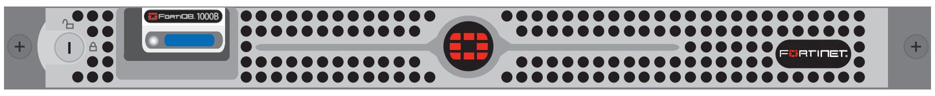
| LED | State | Description |
|---|---|---|
| Ports 1 to 4 Left LED | Green | The correct cable is connected to the copper 10/100/1000 interface and the connected equipment has power. |
| Ports 1 to 4 Right LED | Flashing | Network activity at this interface. |
| | Green | The interface is connected at 1000 Mbps. |
| | Yellow | The interface is connected at 100 Mbps. |

# QuickStart Guide

FortiDB-1000B



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

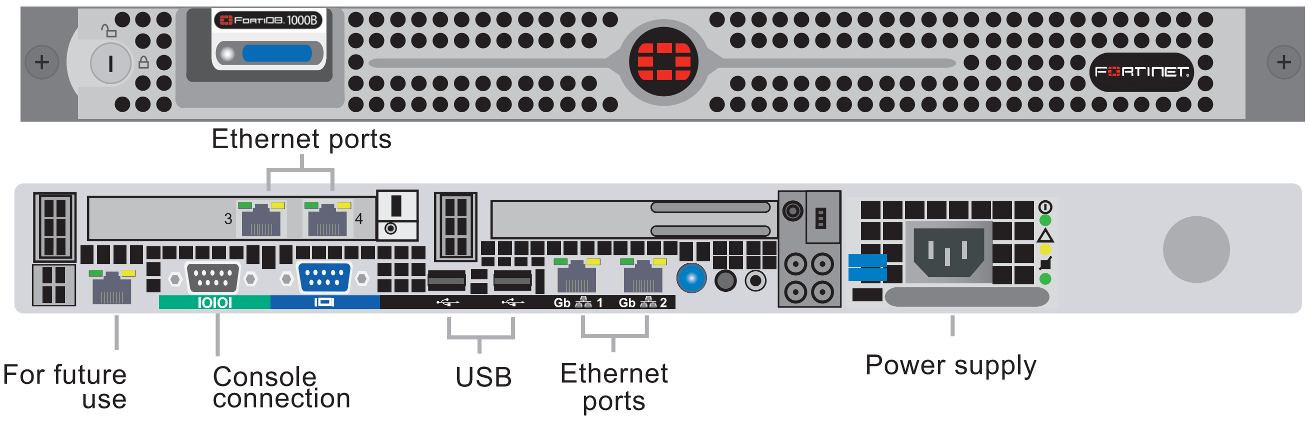
- Technical Documentation - **http://docs.forticare.com**
- Fortinet Knowledge Center - **http://kc.forticare.com**
- Fortinet Technical Support - **http://support.fortinet.com**

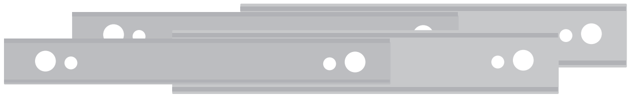
Regulatory Compliance
FCC Class B Part 15 CSA/CUS
30 September 2008

**15-31000-78779-20080930**

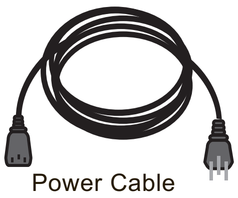
## Package Contents

| 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 | DB-9 | 9600 8/N/1 | RS-232 serial | Optional connection to the management computer. Provides access to the command line interface (CLI). |
| USB | USB | | USB | Optional connection to a USB key for firmware backup and installation. |



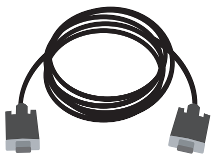


2 Mounting Slide Rails

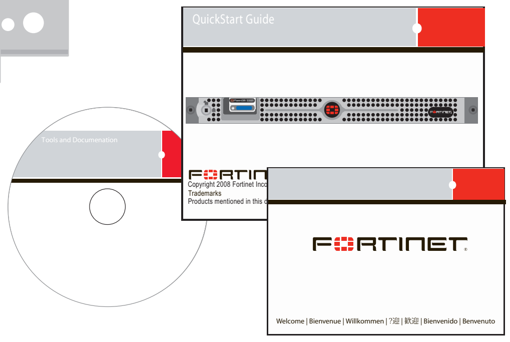


Power Cable

Straight-through Ethernet cable



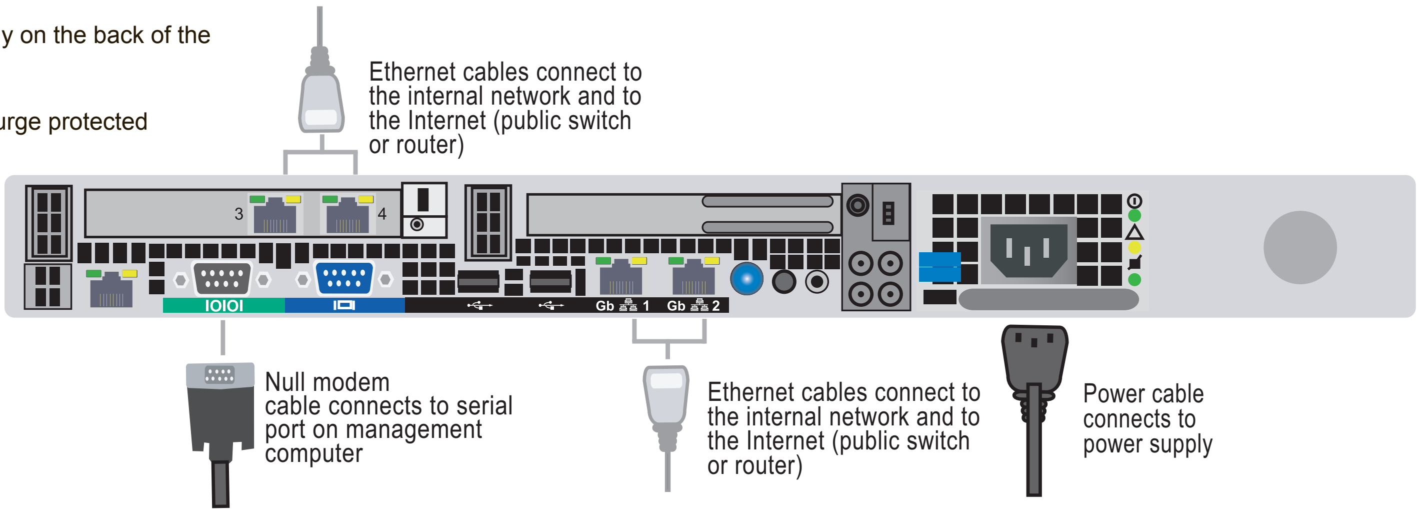
Null-Modem Cable (RS-232)



## 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.
See the *FortiDB-1000B Rack Installation Guide* for details.

- Insert one end of a 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.


Ethernet cables connect to the internal network and to the Internet (public switch or router)
3
4
IOIOI
Gb 1
Gb 2
Null modem cable connects to serial port on management computer
Ethernet cables connect to the internal network and to the Internet (public switch or router)
Power cable connects to 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 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.

## 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 | 0.0.0.0 | **Administrative account settings** | |
| Port 3 interface | 0.0.0.0 | User name | admin |
| Port 4 interface | 0.0.0.0 | Password | fortidb1!$ |

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

```
execute reset all-settings
```

# 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
```

### Application QuickStart

This section 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.

**Note:** 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 is other than an Oracle one, refer to the FortiDB Target Privilege Matrix in the *FortiDB Administration Guide*.

| **RDBMS** | **Required Privilege(s)** |
|---|---|
| Oracle | • CREATE SESSION<br>• SELECT_CATALOG_ROLE<br>• SELECT ON:<br>   • SYS.USER$<br>   • SYS.LINK$<br>   • 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**.
   b. Select Add and select the General tab.
   c. Enter the information in the text boxes marked with an asterisk (*). (Assume a user name of `vauser` and a password of `fdb!23`.)
   d. On the Add New User page, select on the Roles tab.
   e. Select these roles from the Available Roles list box:
      - Target Manager
      - Assessment Manager
      - Report Manager
   g. Select the Right arrow button to move those role names to the Assigned Roles text box.
   h. Select Save.
   i. Select Logout at the top-right of the screen 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**.
   c. Select Add and select the General tab.
   d. 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)
   f. Select Test Connection to verify your target database is reachable and that your connection parameters are correct. You should see a ‘Success’ message.
   g. Select Save. `vatarget` appears on the Targets page under the Alias Name column header.

4. Add the newly created connection to a target-database 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 > Target Groups**.
   b. Select Add.
   c. 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 Database 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 within the name, `vatarget`, that you assigned above.)
   e. Select Apply to see if this filter selects the target you created above.

5. Select the Save icon.

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

6. Assess the vulnerability of the target database in your group.
   a. Go to **Assessment Managment > Assessments**.
   b. Select Add.
   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. 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 select the Right arrow  button to move `mygroup` to the Assigned Target Groups text box.
   f. Associate the appropriate group of FortiDB-shipped policies with your assessment. 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 Right Arrow button 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 Groups list box, policies that belong to the Policy Group are displayed in the Active Policies list box.
   **Note:** The policies in the Active Policies lists box are selectable, but there is not functionality in the selection.
   h. Select Save. You should then see a ready-to-run assessment called myscan on the Assessments page.

7. Run your newly created assessment. 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 Run. After a minute, you should see the Last Run Time column in the myscan row populated with a stop date and time for the assessment you just ran.

8. 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 Reports**.
   b. 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 will see the fields 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  appears in your browser.
   e. To view your report in another of the supported formats, scroll down to the Export as drop down list, select a file format, and select Export. The following file formats are supported:
      - PDF
      - Excel
      - Tab-delimited
      - Comma-separated values