

Backup and Restore a Firepower Threat Defense Device Example

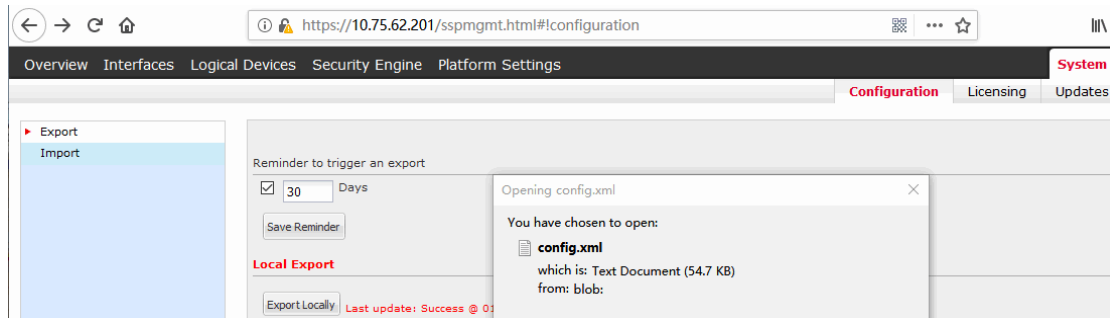
Introduction

The ability to recover from a disaster is an essential part of any system maintenance plan. As part of your disaster recovery plan, Cisco recommends that you back up the Firepower Management Center and the managed devices periodically. Backups are used to restore information while replacing a faulty or failed Firepower Management Center appliance or 7000 or 8000 Series device or a Firepower Threat Defense device.

Step to backup and restore a Firepower Threat Defense device

Step 1. Exporting an FXOS Configuration File

1. Click System > Configuration > Export.
2. Click Local Export > Export.



Step 2. Backing Up Managed Devices from a Firepower Management Center

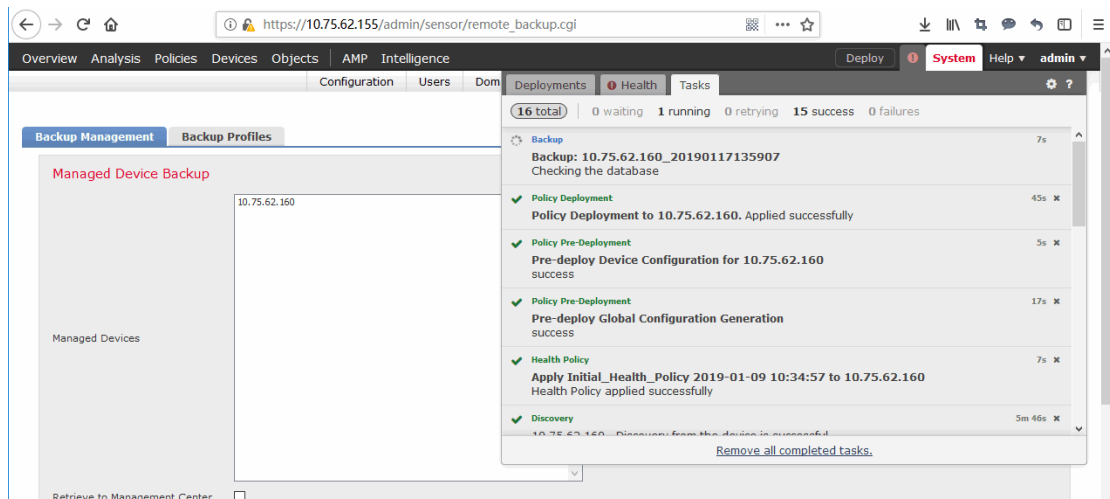
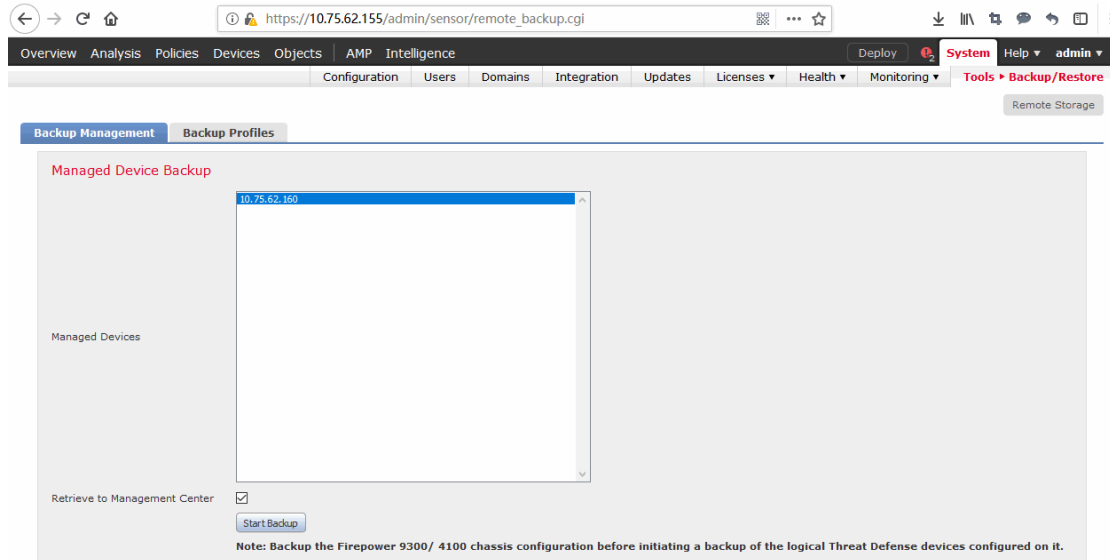
Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any except: NGIPSv Firepower Threat Defense Virtual on KVM, AWS cloud and Microsoft Azure ASA FirePOWER module	Global only	Admin/Maint

1. Select System > Tools > Backup/Restore.
2. Click Managed Device Backup.

In the Managed Devices field, select one or more managed devices.

If you uncheck the Retrieve to Management Center check box, it will save each device's backup file only on the device. Otherwise, a copy of the backup file is saved to the Firepower Management Center.

3. Click Start Backup.



Step 3. Importing an FXOS Configuration File

1. Choose System > Configuration > Import.
2. Click the Local Import > Import
3. Click Choose File to navigate to and select the configuration file that you want to import.
4. Click Import.

A confirmation dialog box opens asking you to confirm that you want to proceed and warning you that the chassis might need to restart.

Click Yes to confirm that you want to import the specified configuration file.

The existing configuration is deleted and the configuration specified in the import file is applied to the Firepower 4100/9300 chassis. If there is a breakout port configuration change during the import, the Firepower 4100/9300 chassis will need to restart.

Pay attention that any configuration at FTD will also be deleted.
 The backup file is retained locally on the Firepower 4100/9300 chassis at /var/sf/backup.
 If you choose to retain a backup on the Firepower Management Center, it is located in the /var/sf/remote-backup directory.

FTD CLI

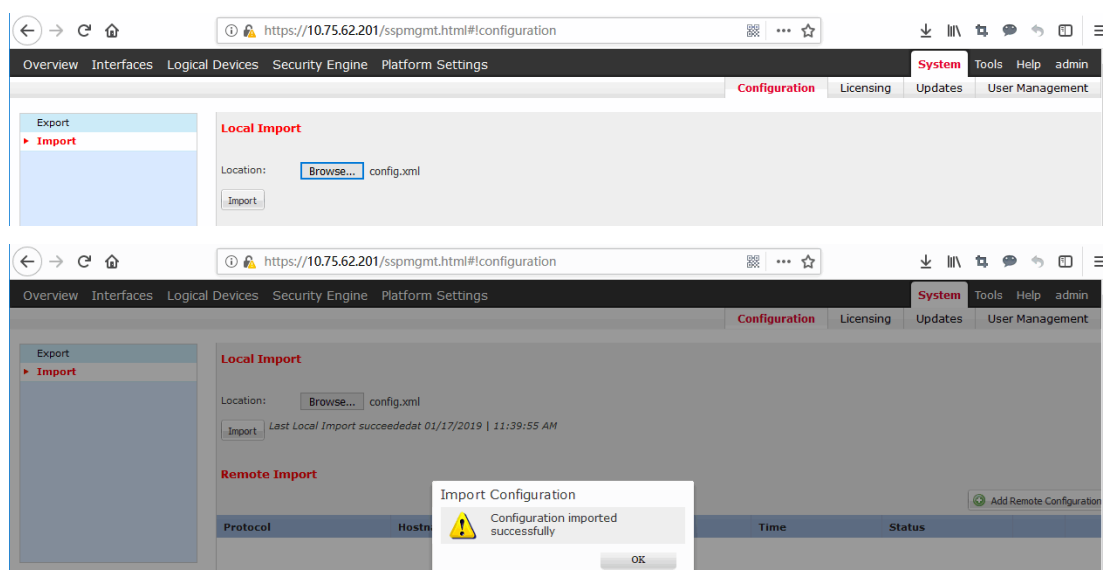
```
root@firepower:/opt/cisco/csp/applications# cd /var/sf/backup
```

```
root@firepower:/var/sf/backup# ls
10.75.62.160_20190117140532.tar
```

FMC CLI

```
root@firepower:/Volume/home/admin# cd /var/sf/remote-backup directory
```

```
root@firepower:/var/sf/remote-backup# ls
10.75.62.160_20190117135907.tar
```



Step 4. Restore a Firepower Threat Defense on a Firepower 4100 Series or Firepower 9300 device

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	N/A	FTD on the Firepower 4100 series and Firepower 9300	Global only	Admin/Maint

If the backup is at FMC, at FTD CLI run

```
> restore remote-manager-backup location 10.75.62.155 admin /var/sf/remote-backup
10.75.62.160_20190117135907.tar
```

Enter SCP password:

```
*****
```

Backup Details

```
*****
```

Model = Cisco Firepower 4120 Threat Defense

Software Version = 6.3.0
Serial = FLM2042NT9J
Hostname = 10.75.62.160
IP Address = 10.75.62.160
VDB Version = 299
SRU Version = 2018-08-23-001-vrt
FXOS Version = 2.4(1.222)
Manager IP(s) = 10.75.62.155
Backup Date = 2019-01-17 13:59:07
Backup Filename = 10.75.62.160_20190117135907.tar

If the backup is at local FTD, at FTD CLI run
> restore remote-manager-backup 10.75.62.160_20190117140532.tar

Backup Details

Model = Cisco Firepower 4120 Threat Defense
Software Version = 6.3.0
Serial = FLM2042NT9J
Hostname = 10.75.62.160
IP Address = 10.75.62.160
VDB Version = 299
SRU Version = 2018-08-23-001-vrt
FXOS Version = 2.4(1.222)
Manager IP(s) = 10.75.62.155
Backup Date = 2019-01-17 14:05:32
Backup Filename = 10.75.62.160_20190117140532.tar
