

Backup Configuration

Backing up the configuration

Using the GUI

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Backup*.
2. Direct the backup to your *Local PC* or to a *USB Disk*.
The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
3. If VDOMs are enabled, indicate whether the scope of the backup is the entire FortiGate configuration (*Global*) or only a specific VDOM configuration (*VDOM*).
If backing up a VDOM configuration, select the VDOM name from the list.
4. Enable *Encryption*. Encryption must be enabled on the backup file to back up VPN certificates.
5. Enter a password, and enter it again to confirm it. This password will be required to restore the configuration.
6. Click *OK*.
7. When prompted, select a location on the PC or USB disk to save the configuration file. The configuration file will have a .conf extension.

Using the CLI

Use one of the following commands:

```
execute backup config management-station <comment>
```

or:

```
execute backup config usb <backup_filename> [<backup_password>]
```

FTP

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>] [<password>]
```

TFTP

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```

VDOM

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
```

```
edit <vdom_name>
```

Using REST-API

REST-API user must have write access to FortiGate and VDOM

Create access profile

```
FGT # config system accprofile
FGT (accprofile) # edit readOnly
new entry 'readOnly' added
FGT (readOnly) # set sysgrp read
FGT (readOnly) # end
```

Create API user in FortiGate

```
FGT # config system api-user
FGT (api-user) # edit api-admin
new entry 'api-admin' added
FGT (api-admin) # set accprofile "readOnly"
FGT (api-admin) # set vdom root
FGT (api-admin) # config trusthost
FGT (trusthost) # edit 1
new entry '1' added
FGT (1) # set ipv4-trusthost 'ip_address_of_your_machine' 255.255.255.255
FGT (1) # end
FGT (api-admin) # end
```

Generate API Token

```
FGT # execute api-user generate-key api-admin
```

New API key: 'your_api_token'

NOTE: The bearer of this API key will be granted all access privileges assigned to the api-user api-admin.

Get the backup

```
HOSTNAME=<hostname>
API_TOKEN=<api-token>
```

```
DATE=`date +%F_%T%S`  
curl -k -o $HOSTNAME_$DATE.conf -H "Authorization: Bearer $API_TOKEN\"\  
"https://$HOSTNAME/api/v2/monitor/system/config/backup/?scope=global&access_token=$API_TOK  
EN"
```

Restoring a configuration

Using the GUI

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Restore*.
2. Identify the source of the configuration file to be restored: your *Local PC* or a *USB Disk*. The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
3. Click Upload, locate the configuration file, and click *Open*.
4. Enter the password if required.
5. Click *OK*.

Using the CLI

```
execute restore config management-station normal 0
```

or:

```
execute restore config usb <filename> [<password>]
```

FTP

```
execute restore config ftp <backup_filename> <ftp_server> [<port>] [<user_name>] [<password>]
```

TFTP

```
execute restore config tftp <backup_filename> <tftp_server> <password>
```

The FortiGate will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Revision #8

Created 28 October 2020 09:51:11

Updated 20 May 2021 14:27:26