

Configure Remote Backup for FMC Using NFS Storage Device

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Topology](#)

[Add an NFS Remote Storage Device](#)

[Setup a Backup Profile](#)

[Schedule a Recurring Task to Backup the FMC](#)

[Schedule a Recurring Task to Backup the FTD](#)

[Troubleshooting](#)

Introduction

This document describes how to obtain a remote backup of Secure Firewall Management Center (FMC) and Secure Firewall Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure FMC configuration via GUI and SSH navigation
- Secure FTD navigation via shell
- Network File System (NFS) configuration

Components Used

The information in this document is based on these software and hardware versions:

- vFMC version 7.2.5
- FPR1140 running FTD 7.2.5
- NFS Windows Server

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The ability to recover from a disaster is an essential part of any system maintenance plan. As part of your disaster recovery plan, it is recommended that you perform periodic backups.

You can store backups locally. However, it is recommended that you back up management centers and managed devices to a secure remote location by mounting an NFS, Server Message Block (SMB), or Secure SHell FileSystem (SSHFS) network volume as remote storage. For the management center, you can use the **Copy when complete** option to securely copy (SCP) completed backups to a remote server.

This document refers to the NFS setup. After you accomplish this, all subsequent backups are copied to that volume, but you can still use the management center in order to manage them.



Warning: The management center setup process schedules weekly configuration-only backups, to be stored locally. This is not a substitute for full off-site backups initial setup finishes. You must review your scheduled tasks and adjust them to fit the requirements of your organization.



Tip: After configuring and choosing remote storage, you can switch back to local storage only if you have not increased the connection database limit.

Configure

Network Topology



Network Diagram

Add an NFS Remote Storage Device

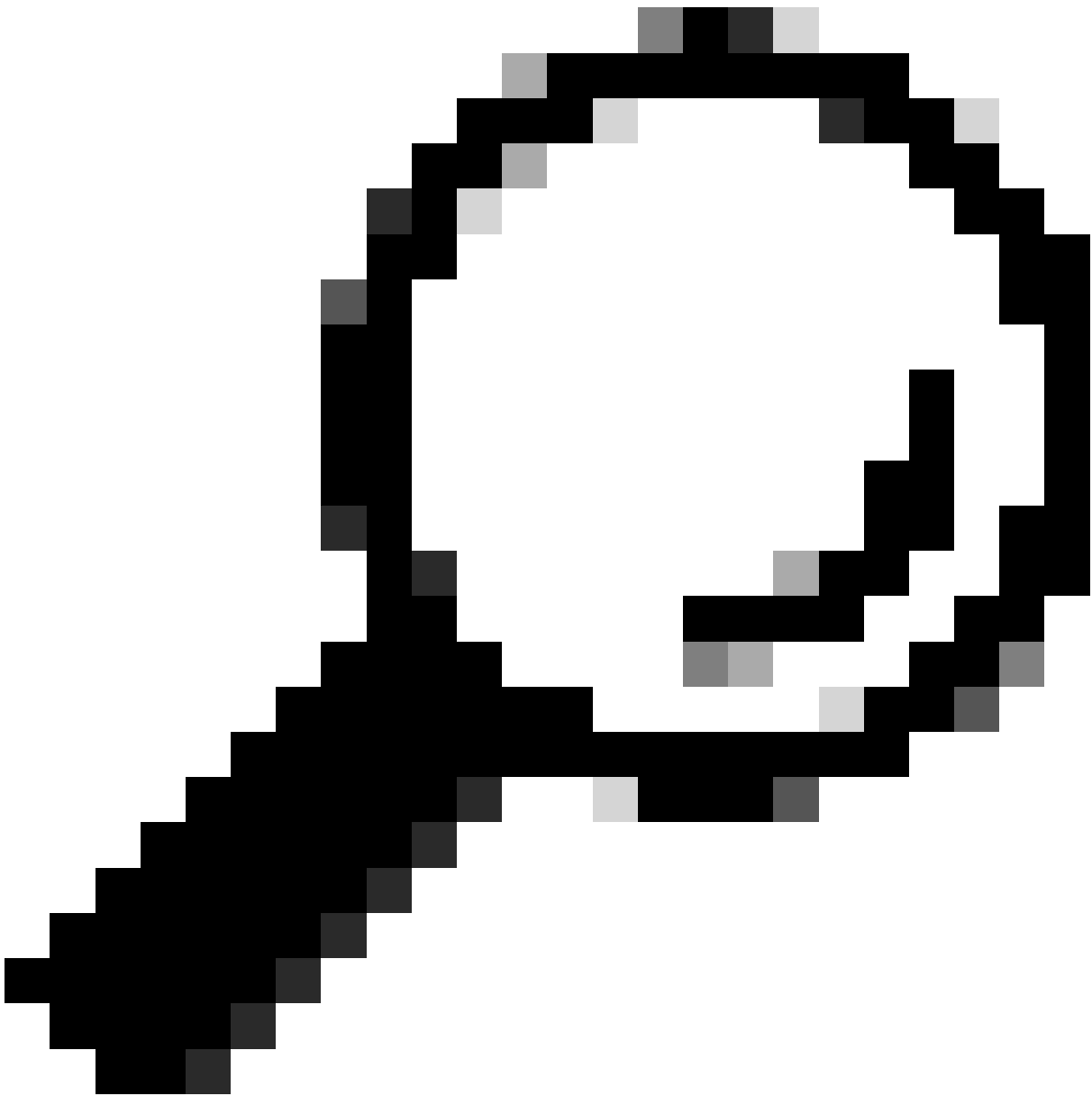
Step 1. In order to implement NFS for remote storage, `rpcbind` must be started first as it is disabled by default.

Open an SSH session to your FMC, navigate to **expert mode**, elevate to sudo rights, and issue the command `/etc/init.d/rpcbind start`.

You can validate that it has started correctly with the command `/etc/init.d/rpcbind status`.

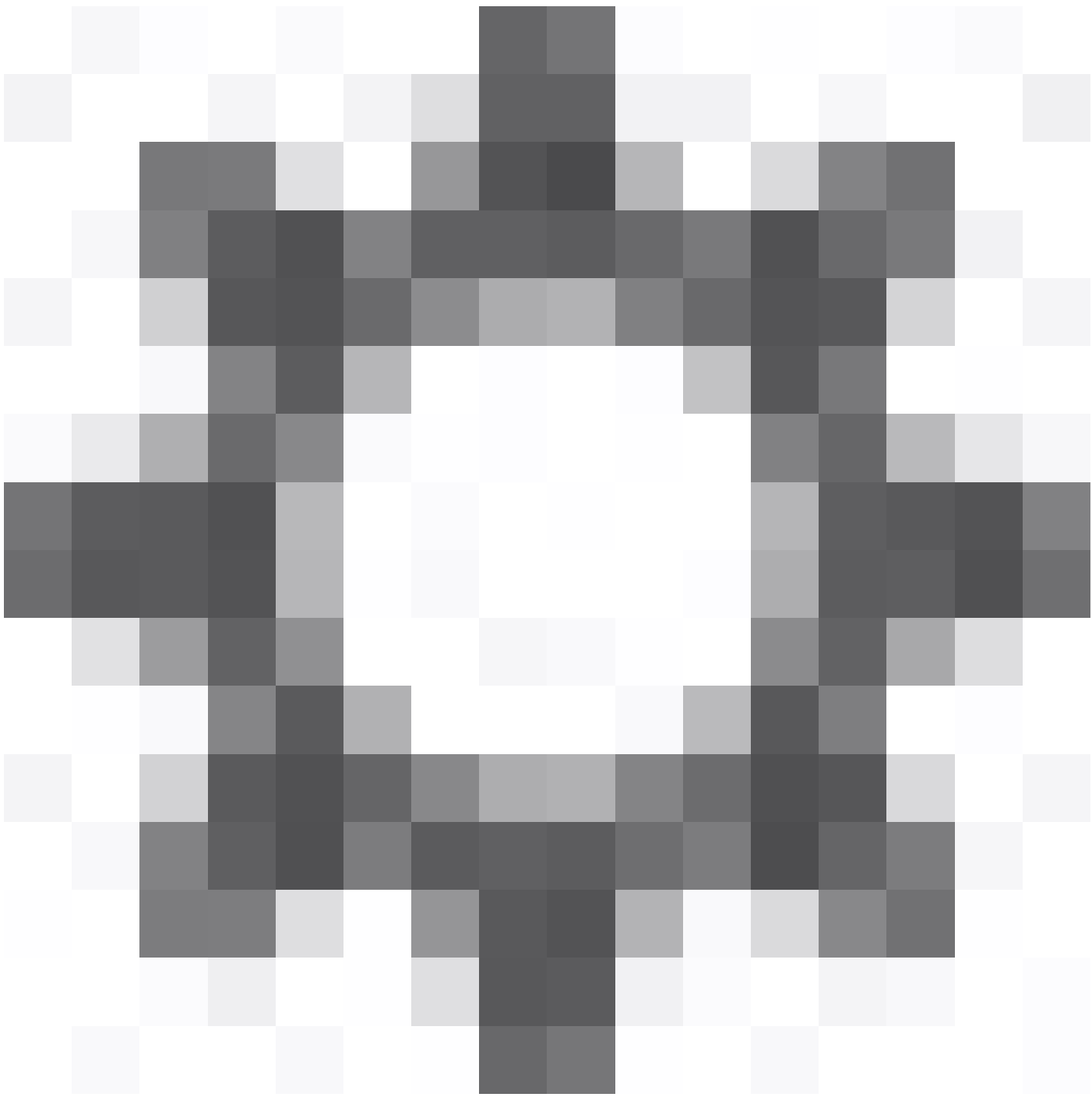
```
> expert
admin@fmc:~$ sudo su
Password:
root@fmc:/Volume/home/admin# /etc/init.d/rpcbind start
Starting rpcbind daemon...done.
root@fmc:/Volume/home/admin# /etc/init.d/rpcbind status
/usr/sbin/rpcbind (pid 30904) is running...
root@fmc:/Volume/home/admin#
```

Start rpcbind

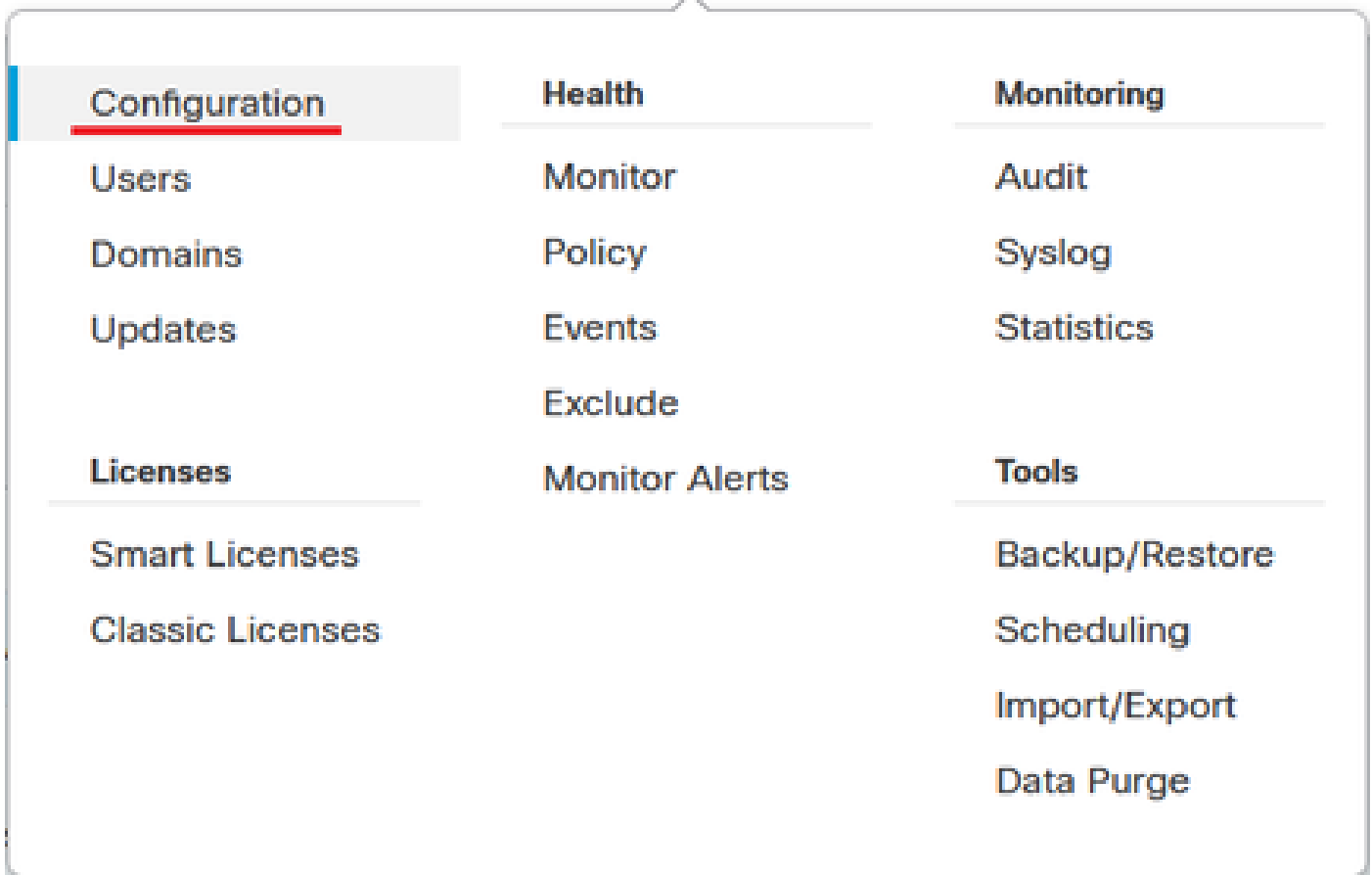


Tip: In order to avoid having to start the `rpcbind` utility in the FMC manually, check the Use Advanced Options checkbox, and fill the Command Line Option with the `-o nolock` command.

Step 2. Log in to your FMC GUI and navigate to System (

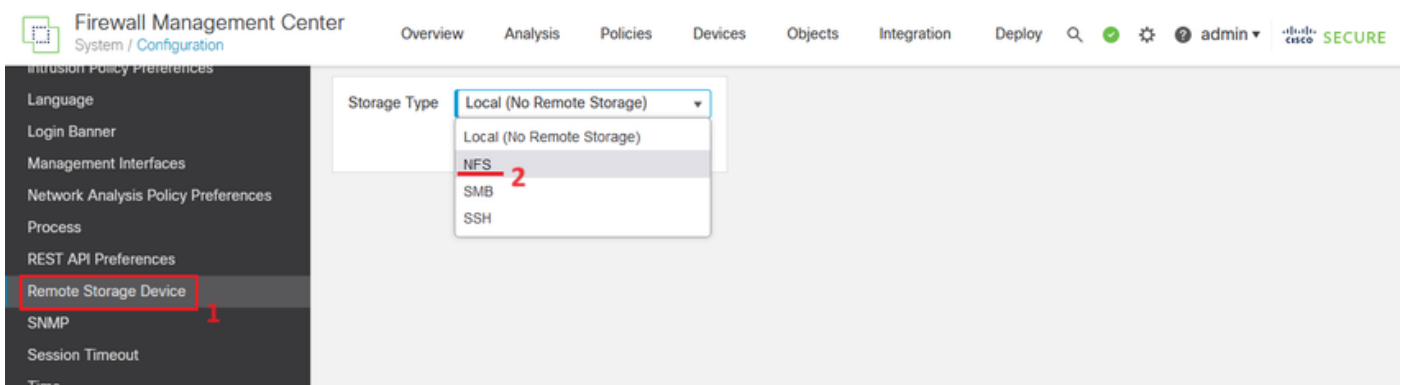


) > Configuration.



System-Configuration

Step 3. Choose Remote Storage Device and then choose **NFS** in the drop-down menu for Storage Type.



NFS Remote Storage

Step 4. Insert your NFS device information.

Enter the IPv4 address or hostname of the storage system in the **Host** field and the path to your storage area in the **Directory** field.

Check the **Use for Backups** checkbox under System Usage and click **Save**.

Storage Type

Connection

Host IP or hostname

Directory

Advanced

Use Advanced Options

System Usage

Use for Backups

Use for Reports

Disk Space Threshold %

NFS Settings

Step 5. A successful integration shows a green Success Saved Remote Storage Device configuration successfully box at the top of the page.

Firewall Management Center Configuration

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ ⓘ admin ▾

Email Notification

External Database Access

HTTPS Certificate

Information

Intrusion Policy Preferences

Language

Login Banner

Management Interfaces

Network Analysis Policy Preferences

Process

REST API Preferences

Remote Storage Device

SNMP

Session Timeout

Time

Time Synchronization

Success
 ✓ Saved Remote Storage Device configuration successfully. ✕

Storage Type

Connection

Host IP or hostname

Directory

Advanced

Use Advanced Options

System Usage

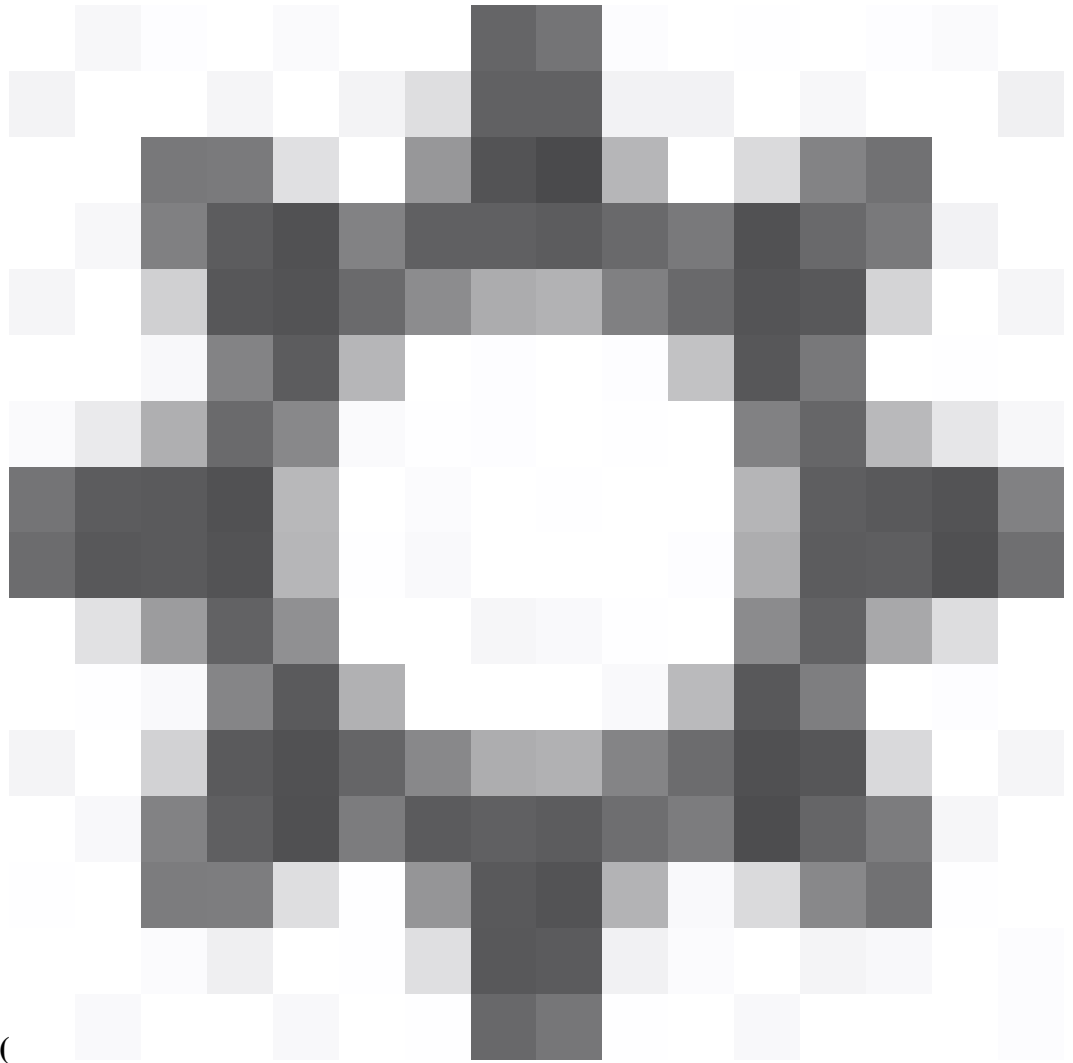
Use for Backups

Use for Reports

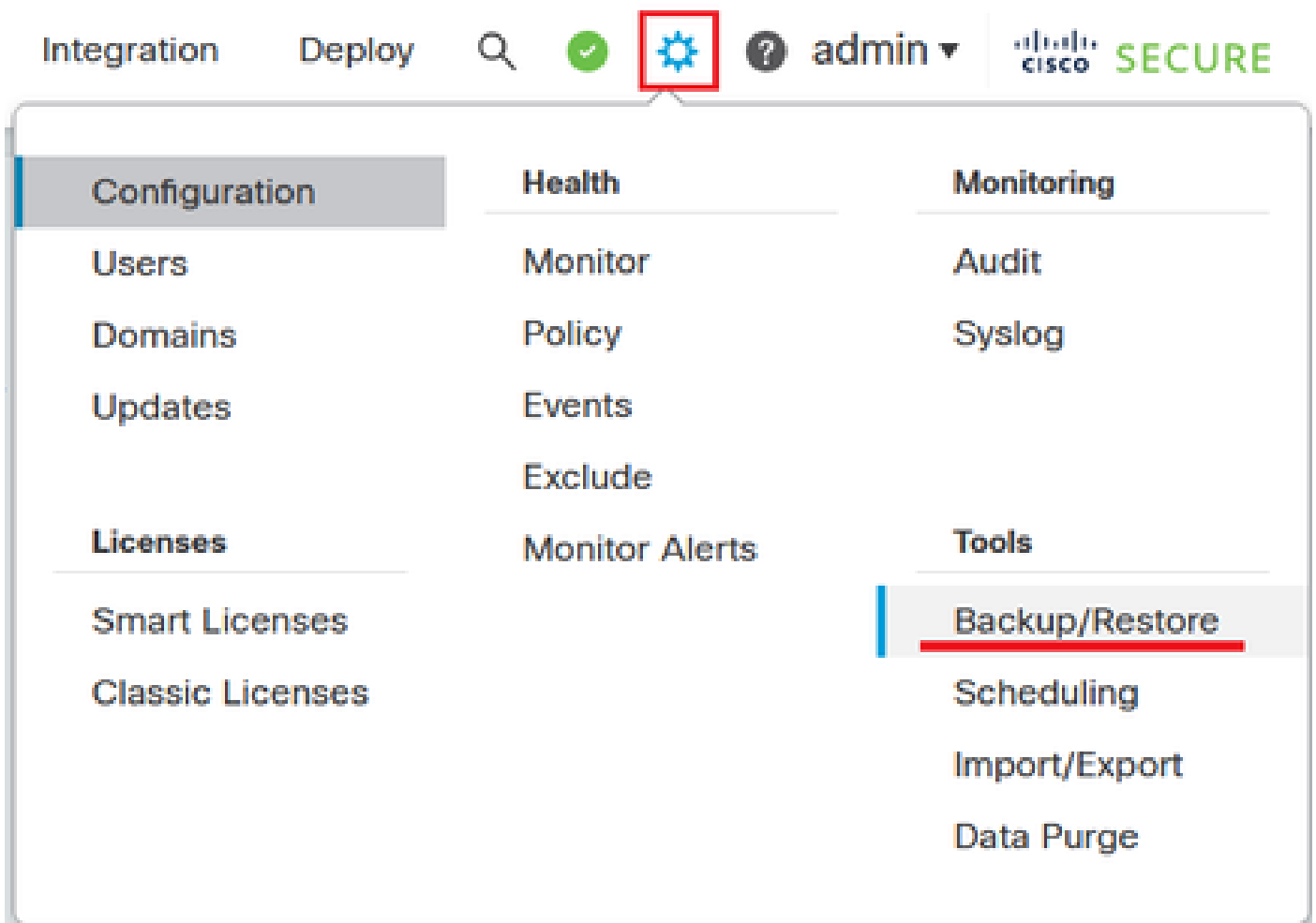
Disk Space Threshold %

Saved Remote Storage Device configuration successfully

Setup a Backup Profile

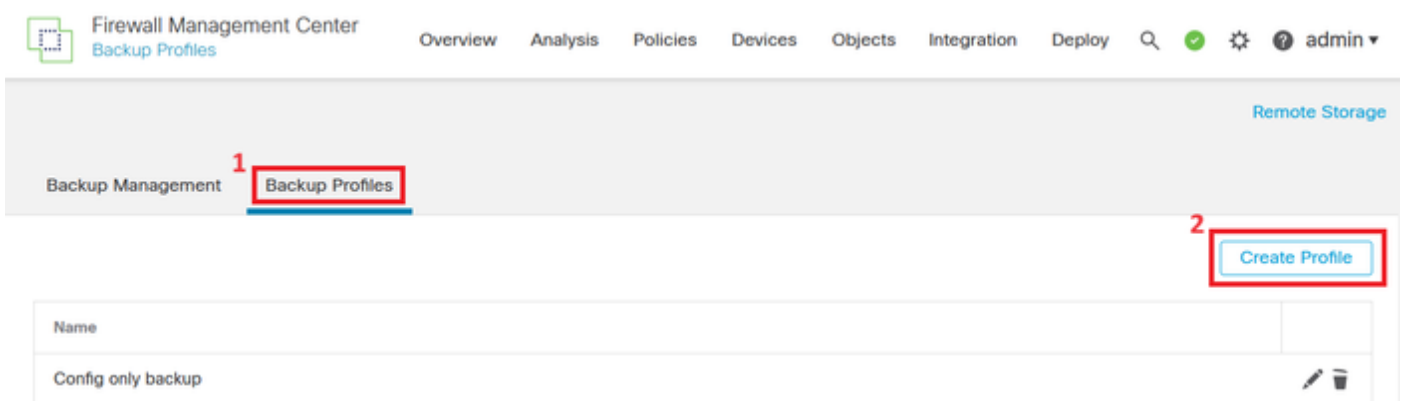


Step 1. Navigate to System (
) > Tools > Backup/Restore.



System-Tools-Backup

Step 2. Move to **Backup Profiles** and click **Create Profile**.



Create Backup Profile

Step 3. Give your profile a **Name** and check all the checkboxes for a full backup profile.

Click **Save As New**.

Create Backup

Name

Storage Location

Back Up Configuration

Back Up Events

Back Up Threat Intelligence
Director

Email Not available. You must set up your mail relay host.

Copy when complete

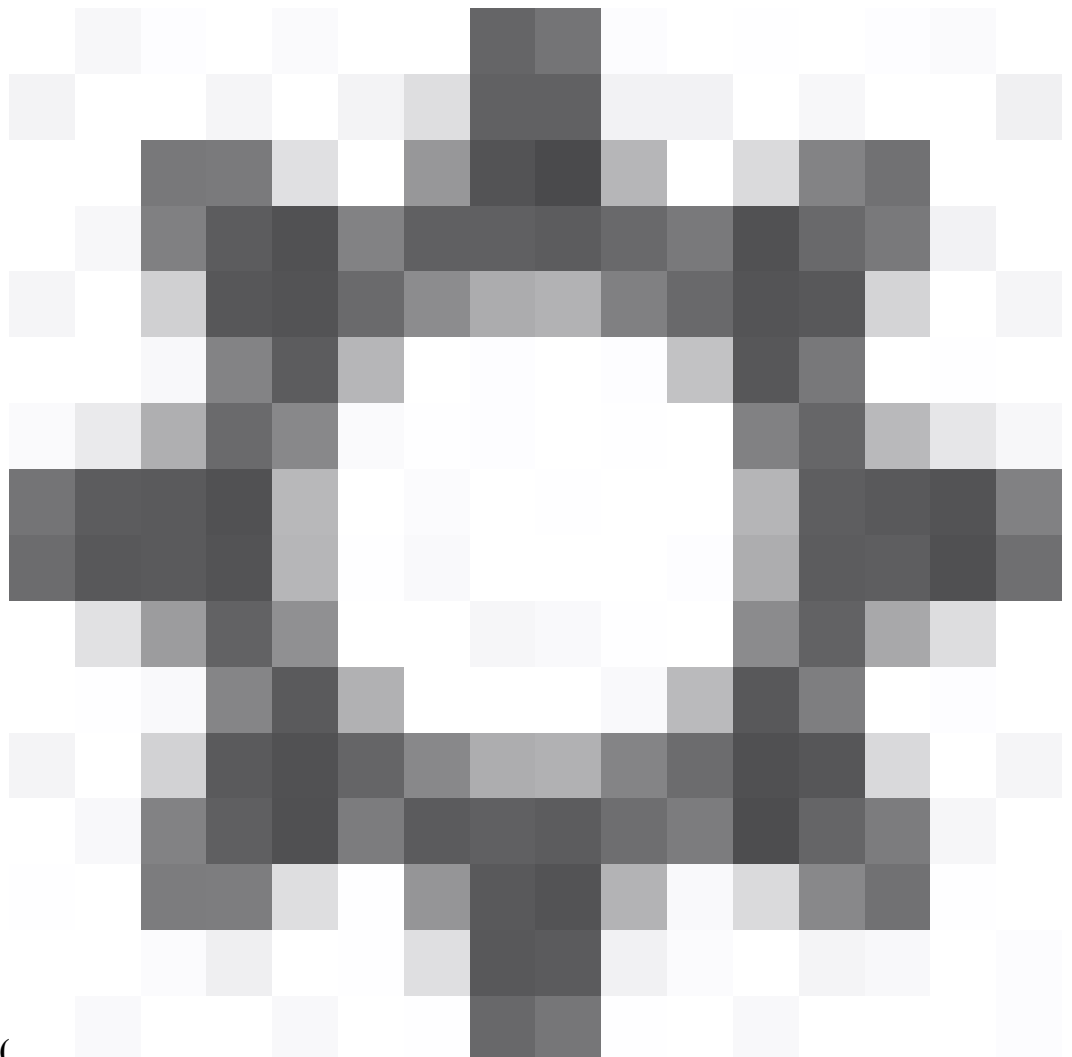
Cancel

Save As New

Start Backup

Profile Settings

Schedule a Recurring Task to Backup the FMC







Step 1. Navigate to System ()> Tools > Scheduling.

Configuration	Health	Monitoring
Users	Monitor	Audit
Domains	Policy	Syslog
Updates	Events	Statistics
	Exclude	
Licenses	Monitor Alerts	Tools
Smart Licenses		Backup/Restore
Classic Licenses		<u>Scheduling</u>
		Import/Export
		Data Purge

Scheduling

Step 2. Click **Add a Task**.

Firewall Management Center
Scheduling

Overview Analysis Policies Devices Objects Integration Deploy     admin ▾

Add Task Today

Add Task

Step 3. Set the schedule as needed and pick **Recurring** as the Schedule task in order to run, and **Management Center** as your Backup Type.

For demonstration purposes, this backup task starts on September 2023 and repeats once a month at 3:00 am every 29th of the month.

Choose the **Backup Profile** you created earlier and click **Save**.

New Task

Job Type

Schedule task to run Once Recurring

Start On America/New York

Repeat Every Hours Days Weeks Months

Run At

Repeat On Day of the Month

Job Name

Backup Type Management Center Device

Backup Profile

Comment

Email Status To Not available. You must set up your mail relay host.

New Task

Step 4. Once saved, you are placed back into your calendar and the new scheduled task is shown under the day you have chosen.

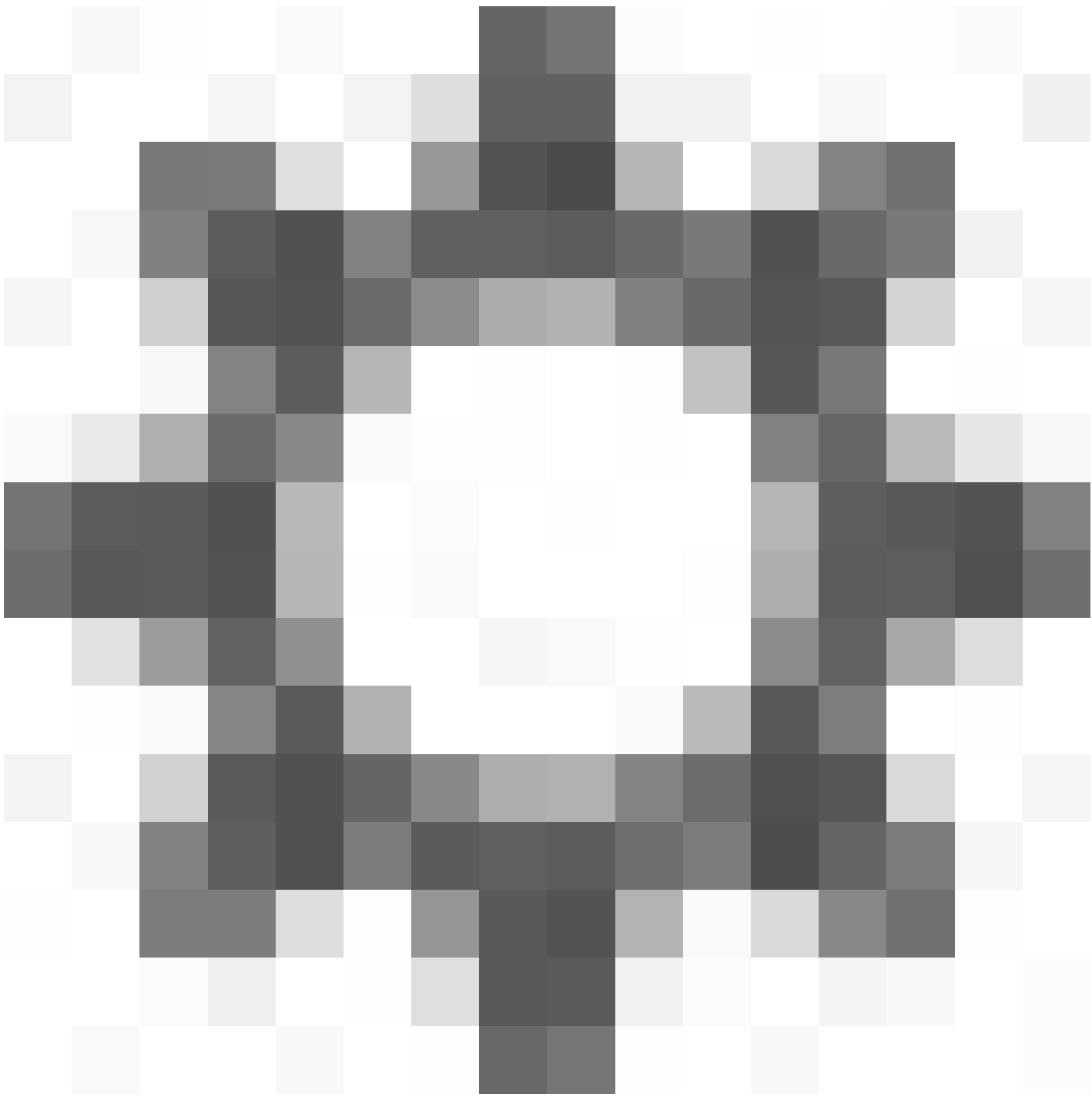


Sun.	Mon.	Tues.	Wed.	Thurs.	Fri.	Sat.
					1	2 Weekly Software Download
3 Weekly config only backup	4	5	6	7	8	9 Weekly Software Download
10 Weekly config only backup	11	12	13	14	15	16 Weekly Software Download
17 Weekly config only backup	18	19	20	21	22	23 Weekly Software Download
24 Weekly config only backup	25	26	27	28	29 Monthly Full Backup	30 Weekly Software Download

Calendar

Schedule a Recurring Task to Backup the FTD

Step 1. Navigate to System (







) > Tools > Scheduling.

Configuration	Health	Monitoring
Users	Monitor	Audit
Domains	Policy	Syslog
Updates	Events	Statistics
	Exclude	
Licenses	Monitor Alerts	Tools
Smart Licenses		Backup/Restore
Classic Licenses		<u>Scheduling</u>
		Import/Export
		Data Purge

Scheduling

Step 2. Click **Add a Task**.

Firewall Management Center
Scheduling

Overview Analysis Policies Devices Objects Integration Deploy     admin ▾

Add Task Today

Add Task

Step 3. Pick **Recurring** as the Scheduled task in order to run and set the schedule as needed.

For demonstration purposes, this backup task starts on September 2023 and repeats once a month at 4:00 am every 29th of the month.

Insert a **Job Name**.

New Task

Job Type

Schedule task to run Once Recurring

Start On America/New York

Repeat Every Hours Days Weeks Months

Run At

Repeat On Day of the Month

Job Name

Backup Type Management Center Device

Backup Profile

Comment

Email Status To Not available. You must set up your mail relay host.

New Task

Step 3.1. Choose **Device** as the Backup Type and click the device that must be backed up recurrently.

Check the Retrieve to Management Center checkbox and click **Save**.

New Task

Job Type

Schedule task to run Once Recurring

Start On America/New York

Repeat Every Hours Days Weeks Months

Run At

Repeat On Day of the Month

Job Name

Backup Type Management Center Device

Device(s)

FTD_192.168.192.102

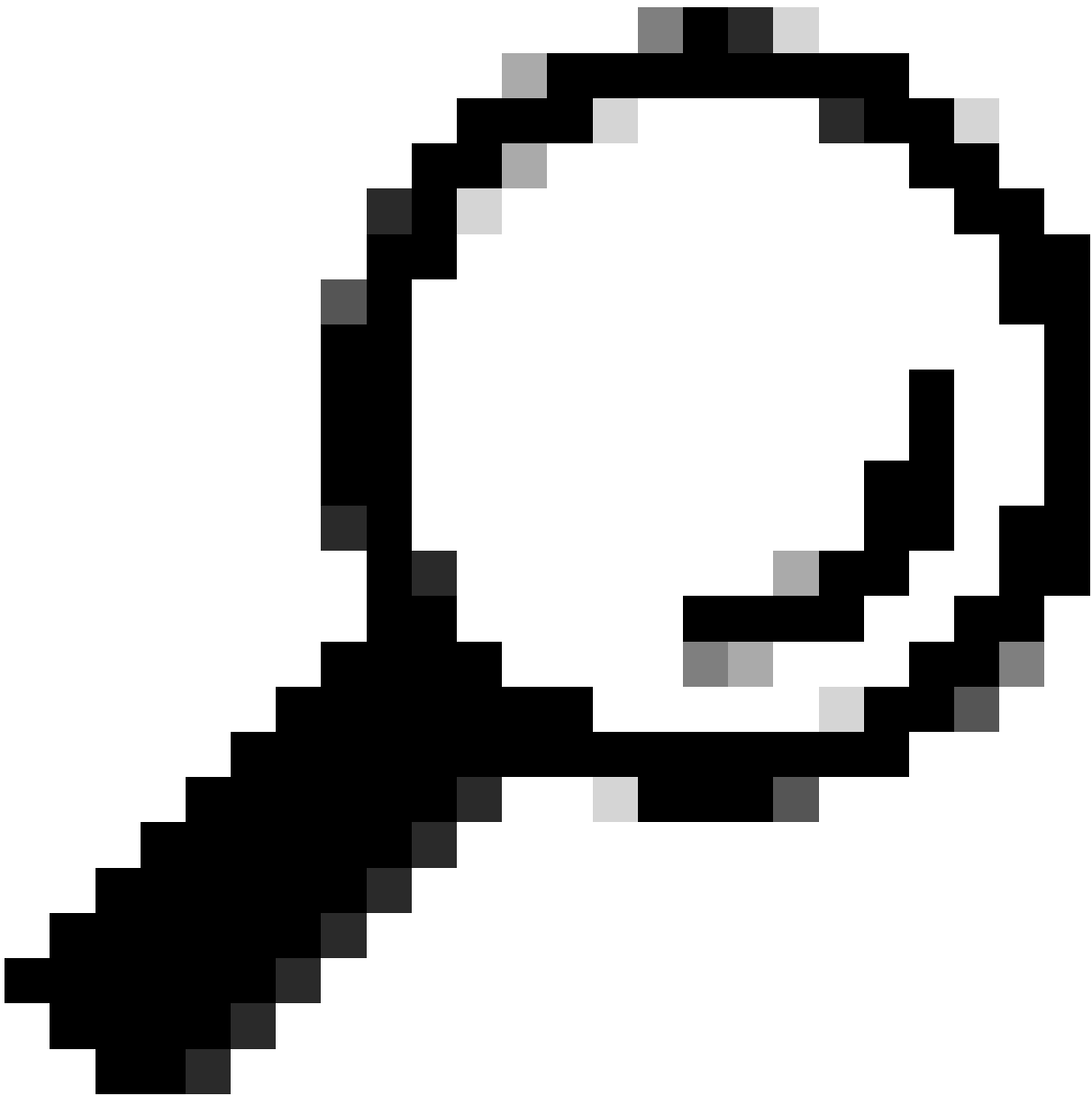
vFTD_192.168.192.83

Note: Backup the Firepower 9300/ 4100 chassis configuration before initiating a backup of the logical Threat Defense devices configured on it.

Retrieve to Management Center

Comment

Email Status To Not available. You must set up your mail relay host.



Tip: You can choose more than one device by pressing the Shift key while clicking over the other device(s).

Step 4. Once saved, you are placed back into your calendar and the new scheduled task is shown under the day you have chosen.

Sun.	Mon.	Tues.	Wed.	Thurs.	Fri.	Sat.
					1	2 Weekly Software Download
3 Weekly config only backup	4	5	6	7	8	9 Weekly Software Download
10 Weekly config only backup	11	12	13	14	15	16 Weekly Software Download
17 Weekly config only backup	18	19	20	21	22	23 Weekly Software Download
24 Weekly config only backup	25	26	27	28	29 Monthly Full Backup FTD102 MonthlyBackup	30 Weekly Software Download

Calendar

Troubleshooting

- Verify that the FMC can reach the Remote Storage device. Open an SSH session to the FMC, navigate to the expert mode, and elevate to sudo rights. Send a ping to the remote storage device.

```
> expert
admin@fmc:~$ sudo su
Password:
root@fmc:/Volume/home/admin# ping 192.168.192.76
PING 192.168.192.76 (192.168.192.76) 56(84) bytes of data.
64 bytes from 192.168.192.76: icmp_seq=1 ttl=128 time=3.02 ms
64 bytes from 192.168.192.76: icmp_seq=2 ttl=128 time=0.444 ms
64 bytes from 192.168.192.76: icmp_seq=3 ttl=128 time=0.754 ms
64 bytes from 192.168.192.76: icmp_seq=4 ttl=128 time=1.07 ms
64 bytes from 192.168.192.76: icmp_seq=5 ttl=128 time=0.585 ms
^C
--- 192.168.192.76 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 21ms
rtt min/avg/max/mdev = 0.444/1.174/3.020/0.946 ms
root@fmc:/Volume/home/admin#
```

Ping test

- The logs of the backup task are stored in the FMC filename `/var/log/backup.log`. If an error occurred and the task did not finish successfully, you can search here for an error or failure.

```
root@fmc:/Volume/home/admin#
root@fmc:/Volume/home/admin# less /var/log/backup.log
```

less command

```

Fri Sep 29 17:09:25 2023 Mounted and chdir: /mnt/remote-storage/sf-storage/c57c072e-ed75-11ec-aeec-c53595860d06/backups
Fri Sep 29 17:09:25 2023 Parent Process ID ... 14353
Fri Sep 29 17:09:26 2023 *****
Fri Sep 29 17:09:26 2023 Backup started
Fri Sep 29 17:09:26 2023 Backup config: 1
Fri Sep 29 17:09:26 2023 Backup events: 1
Fri Sep 29 17:09:26 2023 Backup tid: 1
Fri Sep 29 17:09:26 2023 Backup initiated from FMC
Fri Sep 29 17:09:26 2023 Backup storage type : NFS

Fri Sep 29 17:09:26 2023 Entering: main::update_status
Fri Sep 29 17:09:26 2023 Update Task: Checking the database
Fri Sep 29 17:09:26 2023 Exiting: main::update_status
running database integrity check with the following options:
- use exception directory /usr/local/sf/etc/db_exceptions
- check refererences
- check enterprise objects
- check schema
- check required data
- log to stderr
getting filenames from [/usr/local/sf/etc/db_updates/index]
getting filenames from [/usr/local/sf/etc/db_updates/base-7.2.5]
***** Applying dynamic update files *****
Dynamic update files directory: /usr/local/sf/etc/dynamic_db_updates
Applying file remove_ref_check_rna_ip_os_map.yaml.
Status: Success.
Applying file rule-comments.yaml.
/Backup started

```

backup.log

- This file can also be found in the FTD when it has run a backup task. Find it under **/ngfw/var/log/backup.log**.

```

> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin# less /ngfw/var/log/backup.log

```

Less command

```

Fri Sep 29 17:09:25 2023 Mounted and chdir: /mnt/remote-storage/sf-storage/c57c072e-ed75-11ec-aeec-c53595860d06/backups
Fri Sep 29 17:09:25 2023 Parent Process ID ... 14353
Fri Sep 29 17:09:26 2023 *****
Fri Sep 29 17:09:26 2023 Backup started
Fri Sep 29 17:09:26 2023 Backup config: 1
Fri Sep 29 17:09:26 2023 Backup events: 1
Fri Sep 29 17:09:26 2023 Backup tid: 1
Fri Sep 29 17:09:26 2023 Backup initiated from FMC
Fri Sep 29 17:09:26 2023 Backup storage type : NFS

Fri Sep 29 17:09:26 2023 Entering: main::update_status
Fri Sep 29 17:09:26 2023 Update Task: Checking the database
Fri Sep 29 17:09:26 2023 Exiting: main::update_status
running database integrity check with the following options:
- use exception directory /usr/local/sf/etc/db_exceptions
- check refererences
- check enterprise objects
- check schema
- check required data
- log to stderr
getting filenames from [/usr/local/sf/etc/db_updates/index]
getting filenames from [/usr/local/sf/etc/db_updates/base-7.2.5]
***** Applying dynamic update files *****
Dynamic update files directory: /usr/local/sf/etc/dynamic_db_updates
Applying file remove_ref_check_rna_ip_os_map.yaml.
Status: Success.
Applying file rule-comments.yaml.
/Backup started

```

backup.log

- FTD logs show the backup file is stored locally however, in the end, it is sent to the FMC and then to the remote storage device.

```
Fri Sep 29 17:24:50 2023 Update Task: Copying backup from remote.
Fri Sep 29 17:24:50 2023 Exiting: main::update_status
Fri Sep 29 17:24:50 2023 Entering: main::update_status
Fri Sep 29 17:24:50 2023 Update Task: Copying backup to Firepower Management Center
Fri Sep 29 17:24:50 2023 Exiting: main::update_status
Fri Sep 29 17:24:59 2023 FTD_192.168.192.102_20230929132338.tar
Fri Sep 29 17:24:59 2023 Entering: main::update_status
Fri Sep 29 17:24:59 2023 Update Task: Backup complete, Retrieval to Firepower Management Center successful
Fri Sep 29 17:24:59 2023 Exiting: main::update_status
Fri Sep 29 17:25:00 2023 Sending SIGUSR1 to process 29582 to notify of success
Fri Sep 29 17:25:00 2023 Received success notification from sf-backup-inator
Fri Sep 29 17:25:07 2023 Exiting... (0)
(END)
```

FTD logs