



Quick Start Guide

FortiDB
Version 3.2

FORTINET®

www.fortinet.com

FortiDB Quick Start Guide
Version 3.2
December 19, 2008
15-32000-78779-20081219

© Copyright 2008 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

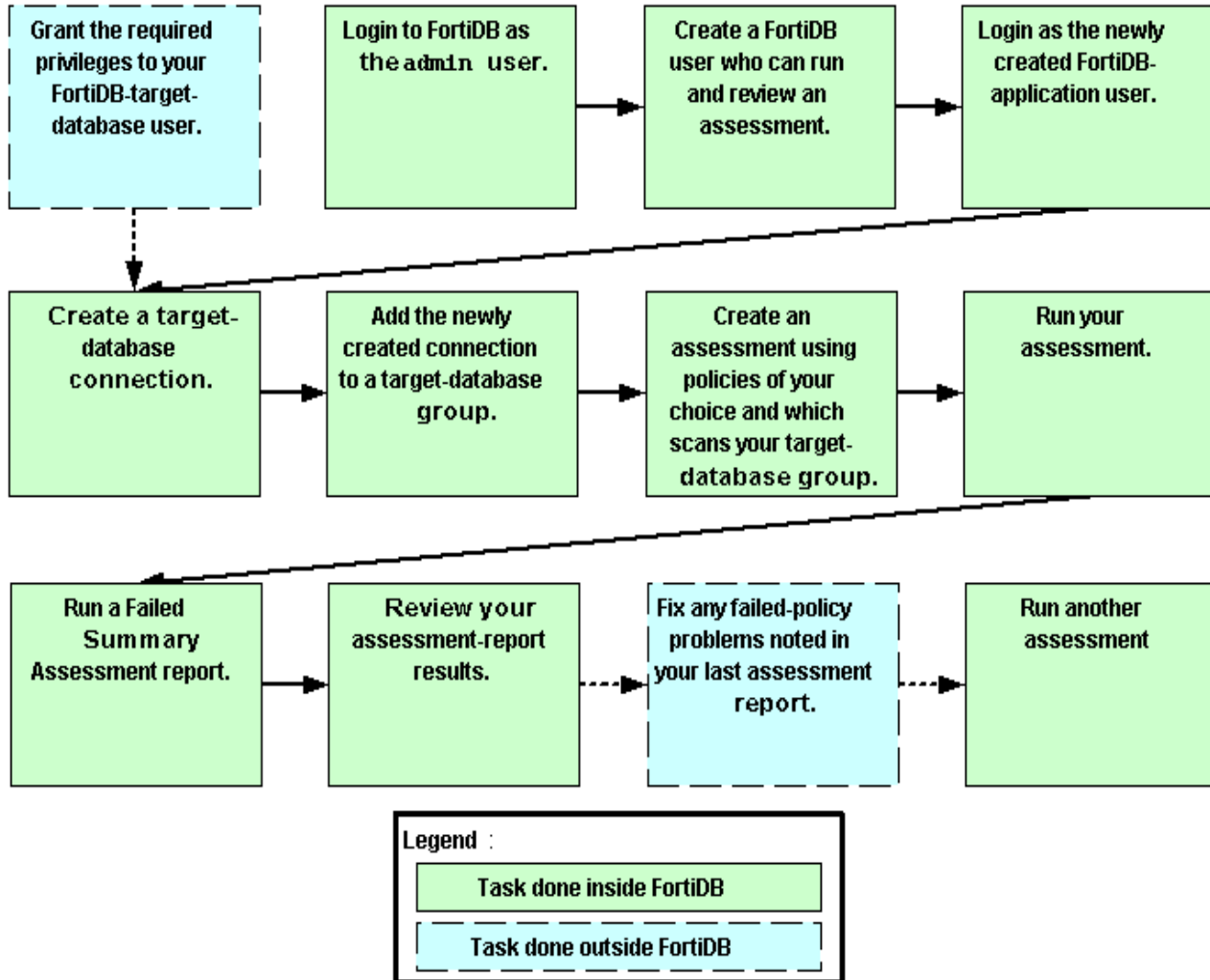
ABACAS, APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiDB, FortiGate, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners

Contents

QuickStart Flow Chart	5
FortiDB QuickStart Guide.....	7

QuickStart Flow Chart

This topic illustrates the Quick Start process detailed in the subsequent topic.



FortiDB 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.

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

RDBMS Type	Required Privilege(s)
Oracle	<ul style="list-style-type: none"> • CREATE SESSION • SELECT_CATALOG_ROLE • SELECT ON: <ul style="list-style-type: none"> – SYS.AUDIT\$ – SYS.REGISTRY\$HISTORY – SYS.USER\$ – SYS.LINK\$ – SYSTEM.SQLPLUS_PRODUCT_PROFILE

1. Login to FortiDB as the FortiDB `admin` user using `fortidb!$` 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 In the left-side navigation menu, click on the **User Management** link within the **Administration** section.
 - b On the **User Management** page, click the **Add** button.
 - c On the **Add New User** page, click 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, click on the **Roles** tab.
 - f On the **Roles**-tab, select these roles from the **Available Roles** list box:
 - **Target Manager**
 - **Assessment Manager**
 - **Report Manager**
 - g Click the  button in order to move those role names to the **Assigned Roles** text box.
 - h Click the **Save** button.
 - i Click 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 In the left-side navigation menu, click on the **Targets** link within the **Target Management** section.
 - c Click on the **Add** button.
 - d On the **Database Form** page, click on the **General** tab.
 - e On the **General**-tab form, fill 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 Click the **Test Connection** button in order to make sure your target database is reachable and that your connection parameters are correct. You should see a 'Success' message.
 - g Click the **Save** button. `vatarget` should appear 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 In the left-side navigation menu, click on the **Target Groups** link within the **Target Management** section.
 - b On the **Target Groups** page, click 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 **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 of the name, `vatarget`, that you assigned above.)
 - e Click the **Apply** button in order to see if this filter selects the target you created above.
 - f Click 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 In the left-side navigation menu, click on the **Assessments** link within the **Assessment Management** section.
 - b On the **Assessments** page, click the **Add** button.
 - c On the **Assessment** page, 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, click on 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 click 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, click on 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 click 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 Groups** 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 Click 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 Click 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 In the left-side navigation menu, click on the **Pre-Defined Report** link within the **Report Management** section.
 - b On the **Pre-Defined Reports** page, click on the **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 Click 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 click the **Export** button. The following file formats are supported:
 - PDF
 - Excel
 - Tab-delimited
 - Comma-separated values