Configuration Import/Export

- About Configuration Import/Export, on page 1
- Setting an Encryption Key for Configuration Import/Export, on page 2
- Exporting an FXOS Configuration File, on page 3
- Scheduling Automatic Configuration Export, on page 5
- Setting a Configuration Export Reminder, on page 6
- Importing a Configuration File, on page 7

About Configuration Import/Export

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can later import that configuration file to quickly apply the configuration settings to your Firepower 4100/9300 chassis to return to a known good configuration or to recover from a system failure.

Guidelines and Restrictions

- Beginning with FXOS 2.6.1, the encryption key is now configurable. You must set the encryption key before you can export a configuration. The same encryption key must be set on the system when importing that configuration. If you modified the encryption key so that it no longer matches what was used during export, the import operation will fail. Make sure you keep track of the encryption key for each exported configuration.
- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.
- Application-specific configuration settings are not contained in the configuration file. You must use the configuration backup tools provided by the application to manage application-specific settings and configurations.
- When you import a configuration to the Firepower 4100/9300 chassis, all existing configuration on the Firepower 4100/9300 chassis (including any logical devices) are deleted and completely replaced by the configuration contained in the import file.
- Except in an RMA scenario, we recommend you only import a configuration file to the same Firepower 4100/9300 chassis where the configuration was exported.
- The platform software version of the Firepower 4100/9300 chassis where you are importing should be the same version as when the export was taken. If not, the import operation is not guaranteed to be

successful. We recommend you export a backup configuration whenever the Firepower 4100/9300 chassis is upgraded or downgraded.

- The Firepower 4100/9300 chassis where you are importing must have the same Network Modules installed in the same slots as when the export was taken.
- The Firepower 4100/9300 chassis where you are importing must have the correct software application images installed for any logical devices defined in the export file that you are importing.
- If the configuration file being imported contains a logical device whose application has an End-User License Agreement (EULA), you must accept the EULA for that application on the Firepower 4100/9300 chassis before you import the configuration or the operation will fail.
- To avoid overwriting existing backup files, change the file name in the backup operation or copy the existing file to another location.

Note You must backup the logicl APP separately as the FXOS import/export will backup only the FXOS configuration. The FXOS configuration import will cause logical device reboot and it rebuilds the device with the factory default configuration.

Setting an Encryption Key for Configuration Import/Export

When exporting configurations, FXOS encrypts sensitive data such as passwords and keys.

Beginning with FXOS 2.6.1, the encryption key is now configurable. You must set the encryption key before you can export a configuration. The same encryption key must be set on the system when importing that configuration. If you have modified the encryption key so that it no longer matches what was used during export, the import operation will fail. Make sure that you keep track of the encryption key that is used for each exported configuration.

If you are importing a configuration into FXOS 2.6.1 or later that was exported from an FXOS release prior to 2.6.1, the system will not check the encryption key and will allow the import.

Note If the platform software version to which you are importing is not the same version as when the export was taken, the import operation is not guaranteed to be successful. We recommend that you export a backup configuration whenever the Firepower 4100/9300 chassis is upgraded or downgraded.

Use the 'Set Version' option and export a backup configuration whenever the Firepower Threat Defense logical appliance is upgraded to a new software so that the new startup version matches the software release of the upgraded version.

Procedure

Step 1 From the FXOS CLI, enter security mode:

scope security

Example:

```
Firepower# scope security
Firepower /security #
```

Step 2 Set the encryption key:

set password-encryption-key

Enter a key: *encryption_key*

Confirm the key: *encryption_key*

The *encryption_key* must be 4-40 characters in length.

Example:

```
Firepower /security #set password-encryption-key
Enter a key:
Confirm the key:
Firepower /security* #
```

Step 3 Commit the configuration:

commit-buffer

Example:

```
Firepower /security* #commit-buffer
Firepower /security #
```

Exporting an FXOS Configuration File

Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server.

Before you begin

Review the About Configuration Import/Export.

Procedure

Step 1 To export a configuration file to a remote server:

scope system

export-config *URL* **enabled**
commit-buffer

Specify the URL for the file being exported using one of the following syntax:

- **ftp**://*username@hostname/path/image_name*
- **scp**://*username@hostname/path/image_name*

- **sftp**://*username@hostname / path / image_name*
- **tftp**://*hostname* **:** *port-num / path / image_name*

Note You must specify the full path including filename. If you do not specify a filename, a hidden file is created in the specified path.

Example:

```
Firepower-chassis# scope system
Firepower-chassis /system # export-config scp://user1@192.168.1.2:/export/cfg-backup.xml
enabled
Firepower-chassis /system/export-config # commit-buffer
```

Step 2 To check the status of the export task:

scope system

scope export-config *hostname*

show fsm status

Example:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope export-config 192.168.1.2
Firepower-chassis /system/export-config # show fsm status

Hostname: 192.168.1.2

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Backup Success
        Timestamp: 2016-01-03T15:32:08.636
        Try: 0
        Progress (%): 100
        Current Task:
```

Step 3 To view existing export tasks:

scope system

show export-config

Step 4 To modify an existing export task:

scope system

scope export-config *hostname*

Use the following commands to modify the export task:

- {**enable**|**disable**}
- **set description** <*description*>
- **set password** <*password*>
- **set port** <*port*>

- **set protocol** {**ftp**|**scp**|**sftp**|**tftp**}
- **set remote-file** *path_and_filename*
- **set user** <*user*>

Step 5 To delete an export task:

scope system

delete export-config *hostname*

commit-buffer

Scheduling Automatic Configuration Export

Use the scheduled export feature to automatically export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server. You can schedule the exports to be run daily, weekly, or every two weeks. The configuration export will be executed according to the schedule based on the when the scheduled export feature is enabled. So, for example, if you enable weekly scheduled export on a Wednesday at 10:00pm, the system will trigger a new export every Wednesday at 10:00pm.

Please review the About Configuration Import/Export for important information about using the configuration export feature.

Procedure

To create a scheduled export task:

a) Set the scope to export policy configuration:

scope org

scope cfg-export-policy default

b) Enable the export policy:

set adminstate enable

c) Specify the protocol to use when communicating with the remote server:

set protocol {**ftp**|**scp**|**sftp**|**tftp**}

d) Specify the hostname or IP address of the location where the backup file should be stored. This can be a server, storage array, local drive, or any read/write media that the Firepower 4100/9300 chassis can access through the network.

If you use a hostname rather than an IP address, you must configure a DNS server.

set hostname *hostname*

e) If you are using a non-default port, specify the port number:

set port *port*

f) Specify the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP:

set user *username*

g) Specify the password for the remote server username. This field does not apply if the protocol is TFTP:

set password *password*

h) Specify the full path to where you want the configuration file exported including the filename. If you omit the filename, the export procedure assigns a name to the file:

set remote-file *path_and_filename*

i) Specify the schedule on which you would like to have the configuration automatically exported. This can be one of the following: Daily, Weekly, or BiWeekly:

set schedule {**daily**|**weekly**|**bi-weekly**}

j) Commit the transaction to the system configuration:

commit-buffer

Example:

```
Firepower-chassis# scope org
Firepower-chassis /org # scope cfg-export-policy default
Firepower-chassis /org/cfg-export-policy # set adminstate enable
Firepower-chassis /org/cfg-export-policy* # set protocol scp
Firepower-chassis /org/cfg-export-policy* # set hostname 192.168.1.2
Firepower-chassis /org/cfg-export-policy* # set remote-file /export/cfg-backup.xml
Firepower-chassis /org/cfg-export-policy* # set user user1
Firepower-chassis /org/cfg-export-policy* # set password
Password:
Firepower-chassis /org/cfg-export-policy* # set schedule weekly
Firepower-chassis /org/cfg-export-policy* # commit-buffer
Firepower-chassis /org/cfg-export-policy #
Firepower-chassis /org/cfg-export-policy # show detail

Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Scp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Weekly
    Port: Default
    Current Task:
```

Setting a Configuration Export Reminder

Use the Export Reminder feature to have the system generate a fault when a configuration export hasn't been executed in a certain number of days.

By default, the export reminder is enabled with a frequency of 30 days.

Note If the reminder frequency is smaller than the number of days in the scheduled export policy (daily, weekly, or bi-weekly), you will receive an export-reminder fault message ("`Config backup may be outdated`"). For example, if your export schedule is weekly, and the reminder frequency is five days, this fault message will be issued every five days if no configuration has been exported in that time.

Procedure

To create a configuration export reminder:

scope org

scope cfg-export-reminder

set frequency *days*

set adminstate {**enable**|**disable**}

commit-buffer

Example:

```
Firepower-chassis# scope org
Firepower-chassis /org # scope cfg-export-reminder
Firepower-chassis /org/cfg-export-reminder # set frequency 10
Firepower-chassis /org/cfg-export-reminder* # set adminstate enable
Firepower-chassis /org/cfg-export-reminder* # commit-buffer
Firepower-chassis /org/cfg-export-reminder # show detail

Config Export Reminder:
    Config Export Reminder (Days): 10
    AdminState: Enable
```

Importing a Configuration File

You can use the configuration import feature to apply configuration settings that were previously exported from your Firepower 4100/9300 chassis. This feature allows you to return to a known good configuration or to recover from a system failure.

Before you begin

Review the About Configuration Import/Export.

Procedure

Step 1 To import a configuration file from a remote server:

scope system

import-config *URL* **enabled**

commit-buffer

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname*:*port-num*/*path*/*image_name*

Example:

```
Firepower-chassis# scope system
Firepower-chassis /system # import-config scp://user1@192.168.1.2:/import/cfg-backup.xml
enabled
Warning: After configuration import any changes on the breakout port configuration will
  cause the system to reboot
Firepower-chassis /system/import-config # commit-buffer
```

Step 2 To check the status of the import task:

scope system

scope import-config *hostname*

show fsm status

Example:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope import-config 192.168.1.2
Firepower-chassis /system/import-config # show fsm status

Hostname: 192.168.1.2

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Import Wait For Switch
        Previous Status: Import Config Breakout
        Timestamp: 2016-01-03T15:45:03.963
        Try: 0
        Progress (%): 97
        Current Task: updating breakout port configuration(FSM-STAGE:sam:dme:
          MgmtImporterImport:configBreakout)
```

Step 3 To view existing import tasks:

scope system

show import-config

Step 4 To modify an existing import task:

scope system

scope import-config *hostname*

Use the following commands to modify the import task:

- {**enable**|**disable**}
- **set description** <*description*>
- **set password** <*password*>
- **set port** <*port*>
- **set protocol** {**ftp**|**scp**|**sftp**|**tftp**}
- **set remote-file** *path_and_filename*
- **set user** <*user*>

Step 5 To delete an import task:

scope system

delete import-config *hostname*

commit-buffer