

Users Guide

**FortiDB VA
Version 3.2**

FORTINET®

www.fortinet.com

FortiDB VA Users Guide
Version 3.2
December 19, 2008
15-32000-86933-20081219

© 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

Table of Contents

FortiDB Login	3
Login Steps	3
Changing Your Password.....	3
Target Databases Management	5
Target Icon Definitions	5
Adding (or Modifying) a Target Connection.....	5
Target Privilege Matrix	6
SSH Connections for Oracle and DB2	12
Using SSH Target-Database Connections.....	12
SSH Environment (for standalone users).....	13
Enabling OS-Level PDP (Solaris Only)	15
Deleting Target Database Connections	15
Adding Target Groups	16
Deleting Target Groups	17
Importing Target Database Data	17
Exporting Target Database Data	18
Auto Discovery	18
Considerations for Successful Discovery of DB2.....	18
Considerations for Successful Discovery of MS SQL Server.....	19
Running Auto Discovery.....	19
Adding Targets from Auto Discovery	20
Policy Management.....	21
About Policies.....	21
Policy Types.....	21
Policy Updates	21
Policy Groups.....	21
Exporting and Importing Policies.....	22
Policy States	22
Column and Group Information for Policies	22
Adding Policy Groups.....	23
Deleting Policy Groups.....	24
Managing Pre-Defined Policies (PDPs)	25
Context.....	25
Available Tasks	25
Exporting Pre-Defined Policies.....	25
Importing Pre-Defined Policies (for Appliance Users)	26
Importing Pre-Defined Policies (for Standalone Users).....	27
OS-Level Pre-Defined Policies.....	27
OS-Level PDP and Permission Requirements.....	28
Setting Access Control List (ACL) for Minimally-Privileged Users	32
Managing User-Defined Policies (UDPs)	34
Context.....	34
Available Tasks	34
Adding User-Defined Policies (UDPs).....	35

Deleting User-Defined Policies (UDPs)	38
Exporting User-Defined Policies	38
Importing User-Defined Policies	38
About the Penetration Test	39
Managing Pen Tests	39
Assessment Management	45
Adding (or Modifying) Assessments	45
Running Assessments	46
Running an Assessment Immediately	46
Running an Assessment At a Specified Date and Time	46
Running Scheduled Assessments	46
Assessment Notifications	47
Notification OIDs for Target-Level Assessments	48
Notification OIDs for Rule-Level Assessments	49
Assessment Reports	51
Evaluating Assessment Results and Aborting Assessments	52
Assessment Results	52
Deleting Assessments	53
Managing the Privilege Summary	54
DB-Type Distinctions	55
Report Management	57
Managing Pre-Defined Reports	57
Pre-defined Report Section Descriptions	58
Managing User-Defined Reports	62
User-Defined Report Example	64
Deleting User-Defined Reports	67
Getting Fortinet Contact Information	69
Index	71

FortiDB Login

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. From the FortiDB Main page, choose Vulnerability Assessment to access to FortiDB VA.

Login Steps

In the FortiDB VA Login page, take the following steps:

1. Enter your assigned username.
2. Enter your assigned password.
3. Click the **Login** button.

You should then get logged in or receive an error.

NOTE: To go back to the FortiDB Main page, click the Home button. In order to go back to the FortiDB Main page after login to VA, first you need to log out by clicking the logout link at the top bar. That will bring you back to the login page.

4. Using the navigation panel on the left side of the page, navigate to the FortiDB component of interest.
-

Changing Your Password

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

1. Login.
2. Click the **My Account** 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. Click the **OK** button.
-

Target Databases Management

Assessments require that you specify one or more target-database groups. A target-database group must contain at least one target.

Target Icon Definitions

The following table shows icons that indicate target database status and GUI locations.

Icon	Indicates	GUI Location
	A discovered target database that has not been added to the target list.	Auto Discovery Results page
	A discovered target database that has been added to the target list.	Auto Discovery Results page
	That a target database for which the information is incomplete	Targets page
	That a target database for which the information is complete	Targets page

Adding (or Modifying) a Target Connection

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

- To display the **Target** page, click either the **Targets** or **Target Groups** link in the **Target Management** section of the left-side tree-navigation menu. If you choose the **Target Groups** link, you will then have to click on an existing **Name** on the **Target Groups** page in order to be taken to the **Target** page.
- Click the **Add** button. (or, to modify a target, click the **Name** of the target database you would like to change.)
- 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.
 - 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

- If you are connecting to a DB2 target, specify the **Retrieval Method** and this associated information in the **DB2 Options** tab of the **Database Form**:

DB2 Retrieval Method	Comments
SSH	See SSH Connections for Oracle and DB2
db2level command	This method requires that you specify: <ul style="list-style-type: none"> • The output of the <i>db2level</i> command or the name of a text file containing that output. • The output of the <i>get dbm cfg</i> command.

4. (Optionally) you may click 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, click 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 clicking the **Save** button.

Target Privilege Matrix

Here are the privileges that must be granted to the FortiDB user for your target databases.

RDBMS Type	Required Privileges for General VA Use	Required Privileges for Privilege Summary Use	Required Privileges for Pen Test Use
DB2 UDB	<ul style="list-style-type: none"> • CREATE TABLE • SELECT on the following SYSIBM tables: <ul style="list-style-type: none"> • SYSCOLAUTH • SYSDBAUTH • SYSINDEXAUTH • SYSPLANAUTH • SYSSCHEMAAUTH • SYSTABAUTH • SYSTBSPACEAUTH 	<ul style="list-style-type: none"> • SELECT on the following SYSCAT tables: <ul style="list-style-type: none"> • COLAUTH • DBAUTH • INDEXAUTH • PACKAGEAUTH • SCHEMAAUTH • TABAUTH • TBSPACEAUTH • SELECT on the following SYSIBM tables: <ul style="list-style-type: none"> • SYSCOLAUTH • SYSDBAUTH • SYSINDEXAUTH • SYSPLANAUTH • SYSSCHEMAAUTH • SYSTABAUTH • SYSSYSTABLESPACES • SYSTBSPACEAUTH • SYSUSERAUTH 	<ul style="list-style-type: none"> • SELECT on the following SYSCAT tables: <ul style="list-style-type: none"> • COLAUTH • DBAUTH • INDEXAUTH • PACKAGEAUTH • SCHEMAAUTH • TABAUTH • TBSPACEAUTH • SELECT on the following SYSIBM tables: <ul style="list-style-type: none"> • SYSCOLAUTH • SYSDBAUTH • SYSINDEXAUTH • SYSPLANAUTH • SYSSCHEMAAUTH • SYSTABAUTH • SYSTBSPACEAUTH • SYSUSERAUTH

RDBMS Type	Required Privileges for General VA Use	Required Privileges for Privilege Summary Use	Required Privileges for Pen Test Use
<p>MS-SQL 2000</p>	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • MASTER.DBO.SPT_VALUES • MASTER.DBO.SYSALTFILES • MASTER.DBO.SYSDATABASES • MASTER.DBO.SYSLOGINS • MASTER.DBO.SYSXLOGINS • SYSCOLUMNS • SYSMEMBERS • SYSOBJECTS • SYSPROTECTS • SYSUSERS • EXECUTE on: <ul style="list-style-type: none"> • MASTER.DBO.XP_CMDSHELL • MASTER.DBO.XP_INSTANCE_REGENUMVALUES • MASTER.DBO.XP_INSTANCE_REGREAD • MASTER.DBO.XP_LOGCONFIG • MASTER.DBO.XP_LOGINFO • MASTER.DBO.XP_REGENUMVALUES • MASTER.DBO.XP_REGREAD <p>NOTE: The MS-SQL <code>sysadmin</code> role is an additional requirement if you want to use these policies during your</p>	<ul style="list-style-type: none"> • For each individual MS-SQL 2000 database you want to connect to, SELECT on: <ul style="list-style-type: none"> • MASTER.DBO.SYSDATABASES (for MS-SQL 2000 server-level connections) • SYSMEMBERS • SYSOBJECTS • SYSPROTECTS • SYSUSERS 	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • MASTER.DBO.SYSDATABASES (for MS-SQL 2000 server-level connections) • MASTER.DBO.SYSLOGINS • SYS.DATABASE_ROLE_MEMBERS • SYSMEMBERS • SYSOBJECTS • SYSPROTECTS • SYSUSERS (for each individual MS-SQL 2000 database you want to connect to)

RDBMS Type	Required Privileges for General VA Use	Required Privileges for Privilege Summary Use	Required Privileges for Pen Test Use
<p>MS-SQL 2005</p>	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • MASTER.DBO.SPT_VALUE S • MASTER.DBO.SYSALT-FILES • MASTER.DBO.SYSDATA-BASES • MASTER.DBO.SYSLOGINS • MASTER.DBO.SYSXLOGINS • SYS.COLUMNS • SYS.MEMBERS • SYS.OBJECTS • SYS.PROTECTS • SYS.USERS • EXECUTE on: <ul style="list-style-type: none"> • MASTER.DBO.XP_CMDSHELL • MASTER.DBO.XP_INSTANCE_REGENUMVALUES • MASTER.DBO.XP_INSTANCE_REGREAD • MASTER.DBO.XP_LOGINCONFIG • MASTER.DBO.XP_LOGINFO • MASTER.DBO.XP_REGENUMVALUES • MASTER.DBO.XP_REGREAD <p>NOTE: The MS-SQL sysadmin role is an additional requirement if you want to use these</p>	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • MASTER.SYS.DATABASES (for MS-SQL 2005 server-level connections) • For each individual MS-SQL 2005 database you want to connect to, SELECT on: <ul style="list-style-type: none"> • SYS.DATABASE_PERMISSIONS • SYS.DATABASE_PRINCIPALS (for each individual MS-SQL 2005 database you want to connect to) • SYS.DATABASE_ROLE_MEMBERS • SYS.OBJECTS 	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • MASTER.SYS.DATABASES (for MS-SQL 2005 server-level connections) • 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

RDBMS Type	Required Privileges for General VA Use	Required Privileges for Privilege Summary Use	Required Privileges for Pen Test Use
Oracle	<ul style="list-style-type: none"> • CREATE SESSION • SELECT_CATALOG_ROLE • SELECT on: <ul style="list-style-type: none"> • SYS.AUDIT\$ • SYS.LINK\$ • SYS.REGISTRY\$HISTORY (Oracle 10g only) • SYS.USER\$ • SYSTEM.SQLPLUS_PRODUCT_PROFILE 	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • ALL_USERS • DBA_COL_PRIVS • DBA_ROLE_PRIVS • DBA_ROLES • DBA_SYS_PRIVS • DBA_TAB_PRIVS 	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • ALL_USERS • DBA_COL_PRIVS • DBA_ROLE_PRIVS • DBA_ROLES • DBA_SYS_PRIVS • DBA_TAB_PRIVS • SYS.USER\$

RDBMS Type	Required Privileges for General VA Use	Required Privileges for Privilege Summary Use	Required Privileges for Pen Test Use
Sybase	<ul style="list-style-type: none"> • The SSO_ROLE and: <ul style="list-style-type: none"> • If the Sybase Server is using SybSecurity, you need: <ul style="list-style-type: none"> • On the MASTER database, you need to add the FortiDB user to the database, and you need SELECT on: • SYSSRVROLES • SYSLOGIN-ROLES • 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: <ul style="list-style-type: none"> • SYSUSERS • If the Sybase Server is not using SybSecurity, you need SELECT on: <ul style="list-style-type: none"> • SYSSRVROLES • SYSLOGIN-ROLES • SYSSECMECHS • SYSDATABASES (AUDFLAGS column) 	<ul style="list-style-type: none"> • For each individual database you want to connect to, SELECT on: <ul style="list-style-type: none"> • MASTER.DBO.SYSDATABASES (for server-level connections) • SYSOBJECTS • SYSPROTECTS • SYSUSERS 	<ul style="list-style-type: none"> • SELECT on: <ul style="list-style-type: none"> • MASTER.DBO.SYSDATABASES (for server-level connections) • SYSOBJECTS • SYSPROTECTS • SYSUSERS (for each individual database you want to connect to)

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. Click 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	<p>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:</p> <ol style="list-style-type: none"> 1 Click System Configuration in the left-side navigation menu. 2 Click the Assessment tab. 3 Click Browse button in the SSH Key File property and locate your SSH private key file. 4 Click the Save button. <p>NOTE: When User Name is empty, FortiDB will use the name of the user that started FortiDB.</p>
Explicit Key Pair (Standalone Only)	<p>Enter:</p> <ul style="list-style-type: none"> • 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 <code>./ssh</code> directory under the directory shown in this field and copy the private key in <code>./ssh</code> directory you created. • (Optionally) a Pass Phrase <p>FortiDB will attempt to use the private key (and, if specified, pass phrase) located in Key Path location at run time.</p>

4. Click 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 <i>authorized_keys</i> file located in the <i>.ssh</i> 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 <i>id_dsa</i> or <i>id_rsa</i> private keys and copy them to the <i>.ssh</i> directory under user's home directory on the SSH client machine. In a Windows environment, depending on Operating systems, the private key should reside in <i>.ssh</i> directory under user's home directories, such as <i>C:\Documents and Settings\All Users</i> . In order to place the private key, take the following steps: <ol style="list-style-type: none"> 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 <i>.ssh</i> directory under the directory shown in the Key Path field. 4 Copy the private key to <i>.ssh</i> 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 <i>db2inst3</i> user and you use the <i>bash</i> shell, add this to your <i>.bashrc</i> : <pre>if [-f /home/db2inst3/sqllib/db2profile]; then . /home/db2inst3/sqllib/db2profile fi</pre>
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 Only)

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

1. Check the **Enable OSVA** check box.
 2. Select **Solaris** for the operating system from the pull-down list.
 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. Click the Save button.
-


Deleting Target Database Connections

This topic describes how to delete target-database connections.

1. Navigate to the **Targets** page.
 2. Check the checkbox(es) corresponding to the **Name(s)** of the target-database connection(s) you want to delete.
 3. Click the **Delete** button.
-

Adding Target Groups

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

1. To add a new target group, click **Target Groups** of **Target Management** section.
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, enter an **Attribute** on which you would like to filter, an **Operator** that associates the **Column** with a **Value**, and a **Value** that the **Column** must match.
 - c. In order to cancel a target-database grouping operation, click the  icon.
 - d. You can add or subtract filtering-criteria rows by clicking 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 1: Filtering Criteria Examples

Attribute	Operator	Value	Return Possibilities
Location	Contains	nd	all databases in London
Database Type	Equals	DB2	all DB2 databases

4. Click **Apply** to test your filtering criteria.
5. Click the Save icon 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. Navigate to the **Target Groups** page.
 2. Check the checkbox(es) corresponding to the **Name(s)** of the target-database group(s) you want to delete.
 3. Click the **Delete** button.
-

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. 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. Navigate to the **Targets** page by clicking on the **Targets** in the **Target Management** section of the left-side tree-navigation menu.
3. Click 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 click the **Browse** button and select the XML file you want to import.
5. Click 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. Click the **Cancel** button in order to go back to the **Targets** page.

Exporting Target Database Data

This topic describes how to export target-database information.

NOTE: The checkboxes next to the individual targets on the **Targets** page have no effect when exporting. No matter how many checkboxes you check, all items will be exported.

1. Click on the **Targets** link in the **Target Management** section of the left-side tree-navigation menu.
2. In the **View** dropdown list, select a group you want to export.
3. Click the **Export** button.

A dialog box will help you to choose a directory in which you can save the file to your disk.

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. To display the **Auto Discovery** page, click on the **Auto Discovery** link in the **Target Management** section of the left-side tree-navigation 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. Click 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, check the checkbox on the left of the IP address or range and click the **Remove** button

4. Specify database types to attempt discovery for and their respective port ranges to discover from the list.
 - a Check or uncheck 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 click 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.
No databases found	There was no database of the specified IP address found.
Idle	Has one of these meanings: <ul style="list-style-type: none"> • User cancelled the Auto Discovery process before completion. • This is the status after <code>Running...</code> • This is the status after <code>No databases found</code>

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

- 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**.

- Run Auto Discovery.
- Check the checkbox(es) next to the targets you want to add to your list of target databases.
- Click the **Add to Targets** button at the bottom.
- Go to the **Targets** page where you should see that the auto-discovered targets databases have been added to the **Targets** list.

Policy Management

This section explains about Policy Management.

About Policies

Policies are best-practice business rules that are applied during assessments.

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).

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

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.

NOTE: The checkboxes next to the individual policies on the **Policies** page have no effect when exporting. No matter how many checkboxes you check, all items will be exported.

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.

Column and Group Information for Policies

This topic gives column-specific information for Pre-Defined Policies and User-Defined Policies.

Table 1: Column Information

Column	Description	Comments
Status	<ul style="list-style-type: none"> • Enabled () • Disabled () • New and Enabled () • New and Disabled () • Modified and Enabled () • Modified and Disabled () 	Status is shown by the particular icon. Click the header to sort.
Name	Policy names	If you click the Policy name, the PDP details information will display. Click the header to sort.
DB Type	Oracle, Sybase, DB2 or SQL Server	Click the header to sort.
Severity	Informational, Cautionary, Minor, Major, Critical	You can specify Severity. Click the header to sort.
Classification	Unclassified, Configuration, Password, Privilege, Database server, Host System	You can specify Classification. Click the header to sort.


Adding Policy Groups

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

1. In order to display the **Policy Groups** page, click **Policy Groups** link in the **Policy Management** section of the left-side tree-navigation menu.
2. Click 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, click the  icon.

Here are some examples of filtering criteria:

Table 2: 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, click the **Apply** button.
5. To save the group you created, click the  icon.

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

Deleting Policy Groups

This topic describes how to delete a policy group.

1. Navigate to the **Policy Groups** page.
2. Check the checkbox(es) corresponding to the policy group(s) you want to delete.
3. Click the **Delete** button.

Managing Pre-Defined Policies (PDPs)


This topic describes the tasks involved with managing pre-defined policies.

Context

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 policies or updates to existing policies.

Available Tasks

From the **Policies** page, you can do the following tasks:

- 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 selected policies as an XML file.

Exporting Pre-Defined Policies

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

1. In order to display the **Policies** page, click on the **Policies** link in the **Policy Management** section of the left-side tree- navigation menu.
2. Click the **Pre-Defined Policies** tab.
3. Click the **Export** button.
4. Save the XML file.

NOTE: The default location for saving your XML files is the browser's download-file directory.

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. In order to display the **Policies** page, click on either the **Policies** or **Policies Groups** link in the **Policy Management** section of the left-side tree-navigation menu.

NOTE: If you choose the **Policies Groups** link, you will then have to click on an existing policy **Name** to be taken to the **Policies** page.

2. Click the **Import** button.

The **Pre-Defined Policy Update** page displays.

3. Check or uncheck 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. Check or uncheck 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 check this checkbox.

5. Click 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** button. After selecting the xml file to upload, click 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. In order to display the **Policies** page, click on either the **Policies** or **Policies Groups** link in the **Policy Management** section of the left-side tree-navigation menu.

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

2. Click the **Import** button.
The **Pre-Defined Policy Update** page displays.
 3. Enter the path to the XML file you downloaded, or click 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. Check or uncheck the **Identify new and modified rules with icons** checkbox.
 - If you check this, you can identify new and modified rules with icons.
 - If you uncheck this, you cannot identify new and modified rules with icons.
 6. Click 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 \(Solaris Only\)](#)

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: <ul style="list-style-type: none"> opatch version applied critical patch numbers 	Oracle 9i, 10g or 11g: <ul style="list-style-type: none"> The SSH user needs execute permission on opatch The SSH user's PATH variable should include the location of opatch Oracle 10g and 11g: <ul style="list-style-type: none"> The SSH user needs read, write, and execute permissions on opatch The SSH user needs read, write, and execute permissions on \$ORACLE_HOME/cfgtool-ogs/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

<p>OSVA ORCL 01.06 Oracle Excessive Directory & File Permissions Check</p>	<p>Alerts if other permissions, on the OracleHome directory (and its contents) specified on the Create/ModifyDatabase Connection screen, include both read and write (and not execute)</p>	<p>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.</p>
<p>OSVA ORCL 01.07 Oracle Correct Directory/File Owner & Group Check</p>	<p>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 permissions. Exempt from this check are:</p> <ul style="list-style-type: none"> • \$ORACLE_HOME/bin/oracle • \$ORACLE_HOME/bin/oradism • \$ORACLE_HOME/bin/dbsnmp 	<p>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.</p>
<p>OSVA ORCL 01.08 Oracle setuid/setgid File Check</p>	<p>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:</p> <ul style="list-style-type: none"> • \$ORACLE_HOME/bin/oracle • \$ORACLE_HOME/bin/oradism • \$ORACLE_HOME/bin/dbsnmp 	<p>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.</p>

OSVA ORCL 01.09 Oracle Database- Configuration-Change Check	<p>This policy checks if these database configuration files change between the previous and current assessments:</p> <ul style="list-style-type: none"> • init.ora • spfle.ora 	<ul style="list-style-type: none"> • 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	<p>This policy check if network configuration files changed between the previous and current assessments</p> <ul style="list-style-type: none"> • listener.ora • tnsnames.ora • sqlnet.ora 	<ul style="list-style-type: none"> • 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	<p>Returns OS name and version</p>	<ul style="list-style-type: none"> • 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- ProcedureProcesses Running Check	<p>Alert if external-procedure process is running on target server.</p>	<p>The SSH user needs execute permission for ps and grep</p>
OSVA ORCL 01.13 Oracle EXTPROC	<p>Alerts if any EXTPROC settings are listed in listener.ora. For example:</p> <pre>(SID_NAME = PLSExtProc)</pre>	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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: <pre>SQLNET.ENCRYPTI ON_SERVER = Requested</pre>	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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: <pre>PASSWORDS_LISTENER = F56401ADBA6810D S</pre>	<ul style="list-style-type: none"> • 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 or 11g 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/patch/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 9,10g or 11g 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.

Managing User-Defined Policies (UDPs)


This topic describes the tasks involved with managing user-defined policies.

Context

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 policies or updates to existing policies.

Available Tasks

From the **Policies** page, you can do the following tasks:

- 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 selected policies as an XML file.

Adding User-Defined Policies (UDPs)

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

1. Navigate to the **Policies** page by clicking on the **Policies** link in the **Policy Management** section of the left-side tree-navigation menu.
2. Click the **User-Defined Policies** tab.
3. Click 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.

<p>Result Column Name(s)</p>	<p>Entries in this field are the column names referred to in the SQL query field. Multiple entries are delimited by semicolons.</p> <p>The names can either be actual column names in your query, like <code>empno</code> in <code>'SELECT empno FROM scott.emp'</code> or aliases like <code>enumber</code> in <code>'SELECT empno AS " enumber"¹FROM scott.emp'</code></p> <p>You can use the <code>'*'</code> 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 <code>'SELECT * FROM scott.emp'</code> against an Oracle target database, you must enter <code>"empno;ename;job;mgr;hiredate;sal;comm;deptno"</code> in this field in order to get a report on all columns in <code>scott.emp</code></p> <p>NOTE: Do not put spaces before or after the semicolons unless your aliased column names also have leading or trailing spaces, respectively.</p>
<p>Result Column Label(s)</p>	<p>Entries in this field are the column names that you would like to see in your reports. Multiple entries are delimited by semicolons.</p> <p>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.</p>
<p>Keywords</p>	<p>Entries in this field can be used when using a filter to create policy groups.</p>

1. Leading or trailing spaces in the alias expression must also be specified in this field for the column's values to appear in your report. For example, assume there are two leading spaces in `" enumber"`; both spaces must be included in your **Result Column Name(s)*** entry.

5. Click the **Save** button.

Here is an Oracle example, which assumes you have access to the `SCOTT` schema:¹

 - a) 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
- b) Click **Save** in order to save myOracleUDP1.
 - c) Create a policy group, myUDPGroup, containing the new UDP
 - d) Create an assessment that runs against an Oracle target-database group and which uses myUDPGroup.
 - e) 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:

- a) 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
- b) Click **Save** in order to save myOracleUDP1.
- c) Create a policy group, myUDPGroup, containing the new UDP
- d) Create an assessment that runs against an Oracle target-database group and which uses myUDPGroup.
- e) 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**

1. This schema used to automatically ship with Oracle; some of the newer versions, beyond 9.x, do NOT ship with it.

Deleting User-Defined Policies (UDPs)

This topic describes how to delete User-Defined Policies.

1. Navigate to the **Policies** page.
 2. Click the **User-Defined Policies** tab.
 3. Check the checkbox(es) corresponding to the user-defined policy you want to delete.
 4. Click the **Delete** button.
-

Exporting User-Defined Policies

This topic describes how to export User-Defined Policies.

1. In order to display the **Policies** page, click on the **Policies** link in the **Policy Management** section of the left-side tree-navigation menu.
 2. Click the **User-Defined Policies** tab.
 3. Click the **Export** button.
 4. Save the XML file.
-

Importing User-Defined Policies

This topic describes how to import User-Defined Policies.

1. Click on the **Policies** link in the **Policy Management** section of the left-side tree-navigation menu.
2. Click the **User-Defined Policies** tab.
3. Click the **Import** button.
4. Enter the path to the XML file you want to import, or click the **Browse** button and select the XML file you want to import.

5. Check or uncheck the **Deactivate 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.
 6. Check or uncheck the **Identify new and modified rules with icons** checkbox.
 - If you check this, you can identify new and modified rules with icons.
 - If you uncheck this, you cannot identify new and modified rules with icons.
 7. Click the **Import** 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 3: Pen Test-related System Properties

Property	Purpose	Tab	Possible Values and Default Values
Enable Pen Test	When set to <code>true</code> , the Pen Test capability is enabled. When set to <code>false</code> , which is the default, the Pen Test capability is disabled.	Assessment	<code>true</code> or <code>false</code> . The default value is <code>false</code> .

Property	Purpose	Tab	Possible Values and Default Values
Enable Pen Test For All Users in Database (Standalone only)	<p>When set to <code>false</code>, FortiDB uses the user names in <code><dbtype>user.txt</code>, where <code>dbtype</code> represents the target-database type and is one of these strings:</p> <ul style="list-style-type: none"> • ora for Oracle • sql for MS-SQL • db2 for DB2 UDB • syb for Sybase <p>When set to <code>true</code>, FortiDB ignores the user names in <code><dbtype>user.txt</code>.</p>	Assessment	<p><code>true</code> or <code>false</code>. The default value is <code>true</code>.</p>

Property	Purpose	Tab	Possible Values and Default Values
Pen Test Method	<p>The Login method actually logs into 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.</p> <p>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.</p>	Assessment	<ul style="list-style-type: none"> • 1=Login method • 2=Hash-based method • 3=Hybrid <p>The default value is <code>Hybrid</code>. (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.)</p>

Property	Purpose	Tab	Possible Values and Default Values
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 click the Save button to complete your selection.	Assessment	“Built-in Dictionary” indicates that the defaultdictionary is being used. “User Dictionary” indicates that you have uploaded your own dictionary file. The filename of thedictionaryyou upload will not appear here. NOTE: When you restore the default dictionary by checking the checkbox, and clicking 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.

- 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.

Policy Name	File Used	Evaluate Content
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 pairing 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 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.

Filename	Content
<i>dictionary.txt</i>	<p>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.</p> <p>NOTE: When FortiDB executes the Pen Test Dictionary policy, the domain name automatically added in the password list.</p>

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. Click 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, click the **Save** button on the Policy details page.
 - Severity
 - Classification
 - Keywords
 - Status
10. Go 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, click the **Pen Test Policy Group** within the **Available Policy Groups** list and then click 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.

Assessment Management

This section explains about 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. Navigate to the **Assessments** page by clicking on the **Assessments** link in the **Assessment Management** section on the left-side tree-navigation menu.
2. Click the **Add** button. (or, to modify a user, click 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 clicking on the  button.
In order to remove a target-database group from **Assigned Target Groups** list on the right, click 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 clicking on the right-arrow button. (In order to remove a policy

- group from the **Assigned Policy Groups** list , click 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. Navigate to the **Assessments** page.
 2. Select the assessment of interest.
 3. Click 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:
In the **Starts at** field group, specify a starting date directly, use the default, or alternatively, click on the calendar icon, and then select a date.
 2. Check 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. Click 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:
In the **Starts at** field group, specify a starting date directly, use the default, or alternatively, click on 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 clicking on the calendar icon.
 3. Check 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. Click 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, check 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. Check 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 clicking 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 click the left-arrow button.

NOTE: In order to see the details associated with any receiver, click on 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

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 1: 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 2: 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. Navigate to the **Reports** tab of the **Assessment** page
2. 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, click 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.
3. 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)**.
4. Click 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. Click on an assessment's **Start Time** (in the top table) in order to view the target databases involved.
2. To see target-specific results, click 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 click 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 click 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 3: 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: <ul style="list-style-type: none"> • 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

Column Name	Description
Total	The total number of policies incorporated by the assessment

Status Icons

Assessments can be in any one of the following states:

Table 4: Assessment Status Icons

Status-Column Icon	Description
	Running
	Idle
	Queued
	Completed
	Error
	Aborted

Deleting Assessments

This topic describes how to delete previously run assessments.

1. Navigate to the **Assessments** page.
2. Check the checkbox(es) corresponding to the assessment(s) you want to delete.
3. Click the **Delete** button.

Managing the Privilege Summary

This topic describes how to display and export the Privilege Summary.

In order to view the Privilege Summary, you must have the Assessment 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, click on the **Privilege Summary** link in the **Assessment Management** section of the left-side tree-navigation menu.
2. From the **Target Group** dropdown list, choose the target-database group which contains the target database for which you would like to see a Privilege Summary.
3. From the **Target** dropdown list, choose the specific target database for which you would like to see a Privilege Summary.

NOTE: MS-SQL 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, choose the name of the specific database for which you would like to see a Privilege Summary.
5. Click on 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.
 - 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** link below 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:

- Users is a distinction used for all RDBMS types.
- Roles is a distinction used for all RDBMS types except DB2 which uses groups instead. (That is, for DB2 target databases, the Roles tab is really a Groups tab.)

Filtering Differences

After clicking on 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 all target-database types, 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
- 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

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.

Report Management

This section explains about Report Management.

Managing Pre-Defined Reports

This topic describes how to manage Pre-Defined Reports.

You should run an assessment before running reports.

FortiDB ships with several Pre-defined Reports. These are the operations that you can perform with each. In general, you can perform the following operations, an example of which is below.

- Specify a specific target database and assessment on which to report
 - Preview a report
 - Make necessary changes
 - Run your report
 - Export your report into one or more of the available output formats.
1. Starting at the **Pre-Defined Reports** page, click on the report type of interest in the **Name** column . For this example, assume that you would like an assessment-summary report. So click on **Summary Report**
 2. In the **Report Parameters** section of the **Vulnerability Assessments Summary Reports** page, select the **Assessment Name**, **Assessment Time**, and **Targets** that correspond to the assessment in which you are interested. You should see the target-database details show up in the **Target Information** tab in the **Report Details** section of the page.
 3. Click on the **Preview Report** tab in the **Report Parameters** section of the page in order to see a screen version of your report.
 4. If you want a file-based report, choose an output-format type from the **Export as** dropdown and then click 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:

- Comma-delimited (.csv)
- Excel (.xls)
- PDF (.pdf)
- Tab-delimited (.txt)

NOTE: Some output-format types may not available for all report types.

Pre-defined Report Section Descriptions

Here are the Pre-Defined Report template descriptions.

Score Report

The pre-defined Score Report template provides you a way to see assessment results in a graphical form.

Table 1: Score Report Sections

Section	Description
Severity	Bar chart by policy-severity type for all assessment results
Category	Bar chart by policy-classification type for all assessment results
Severity/Category	Bubble chart that plots both the severity and classification types for all assessment results

Summary Report

The pre-defined Summary Report template provides a summary of the number and type of all policies used by an assessment.

Table 2: Summary Report Sections

Section	Description
Severity	Summary by policy-severity type for all assessment results
Classification	Summary by policy-classification type
Critical Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Critical.' (Click on the plus (+) sign to expand the list.)
Major Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Major.' (Click on the plus (+) sign to expand the list.)

Minor Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Minor.' (Click on the plus (+) sign to expand the list.)
Cautionary Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Cautionary.' (Click on the plus (+) sign to expand the list.)
Informational Vulnerabilities	Policy names, states, and classification types for all policies assigned a Severity of 'Informational.' (Click on 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 3: Summary Failed Report Sections

Section	Description
Severity	Summary by policy-severity type for just failed assessment results
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.' (Click on the plus (+) sign to expand the list.)
Major Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of 'Major.' (Click on the plus (+) sign to expand the list.)
Minor Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of 'Minor.' (Click on the plus (+) sign to expand the list.)

Cautionary Vulnerabilities	Policy names, states, and classification types for failed policies assigned a Severity of 'Cautionary.' (Click on 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 4: Detailed Report Sections

Section	Description
Severity	Details by policy-severity type of all assessment results
Classification	Details by policy-classification type
Critical Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Critical.' (Click on the plus (+) sign to expand the list.)
Major Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Major.' (Click on the plus (+) sign to expand the list.)
Minor Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Minor.' (Click on the plus (+) sign to expand the list.)
Cautionary Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Cautionary.' (Click on the plus (+) sign to expand the list.)
Informational Vulnerabilities	Detailed policy description and results for all policies assigned a Severity of 'Informational.' (Click on 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 5: Detailed Failed Report Sections

Section	Description
Severity	Details by policy-severity type for just failed assessment results.
Classification	Details by policy-classification type for just failed assessment results.
Critical Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Critical.' (Click on the plus (+) sign to expand the list.)
Major Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Major.' (Click on the plus (+) sign to expand the list.)
Minor Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Minor.' (Click on the plus (+) sign to expand the list.)
Cautionary Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Cautionary.' (Click on the plus (+) sign to expand the list.)
Informational Vulnerabilities	Detailed policy description and results for failed policies assigned a Severity of 'Informational.' (Click on the plus (+) sign to expand the list.)

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 6: 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

Global Report

The pre-defined Global 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 7: Global Report Sections

Section	Description
Risk Exposure (by Severity)	Pie chart by policy-severity type for all assessed databases
Risk Exposure (by Classification)	Pie chart by policy-classification type for all assessed databases
Vulnerability by RDBMS Type	Bubble chart that plots both the severity and classification types for all assessed databases by RDBMS type

Managing 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.

You should run an assessment 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, such as PDF
- Deleting reports

In order to create your own report:





1. Navigate to the **User-defined Reports** page by clicking on the **User-defined Reports** link within the **Report Management** section of the left-side tree-navigation menu.

2. Click on the **Add** button.

NOTE: If you are modifying an existing User-Defined report, click on 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 **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 click the **Right** arrow button in order 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 click the **Left** arrow button.)

NOTE: Your report must contain at least one display column. So , once you have selected at least one column for your report, you may click the **Export** button to see a report sample.

NOTE: By clicking 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. Optionally, in the **Group Data By** drop downs on the **Grouping** tab of the **User-Defined Report** page, enter the column name(s) by which you want to group report results. Optionally, specify a sort order in the **Order** drop-down(s). Optionally, specify a **Day**, **Week**, **Month**, **Quarter**, or **Year** value by which to group date-related report results in the **Group date values by** drop-down.

NOTE: 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. Optionally, in the **Filtering** tab of the **User-Defined Report** page, enter the criteria by which you would like to filter or limit the data that shows up in your report.

NOTE: In order to help you preview your report, you can optionally limit the number of rows you would like to display. In the **Limit Rows** section of the **Filtering** tab, select the **Enter number** radio button and then specify, as your row limit, any positive number less than 1000.

7. Click on the **Save** button in order to save your report.
8. Test your report by:
 - a Specifying an output format in the **Export as** drop down list.
 - b 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.

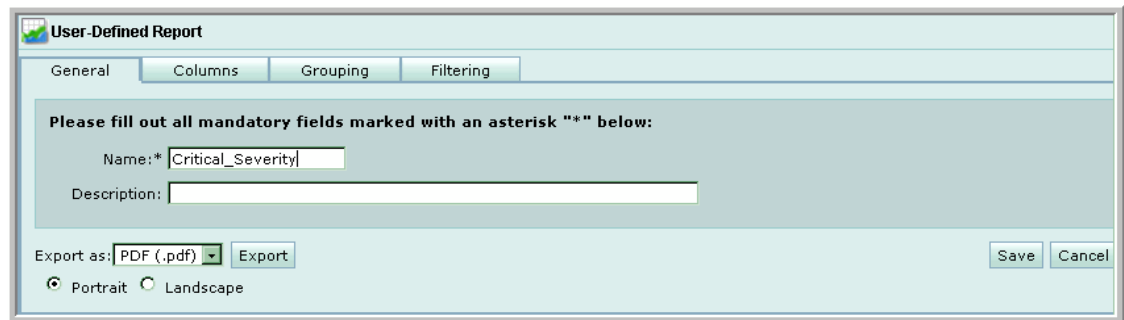
- c Click the **Export** button.
 - d View the result, make setting changes if necessary, and regenerate the report. Once you are satisfied with the result, click the **Save** button.
-

User-Defined Report Example

Here is an example of a User-defined Report setup and results.

Provide a Report Name

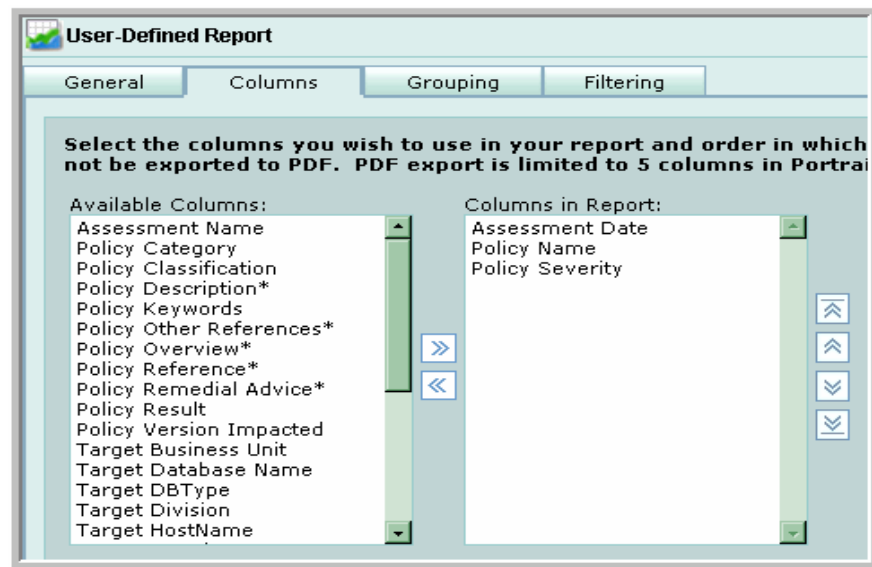
Give your report a **Name** and, optionally, a **Description**.



The screenshot shows a dialog box titled "User-Defined Report" with four tabs: "General", "Columns", "Grouping", and "Filtering". The "General" tab is active. Below the tabs, there is a message: "Please fill out all mandatory fields marked with an asterisk "*" below:". There are two input fields: "Name:*" with the text "Critical_Severity" entered, and "Description:" which is empty. At the bottom left, there is a dropdown menu for "Export as:" set to "PDF (.pdf)", an "Export" button, and two radio buttons for "Portrait" (selected) and "Landscape". At the bottom right, there are "Save" and "Cancel" buttons.

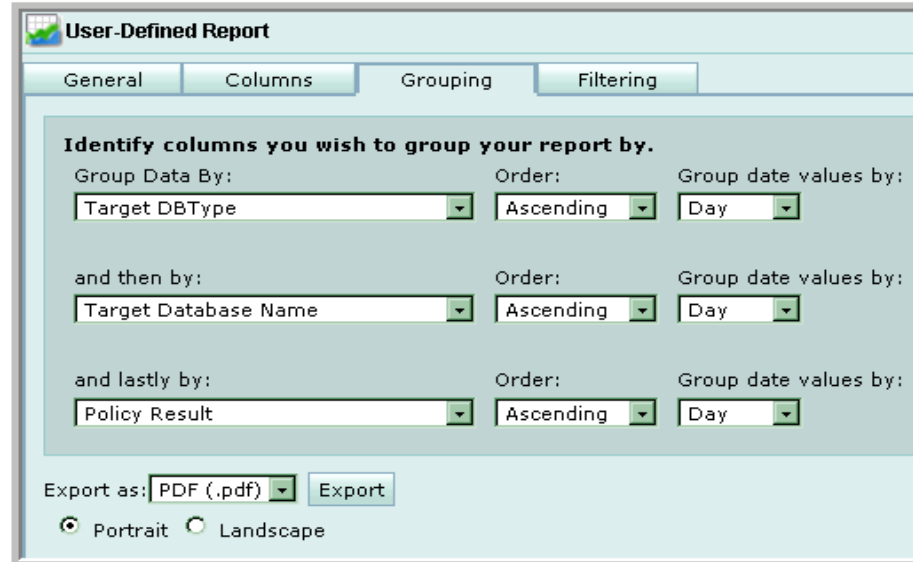
Select Display Columns

If you select these display columns:



Select Group-by Columns

And group by these columns:



PDF Result Before Filtering

You can expect a PDF result like:

2008-07-10 14:06:06.687	DVA IBM DB2 UDB 02.19 Query Complier DoS	MINOR
2008-07-10 14:06:06.687	DVA IBM DB2 UDB 02.16 Remote Command Privelege Escalation	MAJOR
2008-07-10 14:06:06.687	DVA IBM DB2 UDB 05.02 Remote Command Server Privelege Upgrade	CRITICAL
2008-07-10 14:06:06.687	DVA IBM DB2 UDB 02.08 db2dart Buffer Overflow	CRITICAL
2008-07-10 14:06:06.687	DVA IBM DB2 UDB 02.06 Control Center Buffer Overflow	CRITICAL
MSSQL Group-by Columns:		
master	•Target DBType	
FAIL	•Target Database Name	
	•Policy Result	
2008-07-10 14:06:06.687	DVA MSSQL 05.46 Check if sa account has been disabled	MAJOR
2008-07-10 14:06:06.687	DVA MSSQL 05.26 Database Owners Report	MAJOR
2008-07-10 14:06:06.687	DVA MSSQL 01.09 Latest MSSQL Patch not Applied	CRITICAL
2008-07-10 14:06:06.687	DVA MSSQL 05.45 CLR (Common Language Runtime) access level is not SAFE_ACCESS mode.	MAJOR
2008-07-10 14:06:06.687	DVA MSSQL 01.18 Privileges on	

Select Filtering Criteria

You can create a filter to restrict the result set. In this example, we are restricting it to just policies whose Severity is Critical.

The screenshot shows the 'Filtering' tab of the 'User-Defined Report' configuration. The main area contains a filter rule with the following fields:

- Column: Policy Severity
- Operator: Equals
- Value: Critical

Below the filter rule, there is a section titled 'Specify the number of rows to be included in the report.' with two radio button options: 'All' (selected) and 'Enter Number: 100'.

PDF Result After Filtering

You can expect a filtered PDF result like:

2008-07-10 14:06:06.687	DVA IBM DB2 UDB 02.08 db2dart Buffer Overflow	CRITICAL
2008-07-10 14:06:06.687	DVA IBM DB2 UDB 02.06 Control Center Buffer Overflow	CRITICAL
MSSQL		
master		
FAIL		
2008-07-10 14:06:06.687	DVA MSSQL 01.09 Latest MSSQL Patch not Applied	CRITICAL
2008-07-10 14:06:06.687	DVA MSSQL 01.18 Privileges on sp_runwebtask and sp_MSSetServerProperties Procedures	CRITICAL
2008-07-10 14:06:06.687	DVA MSSQL 01.01 password field empty	CRITICAL
2008-07-10 14:06:06.687	DVA MSSQL 01.26 Excessive rights granted to Admin group users	CRITICAL
2008-07-10 14:06:06.687	DVA MSSQL 01.27 Excessive rights	CRITICAL

Only CRITICAL policies show up in results now

Deleting User-Defined Reports

This topic describes how to delete User-Defined reports.

1. Navigate to the **User-defined Reports** page the **Report Management** section of the left-side tree navigator.
2. Check the checkbox(es) corresponding to the **Name(s)** of the report templates you want to delete.
3. Click the **Delete** button.

Getting Fortinet Contact Information

This topic describes how you can get Fortinet contact information.

In order to get contact information for Fortinet:

1. Login.
2. Click the **About Fortinet** link at the top of any page.
3. Then click the **Contact Information** link.

You should be taken to the IPLocks website for the contact information.

NOTE: IPLocks is the previous owner of what is now the FortiDB product.

Index

A

- Access Control List 32
- ACL 32
- Assessment Notifications 47
- Assessment Reports 51
- Assessment Results 52
- Assessments
 - adding 45
 - deleting 53
 - running 46
- Auto Discovery 18
 - adding targets 20
 - running 19

C

- Column Descriptions 52
- Contact Information 69

D

- Detailed Failed Report 61
- Detailed Report 60

G

- Global Report 62

I

- Icon Definitions 5

L

- Login Steps 3

O

- OID 48
- OS-Level PDP 15
 - permission requirement 28

P

- Password
 - changing 3
- PDP 25
- Penetration Test 39
- Policies 21
 - column and group 22
 - exporting and importing 22

- Policy Groups 21
 - adding 23
 - deleting 24
- Policy Types 21
- Policy Updates 21
- Pre-Defined Policies 25
 - exporting 25
 - importing 26
 - OS level 27
- Pre-defined Report
 - section descriptions 58
- Privilege Matrix 6
- Privilege Summary 54

S

- Score Report 58
- SSH
 - environment 13
 - using 12
- SSH Connections 12
- Summary Failed Report 59
- Summary Report 58

T

- Target Connection
 - adding 5
 - modifying 5
- Target Database Connections
 - deleting 15
- Target Database Data
 - exporting 18
 - importing 17
- Target Groups
 - deleting 17
- Target-Database Groups 5

U

- UDP 34
- User-Defined Policies 34
 - adding 35
 - deleting 38
 - exporting 38
 - importing 38
- User-Defined Report
 - example 64
- User-Defined Reports 62
 - deleting 67

