Contents

Introduction

This document describes how to configure Backup/Restore of configuration/events in FirePOWER module using ASDM (On-Box Management)

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of ASA (Adaptive Security Appliance) firewall, ASDM (Adaptive Security Device Manager)
- FirePOWER appliance Knowledge.
- Ensure that Firepower module tab is available in the ASDM configuration.

Components Used

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

- ASA FirePOWER modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) running software version 5.4.1 and above

- ASA FirePOWER module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) running software version 6.0.0 and above

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, make sure that you understand the potential impact of any command.

Background Information

Backup/Restore are primarily useful tasks that an administrator does on regular basis. It helps to restore the firepower module to an operational state after an accident (also called disaster recovery) and module corruption (file or data recovery

Firepower module provides two options for the backup and the restore:

1. ASDM allows you to take the configuration backup where backup can be restored to the same model in the case of disaster recovery/data corruption.
2. Firepower Management Center (FMC) allows Import/Export option which in turn allows the backup of several part of configuration. This includes all types of policies as you can import the exported policies to both same as well as different model with the same version. You can also choose this option to migrate the configuration of one module to another module.

Backup/Restore Configuration

Firepower module can perform the backup to either its own hard drive or remote device.

> **Note**: Firepower module supports only the configuration backup.

Configure the Local Backup/ Remote Backup

In order to take the local backup of Firepower module, navigate to **Configuration > ASA Firepower Configuration > Tools > Backup/ Restore > Backup Management and** click **Device Backup**.

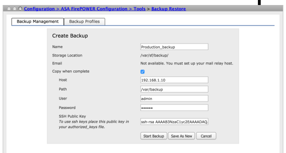
Name: Specify the name of backup.

Storage Location: ASDM support only local storage which is **/var/sf/backup.**

Email: Enable the email notification. you need to configure the System Policy (**ASA Firepower Configuration > SystemPolicy**) for email relay server configuration.

Copy when Complete: Enable the check box to configure **Remote Backup**. Firepower uses the SCP protocol to send the backup to the backup server.

- **Host:** Specify the IP/ Host of the remote server
- **Path:** Specify the remote directory path
- **User:** Specify the remote username
- **Password:** Specify the remote username's password


Configuration > ASA FirePOWER Configuration > Tools > Backup Restore
Backup Management
Backup Profiles
Start Backup
Save As New
Cancel

Create Backup

Name: Production_backup
Storage Location: /var/sf/backup/
Email: Not available. You must set up your mail relay host.
Copy when complete: ☑
Host: 192.168.1.10
Path: /var/backup
User: admin
Password: ••••••
SSH Public Key
To use ssh keys place this public key in your authorized_keys file.: ssh-rsa AAAAB3NzaC1yc2EAAAADAQ.

Click **Start Backup** option to start the backup process. **Save As New** option creates a backup profile which you can use in Backup profile.

Scheduling the Backup

You can schedule the Backup of the configuration of your device in a timely manner. Backup schedule can automate the process of backing up the device by hours/ daily/weekly/monthly timeframe. To schedule the backup, you need to perform two steps:

Step 1. Create the Backup Profile.

Step 2. Schedule the backup tasks

Create the Backup Profile

In order to create backup profile, navigate to **Configuration > ASA Firepower Configuration > Tools > Backup/ Restore > Backup Management** and c **Backup profile**.

Backup profile creation options are similar to previous section (

Schedule the backup tasks

In order to schedule the Backup tasks, navigate to **Configuration > ASA Firepower Configuration > Tools > Scheduling** and click **Add Task.**

Job Type: Select **Backup** as job type in the drop down list.

Schedule Task to run: Select the radio button to define the frequency of task to be scheduled.

Start On: Select Date from the drop down list to define the start date of the backup.

Repeat Every: Specify frequency of iteration of the backup scheduling task on Hours/ Days/ Weeks/ Monthly basis.

Run At: Select the time of start of the backup from the drop down list.

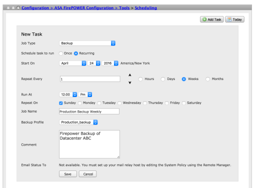
Repeat On: Select the checkbox for the day on which you want to repeat the backup.

Job Name: Specify the name of scheduled job.

Backup Profile: Select the **Backup profile** you have created in the earlier step from the drop down list.

Comment: You can write the description about the job you have created.

Email Status To: You can setup email relay host to send the status of scheduled job backup.



Configuration > ASA FirePOWER Configuration > Tools > Scheduling

New Task

Job Type: Backup

Schedule task to run: ○ Once ● Recurring

Start On: April 24 2016 America/New York

Repeat Every: 1 ○ Hours ○ Days ● Weeks ○ Months

Run At: 12:00 Pm

Repeat On: ☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Job Name: Production Backup Weekly

Backup Profile: Production_backup

Comment: Firepower Backup of Datacenter ABC

Email Status To: Not available. You must set up your mail relay host by editing the System Policy using the Remote Manager.

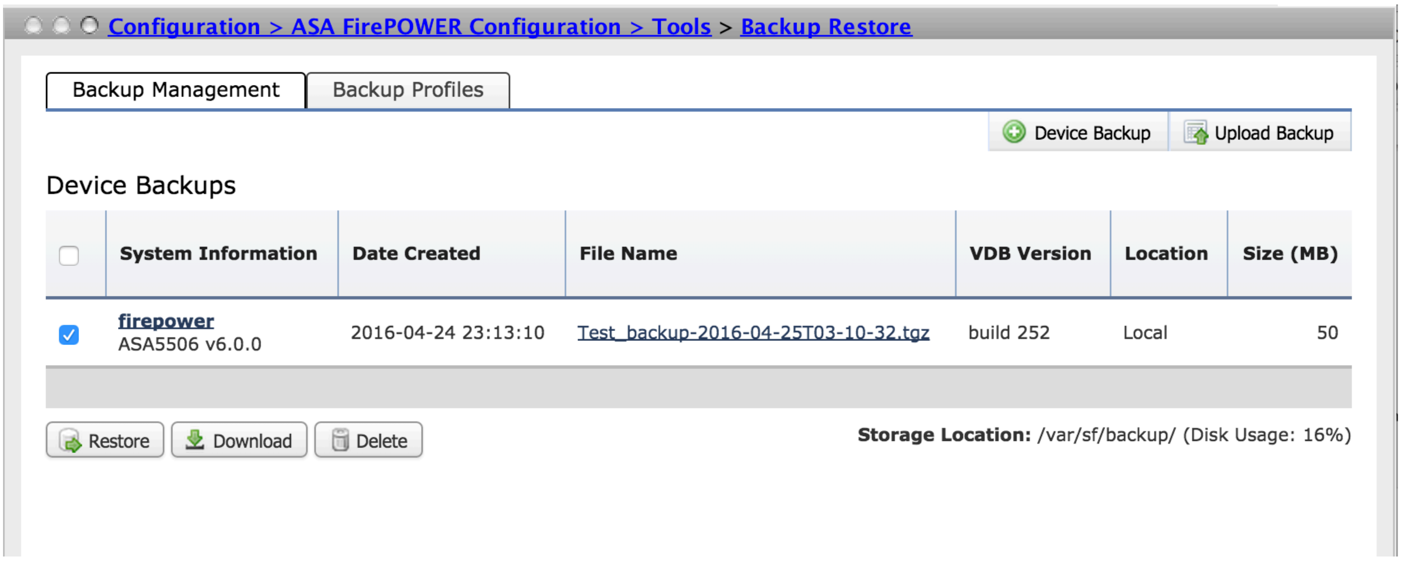
Click **Save** button to save the configuration of the scheduled backup.

Configure the Backup's Restore

Restoration of backup is needed if your device configuration is corrupted or you have reimaged the appliance. You can restore the old configuration to the freshly reimaged appliance.

To restore the backup, navigate to **Configuration > ASA Firepower Configuration > Tools > Backup/ Restore**. If you have configured the remote storage then fetch the backup file from remote storage and choose option **Upload Backup** to upload the backup file.

Uploaded file or already created backup files are available at **Backup Management** page**.** Choose the backup file you want to restore and click **Restore** option to start the restoration backup.



Device Backups

☐	System Information	Date Created	File Name	VDB Version	Location	Size (MB)
☑	firepower ASA5506 v6.0.0	2016-04-24 23:13:10	Test_backup-2016-04-25T03-10-32.tgz	build 252	Local	50

Storage Location: /var/sf/backup/ (Disk Usage: 16%)

Once you click **Restore**, it asks for confirmation to replace configuration data. Click **Restore** again to continue with the restoration process.

Import/ Export Configuration

Firepower module supports the Import/Export feature which is used to copy various type of configurations. This includes policies from one module to another module of the same/ different type.

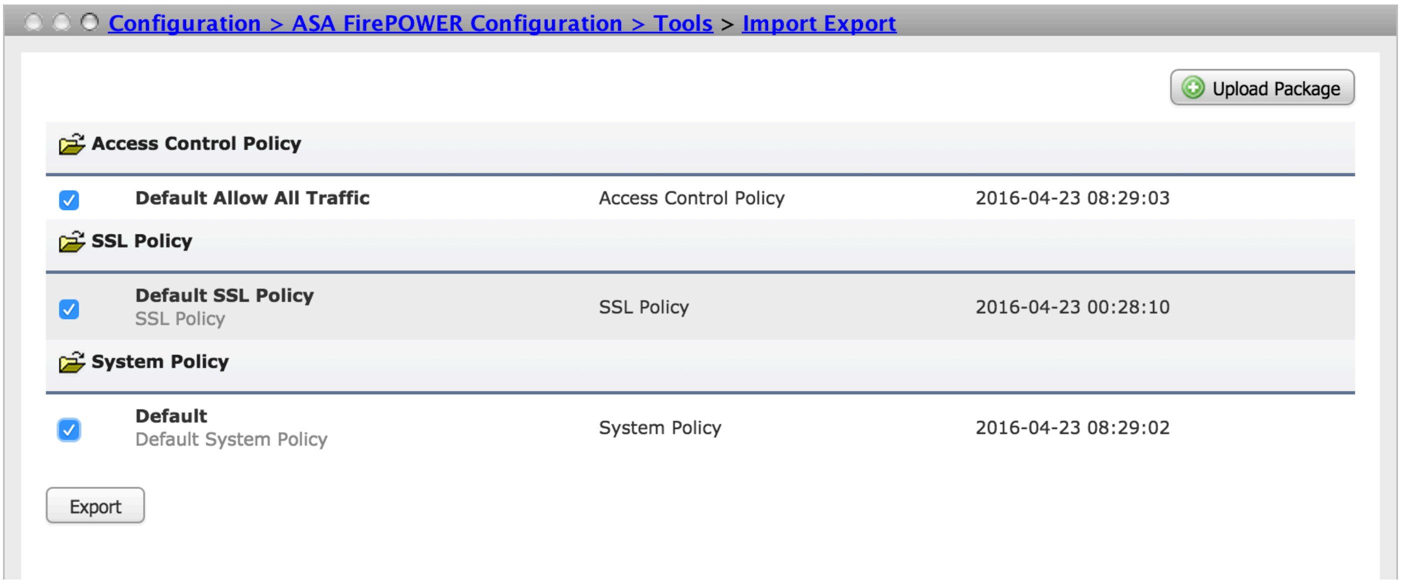
It supports export and import of below types of policies:

- Access Control policies including network analysis and file policies
- Intrusion policies
- System policies
- Alert responses.

Exporting Configuration

In order to export the configuration, navigate to **Configuration > ASA Firepower Configuration > Tools > Import/Export**.

Firepower module supports export of single policy or set of policies of the same type or different type at a single time along with revision number of that configuration.

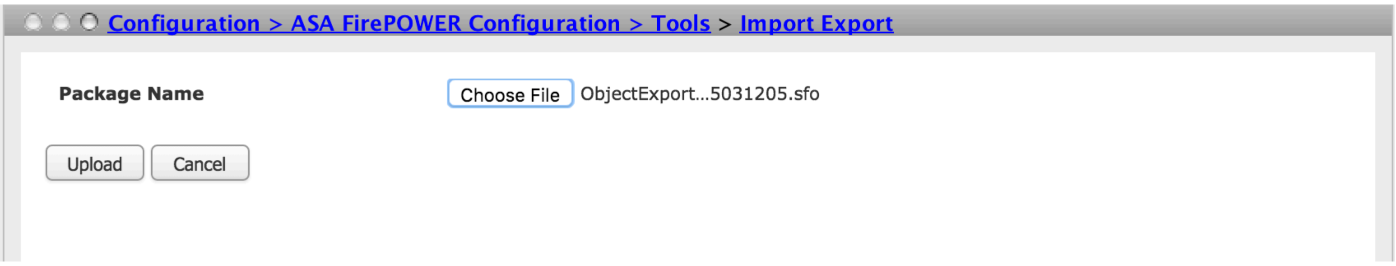

Configuration > ASA FirePOWER Configuration > Tools > Import Export
Upload Package
Export

Access Control Policy			
☑	**Default Allow All Traffic**	Access Control Policy	2016-04-23 08:29:03
SSL Policy			
☑	**Default SSL Policy** SSL Policy	SSL Policy	2016-04-23 00:28:10
System Policy			
☑	**Default** Default System Policy	System Policy	2016-04-23 08:29:02

Click the **Export** button to export the policies. Firepower module asks to save the export file (***.sfo**)

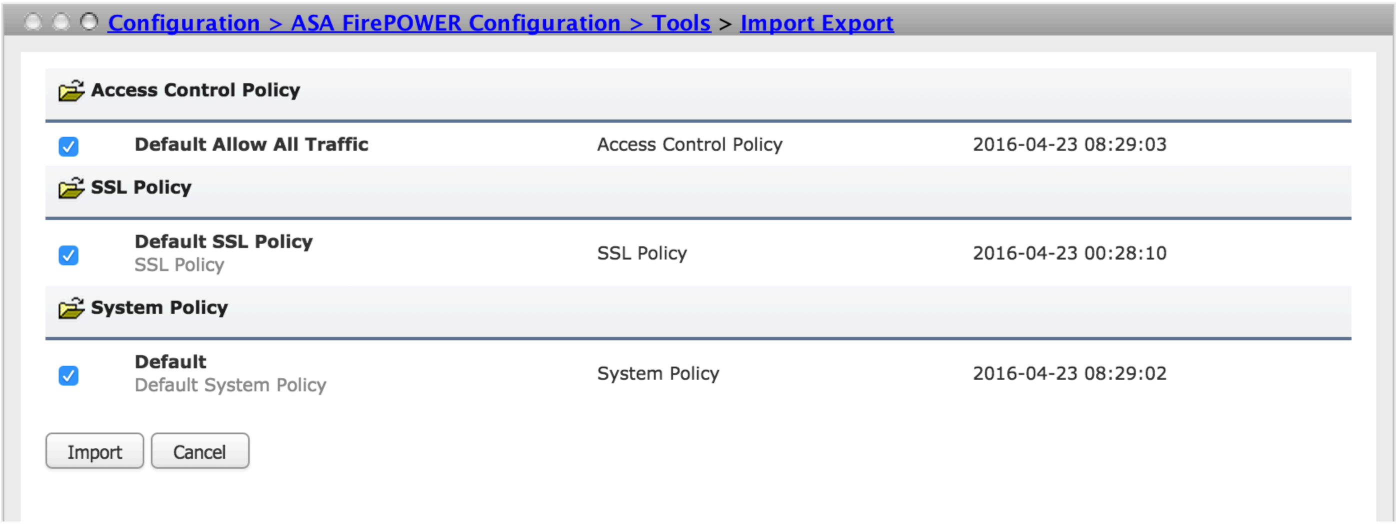
Importing Configuration

In order to Import the saved exported file on ASDM, navigate to **Configuration > ASA Firepower Configuration > Tools > Import/Export** and click on **Upload Package**. It asks you to choose the file that you want to import and click **Upload**.


Configuration > ASA FirePOWER Configuration > Tools > Import Export
Choose File
Upload
Cancel

Package Name ObjectExport...5031205.sfo

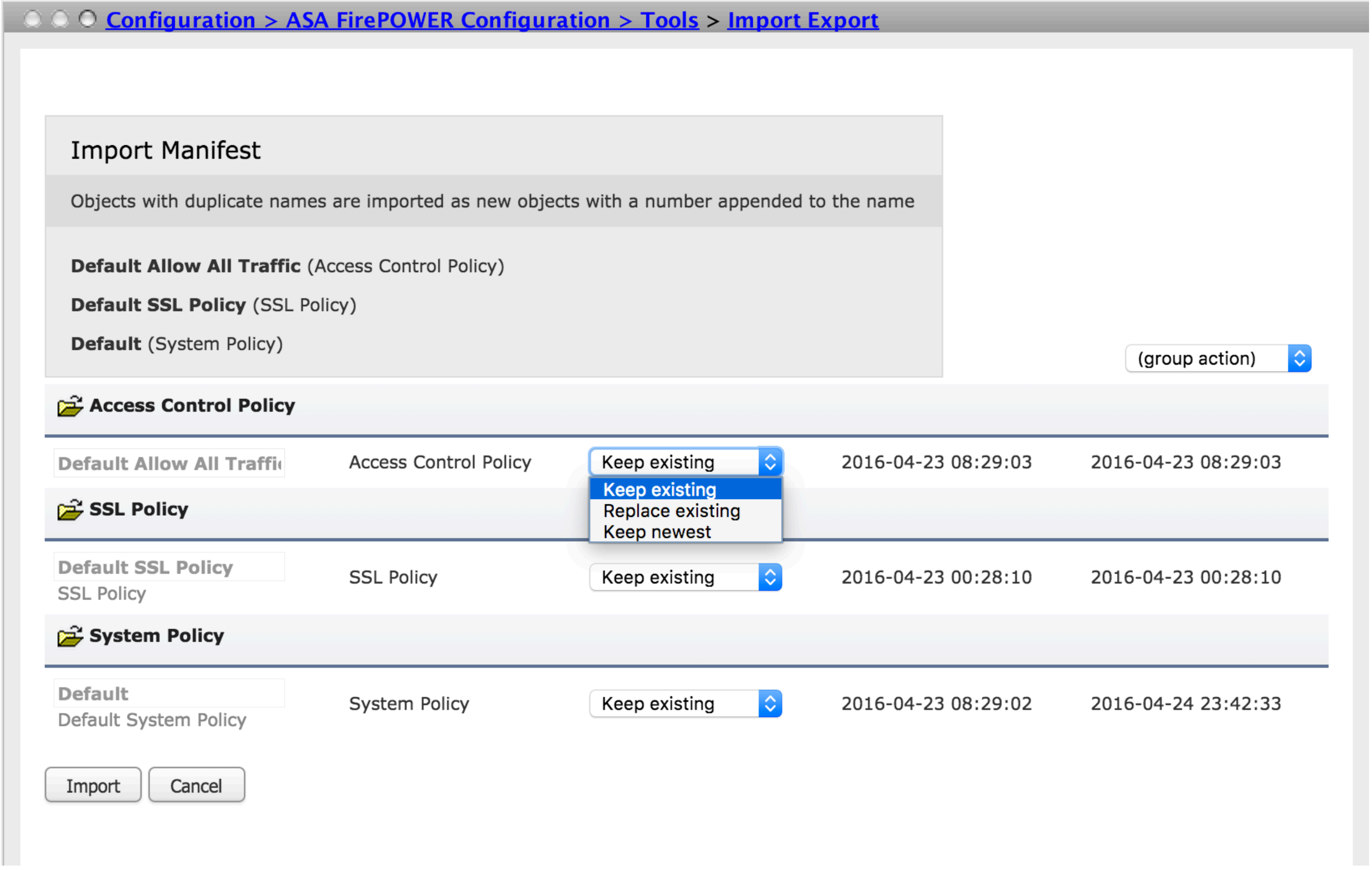
On next page, you will see policies from imported file (***.sfo**), select the policies you want to import on firepower module.


Configuration > ASA FirePOWER Configuration > Tools > Import Export
Import
Cancel

Access Control Policy			
☑	**Default Allow All Traffic**	Access Control Policy	2016-04-23 08:29:03
SSL Policy			
☑	**Default SSL Policy** SSL Policy	SSL Policy	2016-04-23 00:28:10
System Policy			
☑	**Default** Default System Policy	System Policy	2016-04-23 08:29:02

Click the **Import** button to import the policies. If the exported policy name conflicts with policies which exists in the Firepower Module. Firepower module gives these options:

- **Keep Existing:** This option allows to keep the existing policies and do not allow to import new policy
- **Replace Existing:** This option allows to replace the existing policies
- **Keep Newest:** This option checks the time into both (existing and imported) policies and keeps the policy which has more recent changes



Configuration > ASA FirePOWER Configuration > Tools > Import Export

Import Manifest

Objects with duplicate names are imported as new objects with a number appended to the name

Default Allow All Traffic (Access Control Policy)

Default SSL Policy (SSL Policy)

Default (System Policy)

(group action)

Access Control Policy

Default Allow All Traffi	Access Control Policy	Keep existing	2016-04-23 08:29:03	2016-04-23 08:29:03

SSL Policy

Default SSL Policy SSL Policy	SSL Policy	Keep existing	2016-04-23 00:28:10	2016-04-23 00:28:10

System Policy

Default Default System Policy	System Policy	Keep existing	2016-04-23 08:29:02	2016-04-24 23:42:33

Click the **Import** button to import the exported policy.

Troubleshoot

Step 1. Login to module Command-Line Interface (CLI) and check the network connectivity to remote server using Telnet and Ping command.

Step 2. Verify the permission of Secure Copy (SCP) user on the remote directory wherein the backup is stored.

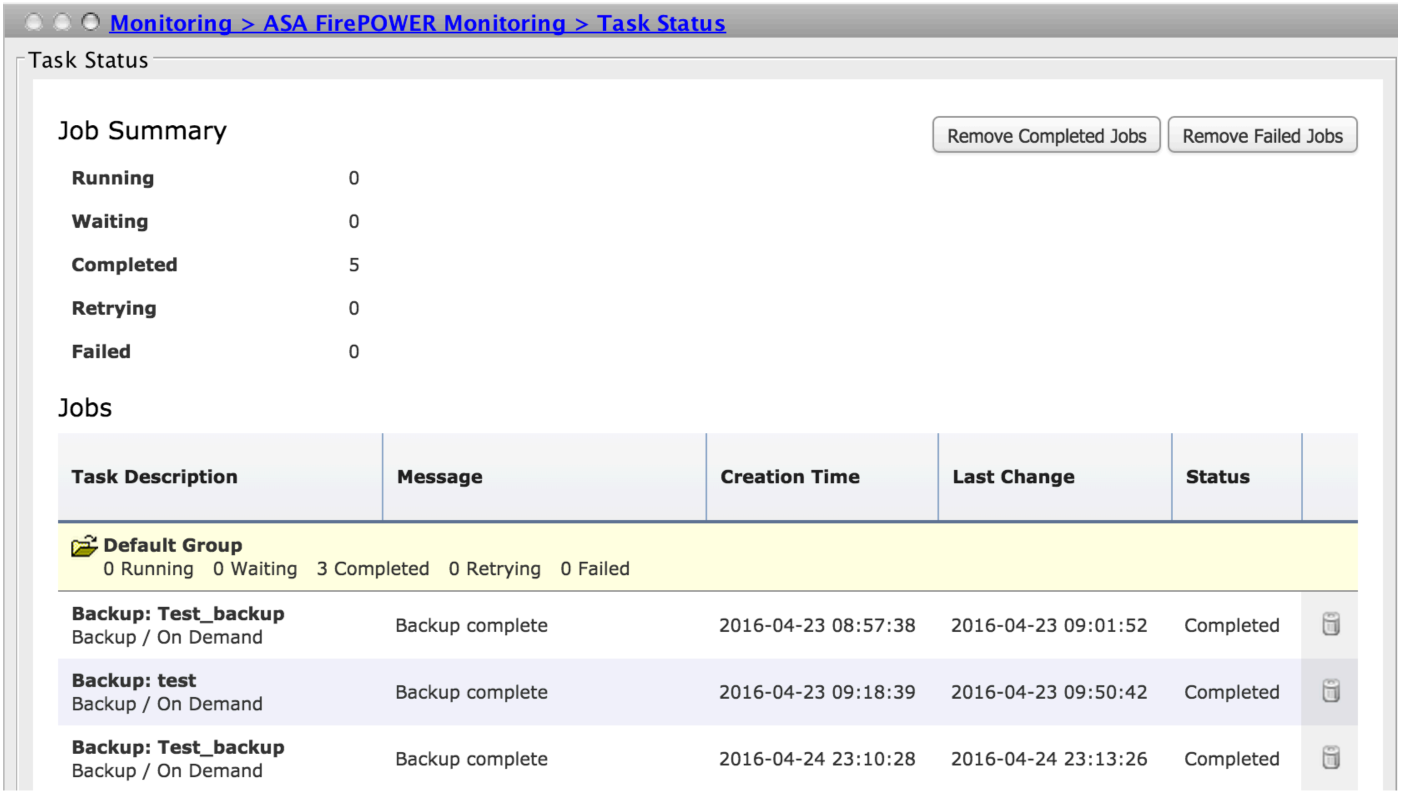
Step 3. The ASA FirePOWER module uses that information to determine whether you can import that configuration onto the another appliance. You cannot import a configuration revision that already exists on an appliance.

Step 4. For backup's restore, you need to ensure that you have same software version, rule update version, VDB version and hardware model.

Step 5. For Import of exported policies, you need to ensure that you have same software version, rule update version, and VDB version.

Verify

Step 1. In order to ensure that the backup/restore task are completed successfully, navigate to **Monitoring > ASA Firepower Monitoring > Task Status** to verify it.



Monitoring > ASA FirePOWER Monitoring > Task Status

Task Status

Job Summary

Running	0
Waiting	0
Completed	5
Retrying	0
Failed	0

Jobs

Task Description	Message	Creation Time	Last Change	Status	
Default Group 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
Backup: Test_backup Backup / On Demand	Backup complete	2016-04-23 08:57:38	2016-04-23 09:01:52	Completed	🗑
Backup: test Backup / On Demand	Backup complete	2016-04-23 09:18:39	2016-04-23 09:50:42	Completed	🗑
Backup: Test_backup Backup / On Demand	Backup complete	2016-04-24 23:10:28	2016-04-24 23:13:26	Completed	🗑

Step 2. Navigate to **Configuration > ASA Firepower Configuration > Tools > Backup/ Restore > Backup Management** to verify whether the backup file is created or not.

Related Information

- **Cisco ASA FirePOWER Module Quick Start Guide**
- **Technical Support & Documentation - Cisco Systems**