



# FortiNAC

## Backup and Restore

Version: 8.x

Date: August 30, 2021

Rev: E

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET KNOWLEDGE BASE**

<http://kb.fortinet.com>

**FORTINET BLOG**

<http://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<http://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**NSE INSTITUTE**

<http://training.fortinet.com>

**FORTIGUARD CENTER**

<http://fortiguard.com>

**FORTICAST**

<http://forticast.fortinet.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>



# Contents

---

Overview .....	4
What it Does .....	4
How it Works .....	4
Database and Database Archive .....	5
System Backups .....	6
Remote Backups .....	7
Scheduling .....	7
Determine Backup Frequency .....	7
Determine Purging Frequency .....	8
Configure Archive/Purge Database Records Schedule.....	8
Configure Database Backups Schedule.....	9
Configure System Backups Schedule .....	11
Manual Backups.....	12
Run Manual Backup.....	12
Remote Backups .....	13
Configure FTP Remote Backups .....	13
Configure SSH Remote Backups .....	14
Restore.....	17
Database Using Administrative UI.....	17
Database Using CLI.....	17
Archived Data .....	18
System Files/Directories .....	19

# Overview

## What it Does

Administering FortiNAC should include a backup plan in case of data corruption or equipment failure. This document describes the best practices for backing up and restoring the FortiNAC components, whether for a single server, a Control Server/Application Server pair, a High Availability (HA) system, or multiple servers managed by a FortiNAC Control Manager (NCM).

## How it Works

FortiNAC has the ability to backup the following:

- **Database:** FortiNAC's mysql database contains the components and configurations viewed/modified through the Administration UI and the last known state of those components. Everything seen in the Administration UI is kept in the database except for Alarms and Events, Connection Logs and Scan Results. Passwords are encrypted.
- **System files:** Files associated with the configurations done through Configuration Wizard as well as additional files required for appliance operation.
- **Alarms and Events:** List of Alarms and Events generated during a specific time period.
- **Connection Logs:** List of historical host/user network connections during a specific time period.
- **Scan Results:** List of scan results during a specific time period.

Backups of the database and other files occur when their corresponding scheduled tasks run. The backup files are stored on the local appliance. The Administrator can additionally configure FortiNAC to place a copy of the database and other directories on an ftp and/or other remote server for safekeeping.

FortiNAC includes these backup/restore capabilities:

- **Database Backup:** A scheduled task that backs up the entire database to the FortiNAC itself.
- **Database Archive and Purge:** Use Database Archive to set age times for selected log files (Connections, Events/Alarms, and Scan Results). Log files are archived and then purged from the FortiNAC database when the age time elapses. Archived data can be imported back into the database if necessary.
- **System Backup:** A scheduled task that creates a backup of all system files that are used to configure FortiNAC, such as license key and web server configurations.
- **Remove local backups:** The number of days desired to keep backups before deleting from the local drive. This setting is available for each of the above backup types.
- **Backup to Remote Server:** Uploads a copy of the Database Backup, Database Archive and System Backup files to a remote server.

## Database and Database Archive

Full database backups and log files that are periodically archived and purged, are stored in a compressed, date-stamped format on the Control Server (in control on an HA) in the `/bsc/campusMgr/master_loader/mysql/backup` directory. The database backup is named:

`<database>_<yyyy_mm_dd_hh_mm_ss>.gz`

The table archive is named:

`<table>_<yy_mm_dd_hh_mm_ss>.gz`

The following is a listing of backup files. Notice that there are entries for the complete database (DataBase\_BackUp) and the archived records (e.g., ALARMS\_Archive). Note that file size will vary.

```
52M FortiNAC_DataBase_BackUp_2017_08_21_00_01_35_bcm.gz
4.6M EVENTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
67K TESTS_RESULTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
43K RESULTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
52K MAC_RESULTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
116K ALARMS_Archive_2017_08_21_01_01_15_bcm.bua.gz
3.1M DYNAMICLOG_Archive_2017_08_21_01_01_15_bcm.bua.gz
1.2M CONNECTIONS_Archive_2017_08_21_23_44_15.bua.gz
```

The following table maps the type of records that are archived to the backup filename.

### Database Backup Filenames

Database Records	Filename
Database	Database_BackUp
Events	EVENTS_Archive
Alarms	ALARMS_Archive
Scan Results	RESULTS_Archive (coupled with TEST_RESULTS and MAC_RESULTS)
Connections	DYNAMICLOG_Archive (coupled with CONNECTIONS_Archive)

## System Backups

A system backup creates a backup of all system files that are used to configure FortiNAC, such as license key and web server configurations. Backups of selected files and directories are stored in a compressed, date-stamped format on the same server where they reside in the

*/bsc/backups/<hostname>* directory as:  
*<hostname>.<yyyy\_mm\_dd>.<directory>.tar.gz*

For example, for a Control/Application Server pair, qa192/qa229, the files on qa192 would be backed up to */bsc/backups/qa192* on qa192, and the files on qa229 would be backed up to */bsc/backups/qa229* on the qa229.

The following is a sample list of file/directory backups on host qa6-74.

```
/bsc/backups/qa6-74
qa6-74.20180514.etc.tar.gz
qa6-74.20180514.bsc-.runtime-data.tar.gz
qa6-74.20180514.root.tar.gz
qa6-74.20180514.var-spool-cron.tar.gz
qa6-74.20180514.bsc-Registration.tar.gz
qa6-74.20180514.bsc-Remediation.tar.gz
qa6-74.20180514.bsc-Hub.tar.gz
qa6-74.20180514.bsc-Authentication.tar.gz
qa6-74.20180514.bsc-DeadEnd.tar.gz
qa6-74.20180514.bsc-CommonJspFiles.tar.gz
qa6-74.20180514.bsc-VPN.tar.gz
qa6-74.20180514.bsc-www.tar.gz
qa6-74.20180514.home-admin.tar.gz
qa6-74.20180514.bsc-siteConfiguration.tar.gz
qa6-74.20180514.bsc-services-tomcat-admin-conf.tar.gz
qa6-74.20180514.bsc-services-tomcat-portal-conf.tar.gz
qa6-74.20180514.bsc-campusMgr-master_loader-telnetMibs.tar.gz
qa6-74.20180514.bsc-campusMgr-master_loader-customTraps.tar.gz
qa6-74.20180514.bsc-campusMgr-.keystore.gz
qa6-74.20180514.bsc-campusMgr-.licenseKey.gz
qa6-74.20180514.bsc-campusMgr-bin-.backup_config.gz
qa6-74.20180514.bsc-campusMgr-bin-.config.properties.gz
qa6-74.20180514.bsc-campusMgr-bin-.sshaccountInfo.gz
qa6-74.20180514.bsc-campusMgr-bin-.networkConfig.gz
qa6-74.20180514.bsc-campusMgr-bin-.yams.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cm.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cmas.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cmas.copy.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cmas.maintenance.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cm.copy.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cm.maintenance.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cmrc.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cmrc.copy.gz
qa6-74.20180514.bsc-campusMgr-master_loader-.cmrc.maintenance.gz
qa6-74.20180514.bsc-campusMgr-agent-scanConfig.tar.gz
qa6-74.20180514.bsc-campusMgr-agent-customScanConfig.tar.gz
```

## Remote Backups

If FortiNAC data is not backed up to a remote server, there is the potential of losing file and database backups if a disk/appliance fails. The Remote Backup feature copies the database and file backups to the specified remote server, using either FTP or SSH. The best practice is to include remote offsite backup using SSH. Refer to Online Help topic **Configure The Remote Backup Destination** for information about configuring communication between the FortiNAC and remote servers.

FTP access utilizes the login credentials (user name and password) set up in the Admin UI, whereas SSH uses an encrypted key which must be copied from the FortiNAC to the remote server, preferably in some account other than ROOT. (See [Configure SSH Backups](#))

**Note:** Bradford does not manage backups on a remote server.

## Scheduling

Scheduling options are available for each of the backup configurations:

- Database
- System files
- Database Archive
  - Alarms and Events
  - Connection Logs
  - Scan Results

## Determine Backup Frequency

How often the various backups are run depends upon the anticipated network activity. Consider the frequency of change for the following, and determine the frequency based on the most frequent occurrence.

- Database
  - New registrations (BYOD, company assets, headless devices, etc)
  - Network infrastructure configuration models added or modified in FortiNAC Topology
  - **Best practice:** Backup the database daily
- System files
  - Changes made via configWizard (DHCP scopes, etc)
  - **Best practice:** Unless needed more often, backup the system files weekly.
- Database Archive
  - Alarms and Events: The frequency alarms and events are generated
  - Connection Logs: Devices connecting and disconnecting from the network
  - Scan Results: How often hosts are scanned

**Note:** Once logs are archived, they are no longer searchable via the Alarms, Events or Connection Logs view.

## Determine Purging Frequency

Decide how long to keep backups before deleting. Keep in mind the possible conflicts between scheduled backups and configured backup removal, and the configured timeout for the backup process:

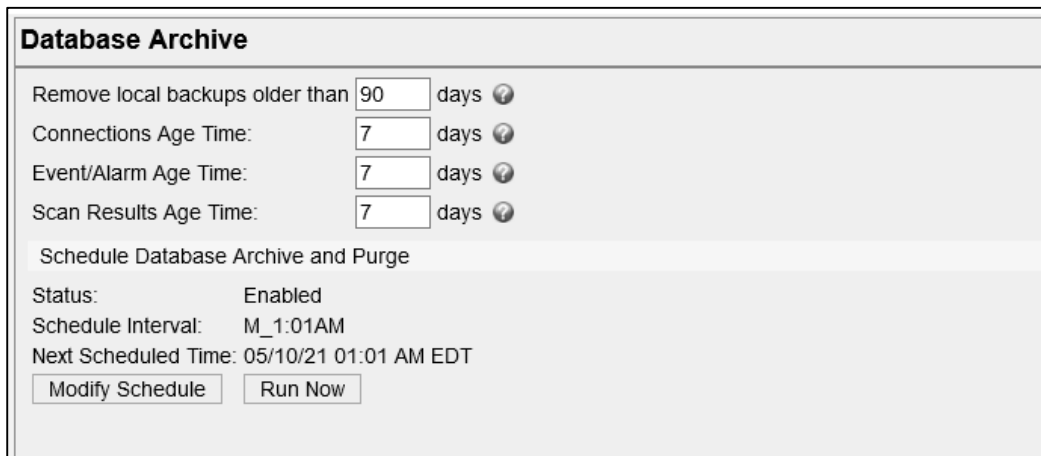
The **Remove Backups Older Than** field is available for all three backup configurations and are independent of each other. This field value should always be larger than the frequency used for the backup. For example, if the field is set to 5 days and the backup task runs every 15 days, all of the backups may be removed inadvertently. However, if the remove option is set to 15 days and the backup task runs every 5 days, then there would always be backup files available.

**Note:** This parameter affects the backups on the local server only, not backups on the remote server.

## Configure Archive/Purge Database Records Schedule

When the Events Archive and Purge task is run, records older than the corresponding Age Time field (in Topology view, FortiNAC Properties tab) are archived to the local Control Server and purged from the database.

1. Navigate to **System > Settings > System Management > Database Archive**

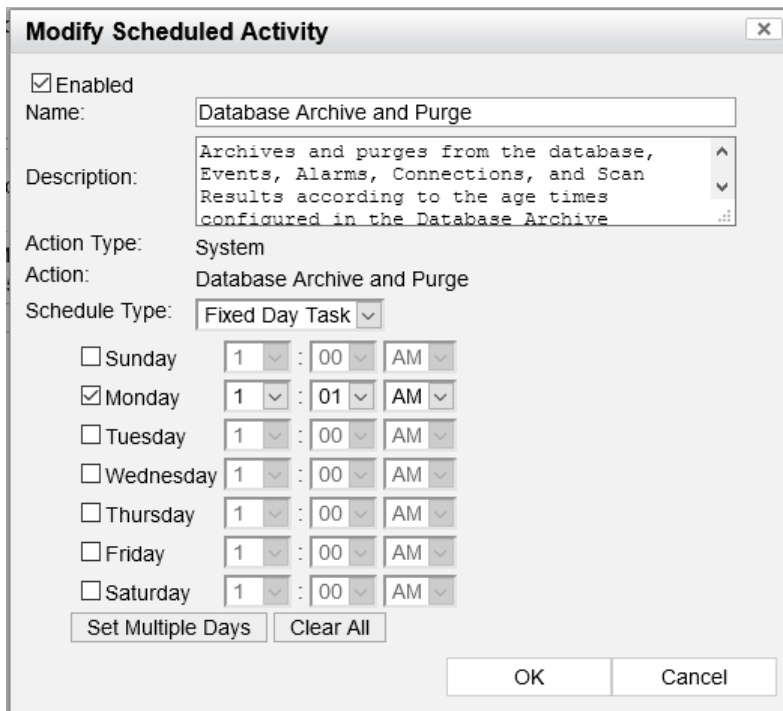


Database Archive	
Remove local backups older than	90 days
Connections Age Time:	7 days
Event/Alarm Age Time:	7 days
Scan Results Age Time:	7 days
Schedule Database Archive and Purge	
Status:	Enabled
Schedule Interval:	M_1:01AM
Next Scheduled Time:	05/10/21 01:01 AM EDT
<input type="button" value="Modify Schedule"/> <input type="button" value="Run Now"/>	

2. Set **Remove local backups older than** to desired value. See [Purging Frequency](#).
3. Set Age Times as desired.
4. Click **Modify Schedule**.

**Note:** This same view can be accessed by navigating to **System > Scheduler**. Double click **Database Archive and Purge**.

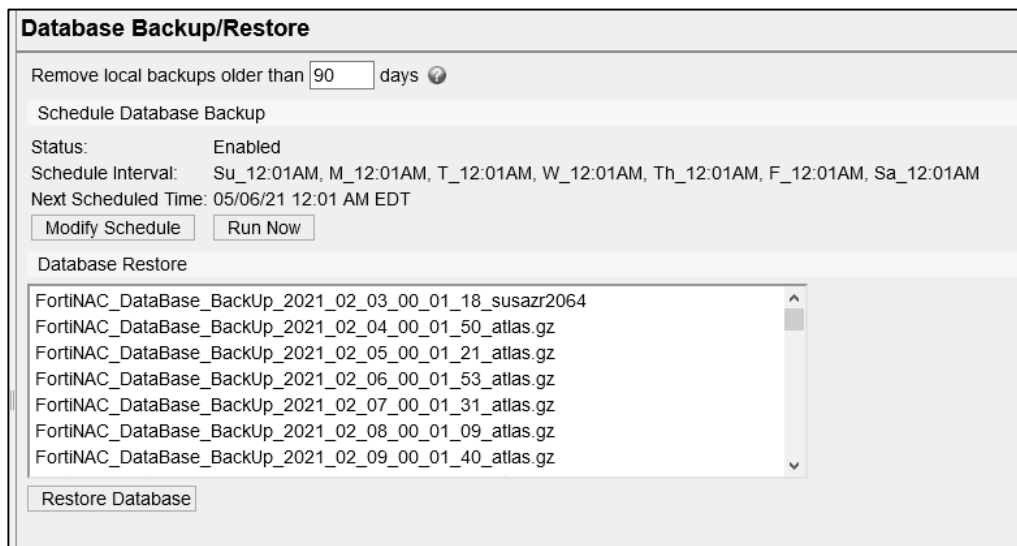




5. Enable the task and edit as appropriate. For details see [Database archive](#) in the Administration Guide.
6. Click **OK**.
7. Click **Save Settings**.

## Configure Database Backups Schedule

1. Navigate to **System > Settings > System Management > Database Backup/Restore**.



2. Set **Remove local backups older than** to desired value. See [Purging Frequency](#).
3. Click **Modify Schedule**.

**Note:** This same view can be accessed by navigating to **System > Scheduler**. Double click **Database BackUp**.

**Modify Scheduled Activity**

Enabled

Name: Database BackUp

Description: Database backup schedule.

Action Type: System

Action: Database Backup

Schedule Type: Fixed Day Task

<input checked="" type="checkbox"/> Sunday	1	:	00	AM
<input checked="" type="checkbox"/> Monday	1	:	00	AM
<input checked="" type="checkbox"/> Tuesday	1	:	00	AM
<input checked="" type="checkbox"/> Wednesday	1	:	00	AM
<input checked="" type="checkbox"/> Thursday	1	:	00	AM
<input checked="" type="checkbox"/> Friday	1	:	00	AM
<input checked="" type="checkbox"/> Saturday	1	:	00	AM

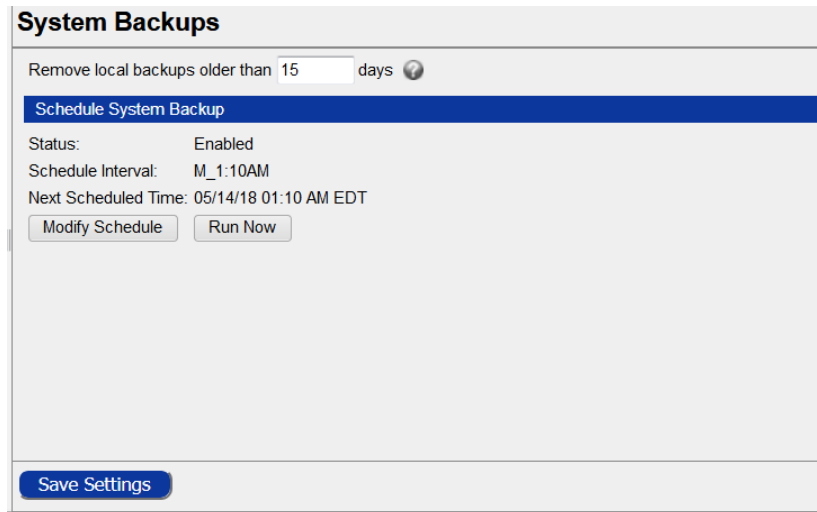
Set Multiple Days Clear All

OK Cancel

4. Enable the task and edit as appropriate. For details see [Backup or restore a database](#) in the Administration Guide.
5. Click **OK** to save schedule settings.
6. Click **Save Settings**.

## Configure System Backups Schedule

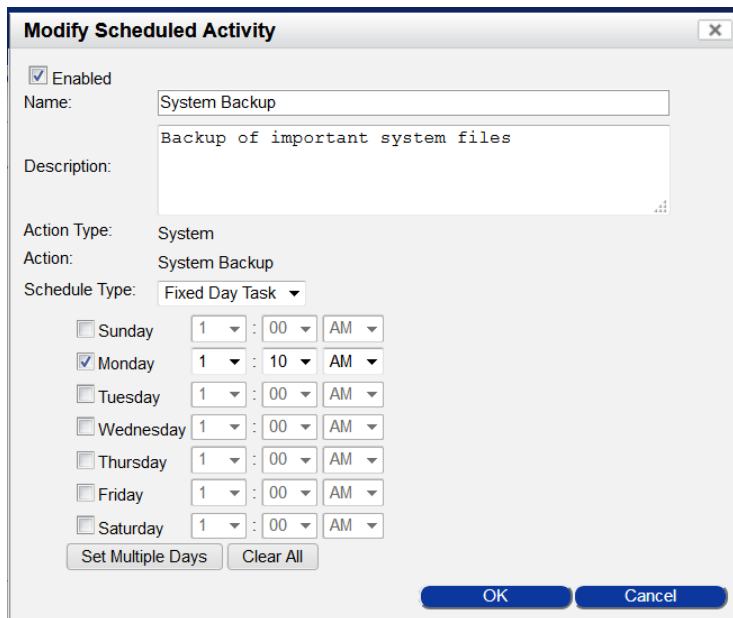
1. Click **System > Settings > System Management > System Backups**.



The screenshot shows the 'System Backups' configuration window. At the top, there is a header 'System Backups'. Below it, a text field indicates 'Remove local backups older than 15 days'. A blue bar highlights the 'Schedule System Backup' section. Under this section, the status is 'Enabled', the schedule interval is 'M\_1:10AM', and the next scheduled time is '05/14/18 01:10 AM EDT'. There are two buttons: 'Modify Schedule' and 'Run Now'. At the bottom of the window, there is a 'Save Settings' button.

2. Set the **Remove local backups older than** to desired value. See [Purging Frequency](#).
3. Click **Modify Schedule**.

**Note:** This same view can be accessed by navigating to **System > Scheduler**. Double click **System Backup**.



The screenshot shows the 'Modify Scheduled Activity' dialog box. It has a title bar with a close button. The 'Enabled' checkbox is checked. The 'Name' field contains 'System Backup' and the 'Description' field contains 'Backup of important system files'. The 'Action Type' is 'System' and the 'Action' is 'System Backup'. The 'Schedule Type' is 'Fixed Day Task'. Below this, there are seven rows for days of the week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. Each row has a checkbox, a dropdown for the day number (all set to '1'), a dropdown for the hour (all set to ':00'), and a dropdown for the period (all set to 'AM'). The 'Monday' checkbox is checked. At the bottom, there are 'Set Multiple Days' and 'Clear All' buttons, and 'OK' and 'Cancel' buttons.

4. Enable the task and edit as appropriate. For details see [System backups](#) in the Administration Guide.
5. Click **OK**.
6. Click **Save Settings**.

# Manual Backups

Scheduled backups should be run before:

- Any major changes to FortiNAC’s configuration
- Upgrading hardware. Before replacing the hardware, back up the database and files/directories list to a remote server.

**Note:** FortiNAC automatically backs up files during software upgrades.

## Run Manual Backup

In addition to the individual configuration views, each backup can be scheduled and run from the Scheduler view.

1. Navigate to **System > Scheduler**.

Filter								
Add Filter: <input type="text" value="Select"/>		<input type="button" value="Update"/>						
<input type="button" value="Add"/>		<input type="button" value="Modify"/>		<input type="button" value="Delete"/>		<input type="button" value="Copy"/>		<input type="button" value="Run Now"/>
Scheduled Activities - Displayed: 8 Total: 8								
Enable: <input checked="" type="checkbox"/> <input type="checkbox"/>								
Name	Action	Group	Enabled	Schedule	Last Scheduled Time	Next Scheduled Time	Last Modified By	Last Modified Date
Auto-Definition Synchronizer	Auto-Definition Synchronizer		✓	7 Days	05/02/21 01:01 AM EDT	05/09/21 01:01 AM EDT	SYSTEM	05/02/21 01:01 AM EDT
CarolynSharedScheduled	Custom Script		✓	7 Days	05/04/21 02:54 PM EDT	05/11/21 02:54 PM EDT	SYSTEM	05/04/21 02:54 PM EDT
Certificate Expiration Monitor	Certificate Expiration Monitor		✓	1 Days	05/05/21 10:00 AM EDT	05/06/21 10:00 AM EDT	SYSTEM	05/05/21 10:00 AM EDT
Database Archive and Purge	Database Archive and Purge		✓	M_1:01AM	05/03/21 01:01 AM EDT	05/10/21 01:01 AM EDT	SYSTEM	05/03/21 01:01 AM EDT
Database BackUp	Database Backup		✓	Su_12:01AM, M_12:01AM, T_12:01AM, W_12:01AM, Th_12:01AM, F_12:01AM, Sa_12:01AM	05/05/21 12:01 AM EDT	05/06/21 12:01 AM EDT	SYSTEM	05/05/21 12:02 AM EDT
Operating System Update Status	Check for OS Updates		✓	7 Days	05/02/21 01:01 PM EDT	05/09/21 01:01 PM EDT	SYSTEM	05/02/21 01:01 PM EDT
Synchronize Users with Directory	Synchronize Users from Directory		✓	1 Days	05/05/21 02:01 AM EDT	05/06/21 02:01 AM EDT	SYSTEM	05/05/21 02:02 AM EDT
System Backup	System Backup		✓	M_1:10AM	05/03/21 01:10 AM EDT	05/10/21 01:10 AM EDT	SYSTEM	05/03/21 01:10 AM EDT

2. Highlight the desired activity:
  - Database Archive and Purge**
  - Database Backup**
  - System Backup**

3. Click **Run Now**.

A second instance of the activity will appear under the original activity, indicating the activity is running.

System Backup	System Backup
System Backup - Running	System Backup

This instance will disappear upon refresh once the backup has completed.

# Remote Backups

Remote Backup Configuration defines the connection details used to copy files to a third party (remote) server when the Database Backup task is run in Scheduler. Transferring the backup files can be done using FTP and/or SSH protocols.

## Configure FTP Remote Backups

### Configure Remote Server

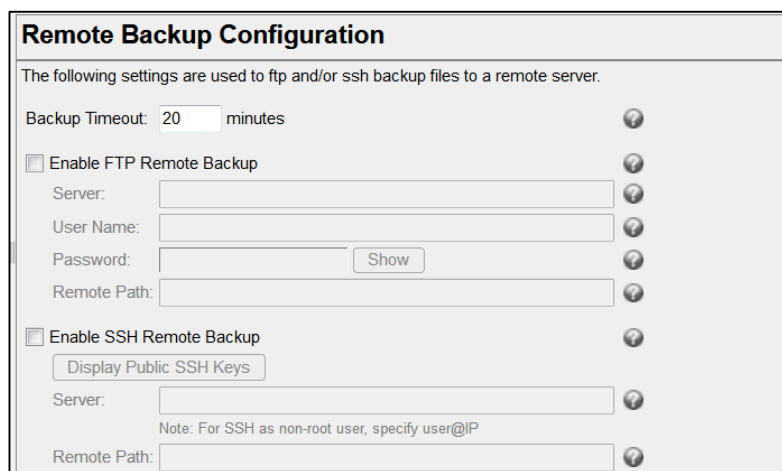
1. Create an account on the remote FTP server to be used by FortiNAC for backup file transfer.
2. Create a folder to which FortiNAC will copy the files.

For instructions on completing the above tasks, consult documentation specific to the FTP application used.

### Configure FortiNAC

Once the remote server has been configured, configure FortiNAC with the appropriate connection information.

1. Navigate to **System > Settings > System Management > Remote Backup Configuration**.



The screenshot shows the 'Remote Backup Configuration' web interface. At the top, it states: 'The following settings are used to ftp and/or ssh backup files to a remote server.' Below this, there are several configuration fields:

- Backup Timeout:** A text input field containing '20' followed by 'minutes' and a help icon.
- Enable FTP Remote Backup:** A checkbox that is currently unchecked, with a help icon.
- FTP Fields:** Four text input fields labeled 'Server:', 'User Name:', 'Password:', and 'Remote Path:'. The 'Password:' field has a 'Show' button to its right. Each field has a help icon.
- Enable SSH Remote Backup:** A checkbox that is currently unchecked, with a help icon.
- SSH Fields:** A 'Display Public SSH Keys' button, a 'Server:' text input field, and a 'Remote Path:' text input field. Each of these has a help icon.
- Note:** A small note below the SSH fields reads: 'Note: For SSH as non-root user, specify user@IP'.

2. In the **Backup Timeout** field, enter the number of minutes for the backup to be created and copied to the remote server.

**Important:** The value in this field should allow sufficient time for the backup to be created and copied to the remote server. If this time elapses before the backup is done, the process is interrupted. The default is 20 minutes, however, large systems may require more time. Keep in mind the transfer time to copy the backup to the remote server may vary depending on other traffic on the network and the server's capabilities.

3. Select **Enable FTP Remote Backup** to enable the remote backup to that server(s).

4. Enter the connection information for the backup server(s). For details see [Backup to a remote server](#) in the Administration Guide.
5. Click **Save Settings**.

### **Validate**

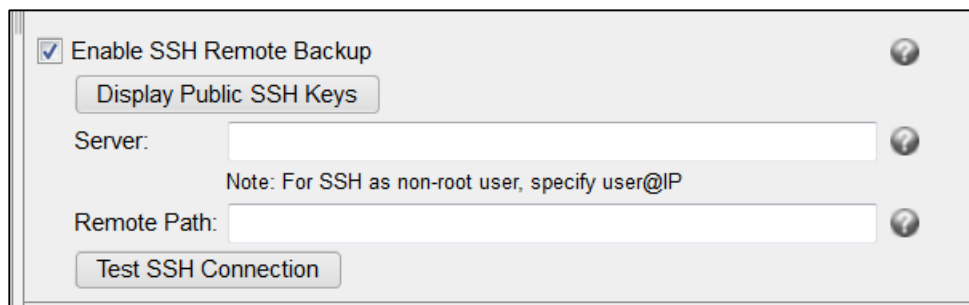
1. Navigate to **System > Scheduler**.
2. Highlight **Database BackUp**.
3. Click **Run Now**.
4. Run manual backups for **Database Archive** and **Purge and System Backup**.
5. Once the activity completes, verify the files were stored on the remote server in the specified directory path.

## **Configure SSH Remote Backups**

SSH communication must be established between the FortiNAC Control Server or FortiNAC Server and the remote backup server for the SSH remote backups to be successful. Ensure that the public key for the root user on the host being backed up has been appended to the `authorized_keys` file in the `<root home dir>/ssh` directory of the remote server. In the case of High Availability, the SSH keys for both the primary and secondary must be appended to the `authorized_keys` file.

### **Configure FortiNAC**

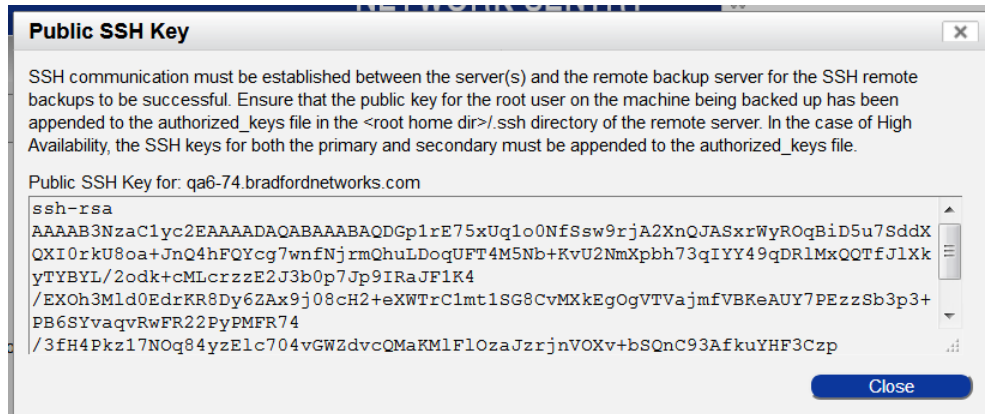
1. From the Admin UI, navigate to **System > Settings > System Management > Remote Backup Configuration** and locate the SSH section.
2. Select the **Enable** checkbox.



The screenshot shows the SSH Remote Backup configuration panel. It includes a checked checkbox for "Enable SSH Remote Backup", a "Display Public SSH Keys" button, a "Server:" text input field, a note "Note: For SSH as non-root user, specify user@IP", a "Remote Path:" text input field, and a "Test SSH Connection" button. Each input field has a help icon to its right.

3. Set the Server field to the backup user account on the remote, using the format `<username>@<ip-address>`

4. Set the remote path to the directory where the backups should be stored. Use a dot (.) to define the current directory.
5. Copy the Public SSH Key for FortiNAC by clicking **Display Public SSH Keys** and copying the key(s) to a text file.



- Alternatively, the keys can be copied from the CLI on the FortiNAC Control Server as **root**.
- a. Navigate to the `.ssh` directory:  
`cd /root/.ssh`
  - b. Display and copy the key:  
`cat id_rsa.pub`

### Configure Remote Server

Copy the key(s) to the remote server account (presumes the remote server uses a Linux platform).

1. Access the remote server where the backups will be stored as `root`.
2. If the `.ssh` directory does not exist, create it:  
`mkdir /home/backup_username/.ssh`
3. Change the permissions:  
`chmod 700 /home/backup_username/.ssh`
4. Navigate to the `.ssh` directory, and then paste (append) the key you copied from the FortiNAC to the `authorized_keys2` file:  
`cd /home/backup_username/.ssh`  
`vi authorized_keys2`

**Note:**

- The format of `authorized_keys2` file is one entry per line.
- The key must be identical to the key on FortiNAC no extra white space or characters.

5. For a Control Server/Application Server pair, repeat this process for the key on the Application Server.
6. Create the backup directory to which the files will be copied.

### **Validate**

1. Validate the SSH Connection.
  - **Administrative UI:** Click **Test SSH Connection** to validate the SSH Server and SSH Remote Path settings.
  - **From the CLI:** Enter the SSH command, specifying the backup user account on the remote:  
`ssh <backup_user>@<ip_remote>`
2. Navigate to **System > Scheduler**.
3. Highlight **Database BackUp**.
4. Click **Run Now**.
5. Run manual backups for **Database Archive** and **Purge and System Backup**.
6. Once the activity completes, verify the files were stored on the remote server in the specified directory path.



## Restore

This section describes how and when (typical scenarios) to restore from a backup file. In a High Availability configuration, the database is restored to the Control Server that is in control at the time of restore.

### Database Using Administrative UI

#### Typical Scenarios

- Data was accidentally deleted which would take extensive time to restore manually, e.g., a domain from Topology view, a list of registered clients from Clients view.
- Database was corrupted.

In these cases, the Admin UI is functioning properly and you just need to recover lost data.

**Note:** Restoring the database will not include any data captured between the time of the backup and the current time.

#### Procedure

1. Click **System > Settings > System Management > Database Backup/Restore**.
2. Click on a backup to select it.
3. Click **Restore Database**.

### Database Using CLI

#### Typical Scenarios

- The disk fails on a RAID-less appliance.
- The appliance has been reset to factory defaults, and you want to restore the pre-reset remote backup of the database.
- You have upgraded the FortiNAC hardware and want to restore the most recent remote backup from the previous FortiNAC appliance.

#### Procedure

1. Copy (e.g., use winscp) the most recent backup from the remote server to the **/bsc/campusMgr/master\_loader/mysql/backup** directory on the FortiNAC Control Server.
2. Log into the CLI on the Control Server with root privileges.
3. Stop the the FortiNAC processes:  
**shutdownCampusMgr**

4. Navigate to the **/bsc/campusMgr/master\_loader/mysql/backup** directory and identify the filename of the backup to be used.

**Example:**

```
FortiNAC_DataBase_BackUp_2018_05_14_00_01_06_qa6-74.gz
```

5. Navigate to the **/bsc/campusMgr/master\_loader/mysql** directory and restore the database:

```
ydb_restore_full_backup <database_name>
```

**Example:**

```
ydb_restore_full_backup
```

```
FortiNAC_DataBase_BackUp_2018_05_14_00_01_06_qa6-74.gz
```

6. Start the FortiNAC processes:

```
startupCampusMgr
```

## Archived Data

When the Purge Events task runs, FortiNAC creates an archive of several different types of records. You can reimport this data if necessary. Importing archived data does not overwrite existing data. It adds the archived records back into the database.

Records that are archived and can be re-imported include the following:

- Alarms View
- Events View
- Scan Results
- Connections

### Procedure

**Note:** If the archived data is not currently in the **/bsc/campusMgr/master\_loader/mysql/backup** directory on the Control Server (in control for HA), transfer a copy from the remote server (use WinSCP) to that directory.

1. Navigate to one of the views listed above.
2. Click the Import button at the bottom of the view to display the Import window.
3. Select the archive from the drop-down list. The archives are listed by date with the name of the view at the beginning. For example, for the Connections View the archive would have the following format:  
**DYNAMICLOG\_Archive\_YY\_MM\_DD.bua.gz**
4. Click **OK**.

Some archive files can be quite large and may take several minutes to import. A progress dialog is displayed as the import is taking place. A message is displayed when the import is complete.

## System Files/Directories

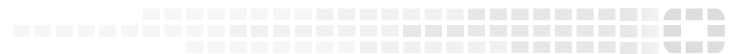
### Typical Scenarios

- Files are corrupted or accidentally deleted
- The disk fails on a RAID-less appliance.
- The appliance has been reset to factory defaults and need to restore customized files from the pre-reset remote backup.
- FortiNAC hardware has been upgraded and need to restore customized files from the pre-reset remote backup from the previous FortiNAC appliance.

### Procedure

1. Access the CLI with root privileges on the Control Server (in control for HA).
  2. Create a temporary directory.
  3. Locate the backup file (e.g., on appliance in the **/bsc/backups/<hostname>** directory, or on a remote server) from which you will restore the file(s).
  4. Copy (use WinSCP if copying from a remote server) the backup file to the temporary directory.
  5. Extract the contents of the backup file to the temporary folder, retaining the original directory structure:  
**tar -xzvf <filename>**
- Example:
- ```
tar -xzvf qa228.20091102.bsc-Authentication.tar.gz
```
6. Locate the files to be restored, and copy them to the appropriate directory(ies).

Contact Support for assistance.



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.