# **Collect Unified Backup of Secure FMC in High Availability**

#### **Contents**

Introduction

**Prerequisites** 

Requirements

Components Used

**Background Information** 

**Procedure of Collecting Backup** 

Restore Management Center from Unified Backup

#### Introduction

This document describes how to collect the unified backup on an active FMC, where a single backup file is created for both active and standby FMCs.

## **Prerequisites**

#### Requirements

Cisco recommends you have knowledge of these topics:

• Secure Firewall Management Center High Availability (FMC HA) concepts and configuration.

### **Components Used**

The information in this document is based on FMCv 7.4.2.

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**

- Unified backup is taken on an active management center, where a single backup file is created for both the active and standby management centers. The unified backup is applicable only for configuration-only backup. If eventing or TID backup is required, you must take separate backups for active and standby management centers. When you select configuration-only backup, by default, unified backup is applied. In a unified backup, if the active management center is unable to get a backup tar file from the standby management center, the normal backup file is generated for the active unit that can be used for restoration. There are several benefits of unified backup over the normal backup.
- Unified backup does not require you to take separate backups on active and standby management centers.

- Redundant data in backups and storage constraints are removed in a unified backup.
- In a normal backup, when the primary unit fails, and if a secondary unit backup is not available, you had to break the high availability pairing for the secondary RMA. This situation is eradicated in a unified backup.
- While executing unified backup, you do not have to pause the HA synchronization to perform backup on the standby unit.

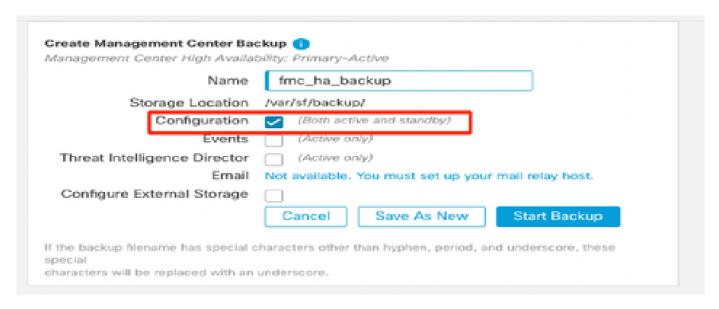
## **Procedure of Collecting Backup**

- Log into the management center and select **System > Tools > Backup/Restore**.
- The Backup Management page lists all locally and remotely stored backup files including the unified backup file (configuration-only).



Backup Management

• Enter the backup name and click Start Backup.



Create Backup

Name	fmc_ha_backup
Storage Location	/var/sf/backup/
Configuration	(Both active and standby)
Events	(Active only)
Threat Intelligence Director	(Active only)
Email	Not available. You must set up your mail relay host.
Configure External Storage	
	Cancel Save As New Start Backup

Start Backup

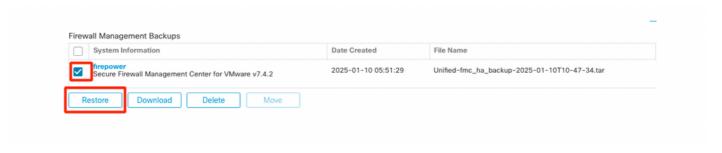
• Backup completed successfully. The file is stored locally.



Backup File Name

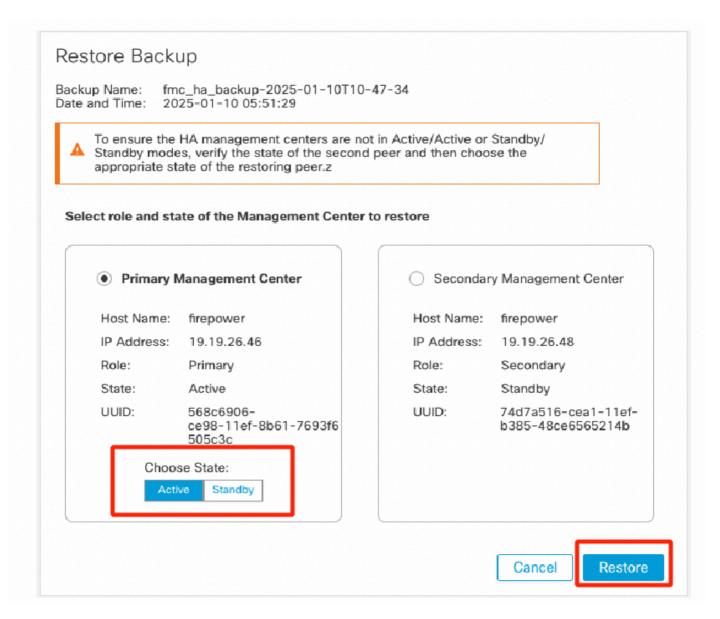
#### **Restore Management Center from Unified Backup**

- Log into the management center you want to restore and select **System > Tools > Backup/Restore.**
- The Backup Management page lists all locally and remotely stored backup files including the unified backup file (configuration-only).
- If the unified backup file is not in the list and you have it saved on your local computer, click **Upload Backup**.
- Select the unified backup file that you want to restore and click **Restore**.



Restore File

• In the **Restore Backup** page, select which unit you want to restore. Because the unified backup stores the backup configuration of both primary and secondary management centers, you need to choose which unit you want to restore.



Choose the Correct State

- To select the state of the restored management center, click the **Active or Standby** radio button. You must verify the role and state of your working management center to avoid having both peers with same role and state configuration. Choosing the incorrect role and state for your management center when restoring can cause HA failure.
- Pause the **HA sync** before restoring the backup.
- Click **Restore**, and then **Confirm Restore** to begin the restoration.

## Confirm Restore

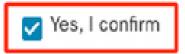


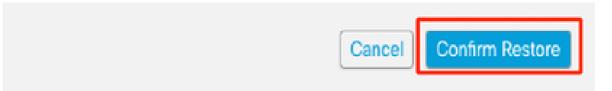


You have selected Primary role and Active state.

Choosing an incorrect role and state for your management center during restoration can result in HA failure.

Make sure you verify the role and state of your working management center to avoid having both peers with same role and state configuration.





Confirm Restore

- You can check the restoration status from the **Message Center > Tasks**.
- Restore (On Demand)

Restore File: Unified-fmc\_ha\_backup-2025-01-10T10-47-34.tar Restore Complete

1m 28s 🗙

Restore Complete