



Administration Guide

FortiDB
Version 3.2

FORTINET®

www.fortinet.com

FortiDB Administrator Guide
Version 3.2
December 19, 2008
15-32000-78778-20081219

© 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

System Information	3
Setting the System Time	3
Changing the FortiDB Host Name	4
Changing the Firmware Version	5
System Resources	5
Network Configuration	6
Interface	6
Changing the Interface Settings	7
DNS	8
Changing the DNS settings	8
Routing	8
Adding Route settings	9
Deleting Route Settings.....	9
Changing Route Settings	9
System Configuration	11
System Properties List	11
User Management	15
Adding (or Modifying) a User.....	15
Role-Dependent Permissions.....	16
Permissions by Role.....	16
User Management Icon Descriptions	18
Deleting Users.....	19
About FortiDB Archiving and Restoring	19
About Archiving	19
Effect of Archiving	20
An Archiving Strategy	20
Archiving Immediately	20
Scheduling an Archive.....	21
Using FortiDB Restore	22
Managing the Entitlement Report	22
Entitlement Report Distinctions	22
Assignable Roles.....	23
Entitlement Report Icons	23
Index	25

System Information

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

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

Setting the System Time

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

1. Navigate to the **System Information** page under **Appliance**.
2. Click the **Change** link to change the system Time.
The **Time Settings** page displays.

3. You have options to set the time as follows.

System Time	The current FortiDB system date and time. Click the Refresh button to update the display of the current FortiDB system date and time.
Time Zone	Select the FortiDB unit's time zone from the pull-down list. NOTE: Changing Time Zone requires rebooting the system to take the change into effect.
Set Time	Select to set the FortiDB system date and time to the values you set in the Year, Month, Day, Hour, Minute and Second fields.
Synchronize with NTP Server	Select to use an NTP server to automatically set the system date and time. You must specify the server and synchronization interval. Alternatively, select Set Time. <ul style="list-style-type: none"> • Server: Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see http://www.ntp.org. • Sync Interval: Specify how often the FortiDB unit should synchronize its time with the NTP server. For example, a setting of 1440 minutes causes the FortiDB unit to synchronize its time once a day.

4. Click **OK**.

Changing the FortiDB Host Name

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

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

Changing the Firmware Version

This topic describes how to change the FortiDB firmware version. When changing the firmware version, the unit will either keep or reset its configuration.

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

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

System Resources

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

CPU Usage

The current status of CPU usage. This field displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

Memory Usage

The current status of memory usage. This field displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

Hard Disk Usage

The current status of hard disk usage. This field displays the amount of hard disk space used.

Network Configuration

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

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

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

Interface

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

Interface

The name of the network interface on the FortiDB unit.

Device IP/Netmask



The IP address and network mask configured for the interface.

Access

A list of the administrative access methods available on the interface.

Status

The status of the network interface.

- A green arrow  indicates the interface is up. Select Modify icon to disable the port.
- A red arrow  indicates the interface is down. Select Modify icon to enable the port.

Modify

Select **Modify** to change the interface settings.

Changing the Interface Settings

This topic describes how to change the FortiDB interface settings.

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

Enable checkbox	You can change the interface status by using this checkbox. To disable the port, uncheck the checkbox. To enable the port, check the checkbox.
Interface Name	The interface name cannot be changed.
Device IP/Netmask	Enter an IP address and network mask. For example, 192.168.10.3 / 255.255.255.0
Access	<p>Select which methods of administrative access should be available on this interface.</p> <ul style="list-style-type: none"> • HTTP allows HTTP connections to the FortiDB. HTTP connections are not secure and can be intercepted by a third party. • HTTPS allows secure HTTPS connections to the FortiDB. • PING allows response to ICMP pings, which are useful for testing connectivity. • SSH allows SSH connections to the FortiDB CLI. • TELNET allows Telnet connections to the FortiDB CLI. Telnet connections are not secure, and can be intercepted by a third party.

5. Click the **Save** button.

DNS

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

Changing the DNS settings

This topic describes how to configure DNS settings.



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

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

4. Click the **Apply** button.

Routing

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

Destination IP/Netmask	The destination IP address and netmask for packets that FortiDB sends to.
Gateway	The IP address of the router where FortiDB forwards packets.
Interface	The names of the FortiDB interfaces through which intercepted packets are received and sent.
Modify	Select to change the route configuration settings or delete them. For changing route settings, click  . For deleting the route settings, click  .

Adding Route settings

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


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

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

5. Click the **Save** button.

Deleting Route Settings

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

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

Changing Route Settings

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

1. Navigate to **Network** under **Appliance**.
2. Click the **Routing** tab.
3. In the row corresponding to the routes you want to change, select the modify icon to modify the route settings.

4. Enter the following options.

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

5. Click the **Save** button.
-

System Configuration

You can configure FortiDB by setting certain FortiDB system properties via the following steps.

- 1) Login as FortiDB user with the System Administrator role.
- 2) Navigate to the **System Configuration** page by clicking on the **System Configuration** link within the **Administration** section of the left-side tree-navigation menu.
- 3) Change the value on the properties of interest and click the **Save** button.

Notes:

- The **All** tab shows the properties in a read-only manner; you must click on one of the other tabs in order to add or change property values.
- No entry in the **Value** column implies an undefined string-type property. A minus 1 (-1) in the **Value** column implies an undefined integer-type property.
- You can convert property values back to their original default values via the **Restore Default(s)** button. (Before clicking this button, you must check the checkbox next to each property whose value you want reverted to the default value.) After you click the **Restore Default(s)** button, you must click the **Save** button to complete the restoration.
- The **Save** and **Restore Default(s)** buttons apply only to the value(s) on the tab which is currently viewed.

System Properties List

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

Property	Purpose	Tab	Possible Values and Default Values
Enable LocalhostAuto Discovery	Enables Auto Discovery to be performed on the machine containing the FortiDB application.	Assessment	true or false. The default value is false.

Property	Purpose	Tab	Possible Values and Default Values
Number of Concurrent Assessments	Total number of assessments which can run simultaneously. The optimum value of this parameter depends on your environment but tuning this parameter will affect assessment performance and CPU usage by FortiDB. NOTE: Assuming at least one target database per assessment, the <code>numberOfConcurrentScans</code> can never exceed <code>numberOfConcurrentTargetScans</code> .	Assessment	The default value is 5.
Number of Concurrent Target Assessments	Total number of target-databases that can be assessed simultaneously during the <code>numberOfConcurrentScans</code> assessments. The optimum value of <code>numberOfConcurrentTargetScans</code> depends on your environment but tuning this parameter will affect assessment performance and CPU usage by FortiDB. NOTE: Assuming at least one target database per assessment, the <code>numberOfConcurrentScans</code> can never exceed <code>numberOfConcurrentTargetScans</code> .	Assessment	The default value is 20.
SSH Key File (Appliance only)	The file that contains the private key used for all SSH connections. Oracle OSVA and DB2 only. The Browse button allows you to locate and set your SSH key file. After setting your key file, click the Save button. CAUTION: If you click <i>Restore Default(s)</i> and then <i>Save</i> button, your key file that you set will be deleted. Please keep your own copy of the file in a safe place.	Assessment	There is no default key set in the appliance. The private key file type, RSA or DSA, can be uploaded. Any uploaded key files will be renamed as <code>id_rsa</code> or <code>id_dsa</code> , depending on the type of key that was uploaded. If you uploads a key file and a key file already exists in the appliance, the old key will be replaced with the new key.
MSSQL Server Level Exclusions	A comma separated list of the databases that will be skipped when a "Server Level" scan of a MS SQL target is done.	Assessment	<code>model,tempdb,pubs,msdb,Northwind</code>

Property	Purpose	Tab	Possible Values and Default Values
Sybase Server Level Exclusions	A comma separated list of the databases that will be skipped when a "Server Level" scan of a Sybase target is done.	Assessment	model,tempdb,pubs2,pubs3,jpubs ,sybsyntax,sybsecurity,sybsystem db,sybsystemprocs
Company Logo	Location and name of file containing your company's logo. When you locate and specify a new image via the Browse button and then save it via the Save button, it will be placed in <i><FortiDB-install directory>/conf/reportlogos</i> for subsequent use in your reports.	Reporting	
Company Name	The company name to be displayed on VA reports.	Reporting	Fortinet
Email Server Host Name	The email server hostname or IP address. Email notifications cannot be sent when the (empty) default value for this property is used.	Notification	
Email Server Port	The server port number associated with <code>emailServerHostName</code> .	Notification	The default value is 25.
Email Server User Name	The user name associated with <code>emailServerHostName</code> .	Notification	
Email Server Password	The password associated with <code>emailServerHostName</code> .	Notification	
Idle Account Expiration	The number of days a user can be inactive after which the account expires.(This does not apply to the FortiDB superuser, admin.) An expired account is "locked" and can be unlocked by a user with Security Administrator privileges.	User Profile/Security	The default value is -1.
Days Until Password Expiration	The number of days after which an unchanged password expires.	User Profile/Security	The default value is -1.

Property	Purpose	Tab	Possible Values and Default Values
Max Number of Failed Login Attempts	The number of login attempts allowed before user account is locked. (This does not apply to the FortiDB superuser, <code>admin</code> .)	User Profile/Security	The default value is -1.
Minimum Password Length	The minimum length of a user password.	User Profile/Security	The default value is -1.
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> .
Enable Pen Test For All Users in Database (Standalone only)	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: <ul style="list-style-type: none"> • <code>ora</code> for Oracle • <code>sql</code> for MS-SQL • <code>db2</code> for DB2 UDB • <code>syb</code> for Sybase When set to <code>true</code> , FortiDB ignores the user names in <code><dbtype>user.txt</code> .	Assessment	<code>true</code> or <code>false</code> . The default value is <code>true</code> .
Pen Test Method	The Login method actually logs in to your target databases. CAUTION: <i>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.</i> 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.	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 default dictionary is being used. “User Dictionary” indicates that you have uploaded your own dictionary file. The filename of the dictionary you upload will not appear here. NOTE: When you restore the default dictionary by checking the checkbox, and clicking Restore Default(s) and then Save, your dictionary file will be deleted from the system.
SNMP Community String	The SNMP community name.	Notification	The default value is <code>public</code> .
SNMP Receiver Host	The SNMP receiver host. SNMP-trap notifications cannot be sent when this field is empty.	Notification	
SNMP Receiver Port	The SNMP receiver port number.	Notification	The default value is <code>0</code> .



User Management

This section describes user management including the task of adding (or modifying) FortiDB users, role-dependent permissions, and deleting users.

Adding (or Modifying) a User

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

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

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

2. Click the **Add** button. (or, to modify a user's settings, click the **User Name** of the user whose settings you want to change.)
3. On the **General** tab of the **Add New User** page (or **User Details** page, if you are modifying an existing user), enter all mandatory items.

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

When choosing a password, use one that follows these rules:

<i>Rule Category</i>	<i>Description</i>
Mandatory Length	By default, no mandatory length is set. You can set the length limitation in System Configuration. Please see the link below for information on setting FortiDB-system properties.
Mandatory Contents	<ul style="list-style-type: none"> • At least one number • At least one special character from this set: !@#\$%^&*()_+ ~- =\`{}[]:":';<>?.,/
Prohibited Contents	<ul style="list-style-type: none"> • Any spaces • User name • User name reversed

Example: wru2rxy? is a valid password.

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

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

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

Role-Dependent Permissions

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

Permissions by Role

Once a given role has been assigned to a user, that user can only perform certain FortiDB operations. For example, a user assigned the System Administrator role will only have access to the **System Configuration** link and to the **Archive/Restore** link on the Navigation Panel.

Here is the mapping between the built-in FortiDB roles and their corresponding permissions.

Table 1: Permissions by Role




Role	Permissions
Assessment Manager	<ul style="list-style-type: none"> • Review target-database connection information. • Review target group connection information • View Pre-defined Policies (PDPs) and User-Defined Policies (UDPs) • Create, modify, delete, and run assessments • Read results of FortiDB-shipped reports • Read results of Custom reports • Perform Penetration Tests • View the Privilege Summary
Policy Manager	<ul style="list-style-type: none"> • Import/export and enable/disable Pre-defined Policies (PDPs) • Import/export and enable/disable User-Defined Policies (UDPs) • Add Policy Groups • Create, modify and delete User-Defined Policies (UDPs)
Report Manager	<ul style="list-style-type: none"> • Review target-database connection information. • Review target group connection information • Review Assessment settings • Read results of FortiDB-shipped reports • Read results of Custom reports • View the Privilege Summary
Security Administrator	<ul style="list-style-type: none"> • Create, modify, delete and enable/disable FortiDB users • Configure and modify user-role assignments • View the Entitlement report

Role	Permissions
System Administrator	<ul style="list-style-type: none"> • Import/export and enable/disable Pre-defined Policies (PDPs) • Import/export and enable/disable User-Defined Policies (UDPs) • Archive and restore assessment results • Change system properties
Target Manager	<ul style="list-style-type: none"> • Create, modify, delete, and import/export connections to target databases • Create, modify, and delete target-groups • Perform Auto Discovery of target databases • Review Assessment settings • Review the Privilege Summary

User Management Icon Descriptions

Here are the User Management icon descriptions:

Table 2: User Management Icon Descriptions

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

Deleting Users

This topic describes how to delete FortiDB users.

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

About FortiDB Archiving and Restoring

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

Assessment-related information in the FortiDB repository can be moved to archive files in order to conserve repository space and improve performance. When an assessment is archived, the information is exported and then deleted, from the repository.

NOTE: FortiDB archives are stored within encrypted files in *<FortiDB-install directory>/data/archives/va*. Depending upon your assessment frequency and upon the number and type of policies and target databases involved, this files in this directory can consume a large amount of space. So, you could move the files to a separate location and then move them back when needed.

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

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

The entry in the **Timestamp** column on **Restore** tab of the **Assessment-Results Archive and Restore** page represents the day and time that the assessment-archive was performed.

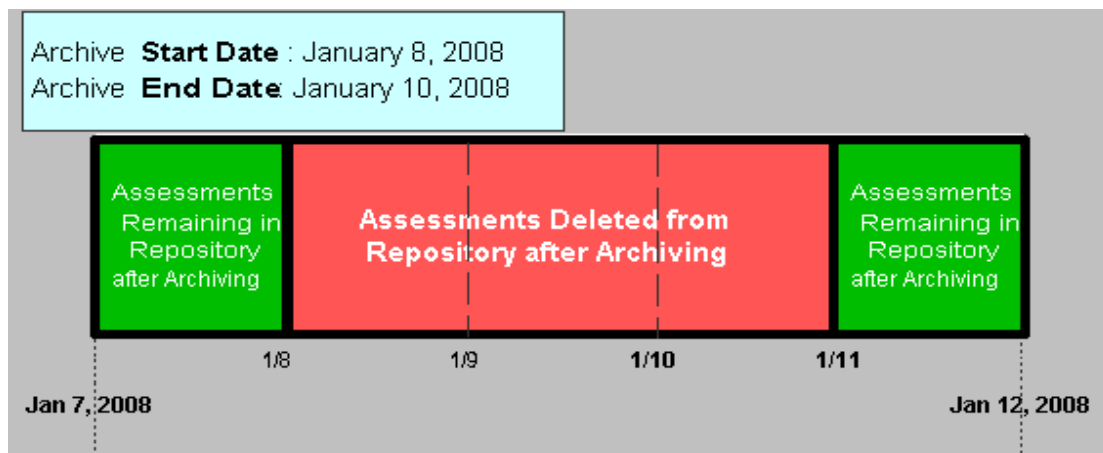
Once restored and in order to prevent duplicate records in the FortiDB repository, any records already in the FortiDB repository will not be restored (again) during the restore process.

About Archiving

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

Effect of Archiving

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



An Archiving Strategy

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

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

Three months worth of assessment information would then remain in your repository.

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

Archiving Immediately

This topic describes the how to archive assessments immediately.

1. In order to archive immediately, click on the **Archive/Restore** link in the **Administration** section of the left-side tree-navigation menu and choose the **Archive** tab.
2. Specify a start and end date for your archive.

NOTE: The archive includes assessments on the start and end dates you choose.

3. Click the **Archive Now** button.

You should then see an `Archive - X/Y - RUNNING` message followed by an `Archive Complete` message in the **Status** area in the upper-right corner of the page. (X represents the number of the archive-file records which are currently restored ; Y represents the total number of archive-file records.)

Scheduling an Archive

This topic describes the how to archive assessments via a schedule.

1. In order to schedule click on the **Archive/Restore** link in the **Administration** section of the left-side tree-navigation menu and choose the **Archive** tab.
2. In the **Archive period** section, specify the archive period for which you want to archive assessment results. Here you can specify the number of days, weeks, or months, prior to the current date, that you want as the last date for the assessment data in the archive.
For example: "3 Month(s) and older" would result in an archive that contained results for all assessments except those run in the last 3 months.
3. In the **Run time** section, specify a **Start at** time or, in the **Recurrence pattern** section, specify either the **Hourly**, the **Daily**, **Weekly**, or **Monthly** radio button.
 - If you choose the **Hourly** radio button, you can then specify the hourly interval in the **Every __ hours** field.
 - If you choose the **Daily** radio button, you can then specify the daily interval in the **Every __ days** field.
 - If you choose the **Weekly** radio button, you can then specify the weekly interval in the **Every __ week(s) on** field. You should then specify on which day(s) of the week you want to run your archive by clicking one or more of the appropriate day checkbox(es).
 - If you choose the **Monthly** radio button, you can then specify which day during the month and which months during the year you want your archive to run. There are checkboxes for you to specify in which months you want to run your assessments. The **Day** radio button and adjacent dropdown list allows you to specify the numeric day for your archive to run in each specified month. Alternatively, you may specify the day in each month, such as the 'first Monday', using the two dropdown lists.
4. If you want your schedule to go into effect immediately, click the **Enable Auto Archive** check box.
5. Click the **Save** button.

Using FortiDB Restore

This topic describes the how to restore FortiDB assessment archives.

1. In order to restore, navigate to the **Assessment-Results Archive and Restore** page, and choose the **Restore** tab.

NOTE: Entries in the **# of Assessments** column represent the number of completed assessments included in the archive of that row.

2. Select the radio button next to the archive file of interest.
3. (Optionally) check the **Delete archive file after restore** checkbox if you want the archive file to be deleted after a successful restoration.
4. Click the **Restore** button.

You should then see a `Restore - X/Y - RUNNING` message followed by an `Restore - X/Y - Complete` message in the **Status** area in the upper-right corner of the page. (*X* represents the number of the currently being restored archive-file record; *Y* represents the total number of archive-file records.)

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

Managing the Entitlement Report

This topic describes how to display, sort, and export the Entitlement Report.

1. In order to display the Entitlement Report page, click on the **Entitlement Report** link in the **Administration** section of the left-side tree-navigation menu.
2. Optionally, you can sort the Entitlement Report by clicking on any of the column headers. That header is used as your sort key.

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

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

3. Optionally, you can export the Entitlement Report as a PDF, Excel, comma-delimited, or tab-delimited file. Just choose the desired format in the **Export as** dropdown and click the **Export** button.

Entitlement Report Distinctions

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

Assignable Roles







The FortiDB Entitlement Report shows which of the roles are assigned to each of your users as well as user status. The roles that ship with FortiDB are:






- System Administrator
- Security Administrator
- Target Manager
- Policy Manager
- Assessment Manager
- Report Manager

Entitlement Report Icons

The Entitlement Report icons are described below:

Table 3: Entitlement Report Icon Descriptions

Icon	Description	Comments
	An Enabled user account	An account can be enabled at any time by a user who has the Security Administrator role.
	A Disabled user account	An account can be disabled at any time by a user who has the Security Administrator role.
	A Locked user account	An account can be locked after unsuccessful login attempts
	The user in this row has the above role	
	The user in this row does not have the above role	
	Values in this column indicate whether or not the user has the System Administrator role	

Icon	Description	Comments
	Values in this column indicate whether or not the user has the Security Administrator role	
	Values in this column indicate whether or not the user has the Target Manager role	
	Values in this column indicate whether or not the user has the Policy Manager role	
	Values in this column indicate whether or not the user has the Assessment Manager role	
	Values in this column indicate whether or not the user has the Report Manager role	

Index

A

- Archive
 - shedule 21
- Archiving 19
 - immediately 20
 - Now 21

D

- DNS 8
- DNS settings
 - changing 8

E

- Entitlement Report
 - Assignable Roles 23
 - distinctions 22
 - icons 23

F

- Firmware Version 3
 - changing 5
- FortiDB Host Name
 - changing 4

H

- Host Name 3

I

- Icon
 - User management 18
- Interface 6
- Interface Settings
 - changing 7

M

- Mandatory Contents 16
- Mandatory Length 16

N

- Network Configuration 6

P

- Permissions
 - Assessment Manager 17
 - by role 16
 - Policy Manager 17
 - Report Viewer 17
 - Role-Dependent 16
 - Security Administrator 17
 - System Administrator 18
 - Target Manager 18
- Prohibited Contents 16

R

- Restoring 19
- Route Settings
 - changing 9
 - deleting 9
- Route settings
 - adding 9
- Routing 8

S

- Security Administrator 17
- Serial Number 3
- System Administrator 18
- System Configuration 11
- System Information 3
- System Properties List 11
- System Resources 5
- System Time 3
 - setting 3

U

- Uptime 3
- User
 - adding 15
 - modifying 15
- User Management 15
- Users
 - deleting 19

