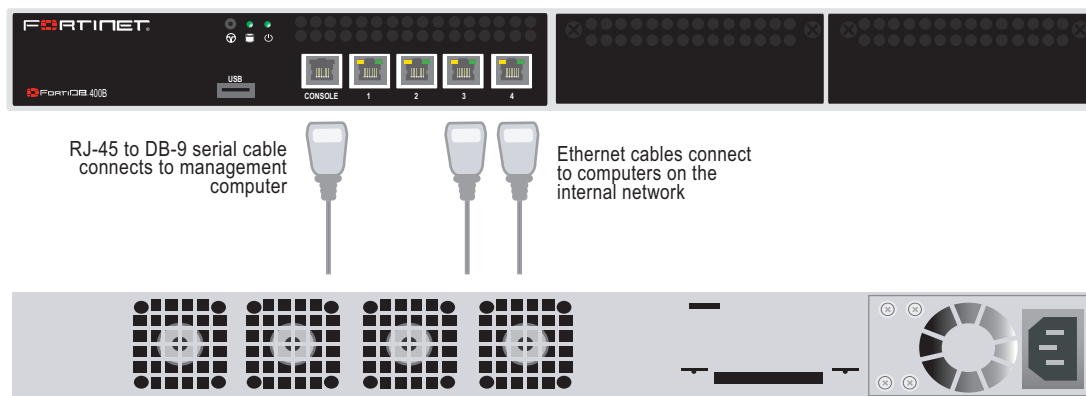
Connector	Type	Speed	Protocol	Description
Ports 1 to 4	RJ-45	10/100/1000 Base-T	Ethernet	Copper gigabit connection to 10/100/1000 copper networks.
CONSOLE	RJ-45	9600 8/N/1	RS-232 serial	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB	USB		USB	For future use.



Connecting

Connect the following to the FortiDB unit. Ensure the FortiDB unit is placed on a stable surface or install in a standard 19 inch rack.

- Insert one end of an Ethernet cable into port 1.
- Connect the other end of the Ethernet cable to the network hub or switch.
- Connect the AC Power cable to the Power Supply on the back of the FortiDB unit.
- Connect the other end of the Power cable to a surge protected power bar or power supply.



Configuration Tools

Web-based manager

The FortiDB web-based manager is an easy-to-use management tool. Use it to configure the administrator password, the interface and default gateway addresses, and configure reports.

Requirements:

- An Ethernet connection between the FortiDB unit and management computer.
- A web browser such as FireFox or Internet Explorer on the management computer.

Command Line Interface (CLI)

The CLI is a full-featured management tool. Use it to configure the administrator password, the interface addresses, the default gateway address, and the DNS server addresses. To configure advanced settings, see the Tools and Documentation CD included with the FortiDB unit.

Requirements:

- The RJ-45 to DB9 serial connection between the FortiDB unit and management computer.
- A terminal-emulation application such as HyperTerminal for Windows, on the management computer.

Collecting Information

Port Information

Port 1	IP:	_____
	Netmask:	_____
Port 2	IP:	_____
	Netmask:	_____
Port 3	IP:	_____
	Netmask:	_____
Port 4	IP:	_____
	Netmask:	_____

The internal interface IP address and netmask must be valid for the internal network.

Configuring

Use the following CLI commands to configure the FortiDB unit for the network. For details on using the CLI, see the *CLI Reference*.

Configuring the IP address and netmask

```
config system interface
  edit port1
    set ip <intf_ip><netmask>
  end
```

Configure the default gateway

```
config system route
  edit 1
    set device <port_number>
    set dst <ip_address><netmask>
    set gateway <gateway_ip>
  end
```

VA QuickStart Guide

This guide leads you through the process that results in the creation of a vulnerability assessment report for one of your target databases. The example below assumes you will be assessing an Oracle target database. Before starting assessment, you will need to make sure that the FortiDB user for your Oracle target database has the following privileges:

- CREATE SESSION
- SELECT_CATALOG_ROLE
- SELECT SYS.AUDIT\$
- SELECT SYS.REGISTRY\$HISTORY
- SELECT SYS.USER\$
- SELECT SYS.LINK\$
- SELECT SYSTEM.SQLPLUS_PRODUCT_PROFILE

1. Login to FortiDB as the FortiDB default admin user (admin) using `fortidb1!$` for the password.
2. Create a target-database connection.
 - a. Select **Targets** link under **Target Management**.
 - b. Select **Add** and select the **General** tab.
 - 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:** vatarget
 - **Type:** Oracle
 - **Port:** 1521
 - **Host Name:** (IP address or machine name on your system that contains the Oracle target database.)
 - **User Name:** (Name of the FortiDB user for your Oracle target database)
 - **Password:** (Password of the FortiDB user for your Oracle target database)
 - d. Select the **Test Connection** to verify your target database is reachable and that your connection parameters are correct. You should see a 'Success' message.
 - e. Select **Save**. vatarget appears on the Targets page under the **Name** column header.
3. Run assessment against your target database.
 - a. Go to **Assessments** under **Assessments Management**.
 - b. Select the check box to the left of **Scan All Oracle Databases** which your target database belongs to.
 - c. Select **Run**. After a minute or so, you should see the Last Run Time column in the Scan All Oracle Database row get populated with a stop date and time for the assessment you just ran.

Note: If you want to create your own target group, policy group, or assessment, please refer to online help for detailed instructions.

Generating a Report

We will examine our assessment with the Summary Failed Report which summarizes failed-policy results.

1. Go to **Pre-Defined Report** under **Report Management**.
2. Select **Summary Failed Report**.
3. On the Vulnerability Assessment Summary Failed Report page, select:
 - **Scan All Oracle Databases** from the Assessment Name dropdown list
 - The start date and time associated with Scan All Oracle Databases from the Assessment Time dropdown list.
 - Target name, which is vatarget in this example, from the **Target** dropdown list.
4. Select the **Preview Report** tab and, after it is compiled, a Summary Failed Report will appear in your browser.
5. 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 click the **Export** button. The following file formats are supported:
 - PDF
 - Excel
 - Tab-delimited
 - Comma-separated values

FortiDB MA Quick Start

This section leads you through the process that results in the creation of a Monitoring and Auditing report for one of your target databases. The example below assumes monitoring of an Oracle target database and generating alerts using User Behavior Monitor, and creating reports using Alert Report Manager. If you want to set to audit_trail=OS, you need to run FortiDB Audit log agent. For details, see the *Administration Guide*.

Note: To display FortiDB MA Web user interface, you need to use Internet Explorer 7. To allow FortiDB MA to assess or monitor Oracle databases, create an Oracle user with the following privileges. For other modules, see the Administration Guide.

General settings

Administrator password:		
Network Settings:	Default Gateway:	_____
	Primary DNS Server:	_____
	Secondary DNS Server:	_____

Factory default settings

NAT/Route mode	Transparent mode		
Port 1 interface	192.168.1.99	Management IP	0.0.0.0
Port 2 interface	192.168.2.99	Administrative account settings	
Port 3 interface	192.168.3.99	User name	admin
Port 4 interface	192.168.4.99	Password	fortidb1!\$

To reset the FortiDB unit to the factory defaults, in the CLI type the command

```
execute reset all-settings
```

- CREATE SESSION
- SELECT_CATALOG_ROLE
- DELETE_CATALOG_ROLE
- AUDIT ANY
- AUDIT SYSTEM
- SELECT SYS.AUD\$
- SELECT on the monitored tables or SELECT ANY TABLE

1. Login to FortiDB MA as admin using `fortidb1!$` for the password.
2. Create a FortiDB MA user who has User Behavior Monitor User Role and Report Manager User Role.
 - a. In the left-side navigation tree, click on **User Administration**.
 - b. Select **Add New User** link at the bottom.
 - c. On the **Add New User** page, enter the following information.
 - User Name
 - Password
 - Password Again
 - First Name and Last Name
 - Email Address
 - d. On the **Status** field, check **Active** to activate a new user you will create.
3. On the **Software Module** section, check the User role of User Behavior Monitor and Alert Report Manager.
 - a. Click the **Save** button.
 - b. Click the **Logout** link at the top-right of the screen in order to logout as the admin user.
4. Log in as the newly created user, and create a target-database connection.
 - a. In the left-side navigation tree, click on the **User Behavior Monitor** link.
 - b. Click **Database > New** from the top menu
 - c. On the **Create New Database Connection** page, enter Oracle target database information:
 - **Database Connection Name:** specify any name (ex. ora123)
 - **Database Server Name, IP address, and port number:** enter <IP address>:1521 (ex. 172.30.62.11:1521)
 - **Database Server type :** select Oracle from the pull-down list
 - **Database Name:** enter your target database name (ex. Ora123)
 - **User Name:** enter your target database user name (ex. testuser1)
 - **Password:** enter your target database password (ex. fortinet123)
 - d. Click the **Create** button.
 - e. To open the connection, go to **Database > Open**. Highlight the target database, ora123, and click the **Open and Run** button. The connection icon becomes the open status icon (green) in the left-side navigation tree.
5. To create an Object Policy, click **Set Policies > Object Policies**. In this example, we monitor security violation and suspicious OS user for SCOTT.BONUS table.
 - a. In the **Object Policies Configuration** page, click the **Add Item** link at the bottom.
 - b. In the **Item Settings** tab, click **S** in the **Show Schema** field, and select **SCOTT** from the schema pull-down list.
 - c. Click **ALL** in the **Show Table** field, and select **BONUS** from the **table** list.
 - d. For Audit-action type, check both **SELECT** and **INSERT/UPDATE/DELETE**.
 - e. In the **Access Violation Settings** tab, check the **Active** box of "Security Violation" and "Suspicious OS User".
 - f. Check the **Enable this guard** item box.
 - g. Click the **Save** button.
6. To create a schedule, click **Set Defaults > Module Guard Schedule** on the top menu. For example, enter 1 in Minutes field of Interfal section to retrieve data every 1 minute.
7. Click the **Set Timer** button.
8. Login to your target database and execute SQL statements to generate alerts. For this example, login as SCOTT and select a table BONUS or insert/update/delete some data.
9. Go to **Analysis > Alerts Messages** to check alerts

Generating a Report

We will generate reports based on alerts created by User Behavior Monitor. The example below assumes that you will generate a one time only report in PDF format.

1. In the left-side navigation tree, click on the **Report Manager**.
2. Click **New Reports** under **Alert Report Manager**. Specify the following fields.
 - **Report Name (required):** enter "My Report 1" for example.
 - **Module:** check User Behavior Monitor check box.
 - **Database:** select ora123.For other fields, leave as default.
3. In the **Report Generate Schedule** section, check the **One Time Only** check box.
4. In the **Report Format** section, check the **Show Column of Description** (the default is unchecked).
5. Check **Enable Report** check box.
6. Click the **Save** button. The Current Reports page will display.
7. Click **Summary** in the Action column of My Report 1.
8. Click the **PDF** button to save the report in PDF format. You can save your report in these formats:
 - PDF
 - Excel
 - Tab Delimited
 - Comma Delimited