



# Using Cisco Fabric Services

This chapter contains the following sections:

- [Information About CFS, on page 1](#)
- [Guidelines and Limitations for CFS, on page 2](#)
- [CFS Distribution, on page 3](#)
- [CFS Support for Applications, on page 4](#)
- [CFS Regions, on page 8](#)
- [Configuring CFS over IP, on page 11](#)
- [Default Settings for CFS, on page 13](#)

## Information About CFS

Some features in the Cisco Nexus Series switch require configuration synchronization with other switches in the network to function correctly. Synchronization through manual configuration at each switch in the network can be a tedious and error-prone process.

Cisco Fabric Services (CFS) provides a common infrastructure for automatic configuration synchronization in the network. It provides the transport function and a set of common services to the features. CFS has the ability to discover CFS-capable switches in the network and to discover feature capabilities in all CFS-capable switches.

Cisco Nexus Series switches support CFS message distribution over IPv4 networks.

CFS provides the following features:

- Peer-to-peer protocol with no client-server relationship at the CFS layer.
- CFS message distribution over IPv4 and IPv6 networks.
- Three modes of distribution.
  - Coordinated distributions: Only one distribution is allowed in the network at any given time.
  - Uncoordinated distributions: Multiple parallel distributions are allowed in the network except when a coordinated distribution is in progress.
  - Unrestricted uncoordinated distributions: Multiple parallel distributions are allowed in the network in the presence of an existing coordinated distribution. Unrestricted uncoordinated distributions are allowed to run in parallel with all other types of distributions.

The following features are supported for CFS distribution over IP:

- One scope of distribution over an IP network:
  - Physical scope: The distribution spans the entire IP network.

## Cisco Fabric Services over Ethernet

The Cisco Fabric Services over Ethernet (CFS over Ethernet) is a reliable state transport mechanism that you can use to synchronize the actions of the vPC peer devices. CFS over Ethernet carries messages and packets for many features linked with vPC, such as STP and IGMP. Information is carried in CFS/CFS over Ethernet protocol data units (PDUs).

When you enable the vPC feature, the device automatically enables CFS over Ethernet, and you do not have to configure anything. CFS over Ethernet distributions for vPCs do not need the capabilities to distribute over IP or the CFS regions. You do not need to configure anything for the CFS over Ethernet feature to work correctly on vPCs.

You can use the `show mac address-table` command to display the MAC addresses that CFS over Ethernet synchronizes for the vPC peer link.




---

**Note** Do not enter the `no cfs eth distribute` or the `no cfs distribute` command. CFS over Ethernet must be enabled for vPC functionality. If you do enter either of these commands when vPC is enabled, the system displays an error message.

---

When you enter the `show cfs application` command, the output displays "Physical-eth," which shows the applications that are using CFS over Ethernet.

## Guidelines and Limitations for CFS

CFS has the following configuration guidelines and limitations:

- If the virtual port channel (vPC) feature is enabled for your device, do not disable CFS over Ethernet.




---

**Note** CFS over Ethernet must be enabled for the vPC feature to work.

---

- All CFS over IP-enabled devices with similar multicast addresses form one CFS over IP fabric.
- Make sure that CFS is enabled for the applications that you want to configure.
- Anytime you lock a fabric, your username is remembered across restarts and switchovers.
- Anytime you lock a fabric, configuration changes attempted by anyone else are rejected.
- While a fabric is locked, the application holds a working copy of configuration changes in a pending database or temporary storage area, not in the running configuration.
- Configuration changes that have not been committed yet (still saved as a working copy) are not in the running configuration and do not display in the output of `show` commands.

- If you start a CFS session that requires a fabric lock but forget to end the session, an administrator can clear the session.
- An empty commit is allowed if configuration changes are not previously made. In this case, the **commit** command results in a session that acquires locks and distributes the current database.
- You can use the **commit** command only on the specific device where the fabric lock was acquired.
- CFSoIP and CFSoE are not supported for use together.
- CFS regions can be applied only to CFSoIP applications.

## CFS Distribution

The CFS distribution functionality is independent of the lower layer transport. Cisco Nexus Series switches support CFS distribution over IP. Features that use CFS are unaware of the lower layer transport.

### CFS Distribution Modes

CFS supports three distribution modes to accommodate different feature requirements:

- Uncoordinated Distribution
- Coordinated Distribution
- Unrestricted Uncoordinated Distributions

Only one mode is allowed at any given time.

#### Uncoordinated Distribution

Uncoordinated distributions are used to distribute information that is not expected to conflict with information from a peer. Parallel uncoordinated distributions are allowed for a feature.

#### Coordinated Distribution

Coordinated distributions allow only one feature distribution at a given time. CFS uses locks to enforce this feature. A coordinated distribution is not allowed to start if locks are taken for the feature anywhere in the network. A coordinated distribution consists of three stages:

- A network lock is acquired.
- The configuration is distributed and committed.
- The network lock is released.

Coordinated distribution has two variants:

- CFS driven—The stages are executed by CFS in response to a feature request without intervention from the feature.
- Feature driven—The stages are under the complete control of the feature.

Coordinated distributions are used to distribute information that can be manipulated and distributed from multiple switches, for example, the port security configuration.

## Unrestricted Uncoordinated Distributions

Unrestricted uncoordinated distributions allow multiple parallel distributions in the network in the presence of an existing coordinated distribution. Unrestricted uncoordinated distributions are allowed to run in parallel with all other types of distributions.

## Verifying the CFS Distribution Status

The `show cfs status` command displays the status of CFS distribution on the switch:

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Enabled
```

# CFS Support for Applications

## CFS Application Requirements

All switches in the network must be CFS capable. Switches that are not CFS capable do not receive distributions, which results in part of the network not receiving the intended distribution. CFS has the following requirements:

- **Implicit CFS usage**—The first time that you issue a CFS task for a CFS-enabled application, the configuration modification process begins and the application locks the network.
- **Pending database**—The pending database is a temporary buffer to hold uncommitted information. The uncommitted changes are not applied immediately to ensure that the database is synchronized with the database in the other switches in the network. When you commit the changes, the pending database overwrites the configuration database (also known as the active database or the effective database).
- **CFS distribution enabled or disabled on a per-application basis**—The default (enable or disable) for the CFS distribution state differs between applications. If CFS distribution is disabled for an application, that application does not distribute any configuration and does not accept a distribution from other switches in the network.
- **Explicit CFS commit**—Most applications require an explicit commit operation to copy the changes in the temporary buffer to the application database, to distribute the new database to the network, and to release the network lock. The changes in the temporary buffer are not applied if you do not perform the commit operation.

## Enabling CFS for an Application

All CFS-based applications provide an option to enable or disable the distribution capabilities.

Applications have the distribution enabled by default.

The application configuration is not distributed by CFS unless distribution is explicitly enabled for that application.

## Verifying Application Registration Status

The **show cfs application** command displays the applications that are currently registered with CFS. The first column displays the application name. The second column indicates whether the application is enabled or disabled for distribution (enabled or disabled). The last column indicates the scope of distribution for the application (logical, physical, or both).



**Note** The **show cfs application** command only displays applications registered with CFS. Conditional services that use CFS do not appear in the output unless these services are running.

```
switch# show cfs application

-----
Application      Enabled   Scope
-----
ntp              No       Physical-all
fscm             Yes      Physical-fc
rscn            No       Logical
fctimer         No       Physical-fc
syslogd         No       Physical-all
callhome        No       Physical-all
fcdomain        Yes      Logical
device-alias    Yes      Physical-fc
Total number of entries = 8
```

The **show cfs application name** command displays the details for a particular application. It displays the enabled/disabled state, timeout as registered with CFS, merge capability (if it has registered with CFS for merge support), and the distribution scope.

```
switch# show cfs application name fscm

Enabled          : Yes
Timeout          : 100s
Merge Capable    : No
Scope           : Physical-fc
```

## Locking the Network

When you configure (first-time configuration) a feature (application) that uses the CFS infrastructure, that feature starts a CFS session and locks the network. When a network is locked, the switch software allows configuration changes to this feature only from the switch that holds the lock. If you make configuration

changes to the feature from another switch, the switch issues a message to inform the user about the locked status. The configuration changes are held in a pending database by that application.

If you start a CFS session that requires a network lock but forget to end the session, an administrator can clear the session. If you lock a network at any time, your username is remembered across restarts and switchovers. If another user (on the same machine) tries to perform configuration tasks, that user's attempts are rejected.

## Verifying CFS Lock Status

The **show cfs lock** command displays all the locks that are currently acquired by any application. For each application the command displays the application name and scope of the lock taken. If the application lock is taken in the physical scope, then this command displays the switch WWN, IP address, user name, and user type of the lock holder. If the application is taken in the logical scope, then this command displays the VSAN in which the lock is taken, the domain, IP address, user name, and user type of the lock holder.

```
switch# show cfs lock

Application: ntp
Scope      : Physical
-----
Switch WWN          IP Address      User Name      User Type
-----
20:00:00:05:30:00:6b:9e  10.76.100.167  admin         CLI/SNMP v3
Total number of entries = 1

Application: port-security
Scope      : Logical
-----
VSAN   Domain   IP Address      User Name      User Type
-----
1      238     10.76.100.167  admin         CLI/SNMP v3
2      211     10.76.100.167  admin         CLI/SNMP v3
Total number of entries = 2
```

The **show cfs lock name** command displays the lock details for the specified application.

```
switch# show cfs lock name ntp

Scope      : Physical
-----
Switch WWN          IP Address      User Name      User Type
-----
20:00:00:05:30:00:6b:9e  10.76.100.167  admin         CLI/SNMP v3

Total number of entries = 1
```

## Committing Changes

A commit operation saves the pending database for all application peers and releases the lock for all switches.

The commit function does not start a session; only a lock function starts a session. However, an empty commit is allowed if configuration changes are not previously made. In this case, a commit operation results in a session that acquires locks and distributes the current database.

When you commit configuration changes to a feature using the CFS infrastructure, you receive a notification about one of the following responses:

- One or more external switches report a successful status—The application applies the changes locally and releases the network lock.
- None of the external switches report a successful state—The application considers this state a failure and does not apply the changes to any switch in the network. The network lock is not released.

You can commit changes for a specified feature by entering the **commit** command for that feature.

## Discarding Changes

If you discard configuration changes, the application flushes the pending database and releases locks in the network. Both the abort and commit functions are supported only from the switch from which the network lock is acquired.

You can discard changes for a specified feature by using the **abort** command for that feature.

## Saving the Configuration

Configuration changes that have not been applied yet (still in the pending database) are not shown in the running configuration. The configuration changes in the pending database overwrite the configuration in the effective database when you commit the changes.




---

**Caution** If you do not commit the changes, they are not saved to the running configuration.

---

## Clearing a Locked Session

You can clear a lock held by an application from any device in the fabric.




---

**Caution** When you clear a lock in the fabric, any pending configurations in any device in the fabric are discarded.

---

### Before you begin

You must have administrator permissions to release a lock.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	(Optional) switch# <b>show</b> <i>application-name</i> <b>status</b>	Shows the current application state.
<b>Step 2</b>	Required: switch# <b>clear</b> <i>application-name</i> <b>session</b>	Clears the application configuration session and releases the lock on the fabric. All pending changes are discarded.
<b>Step 3</b>	(Optional) switch# <b>show</b> <i>application-name</i> <b>status</b>	Shows the current application state.

### Example

```
switch# show ntp status
Distribution : Enabled
Last operational state: Fabric Locked
switch# clear ntp session
switch# show ntp status
Distribution : Enabled
Last operational state: No session
```

## CFS Regions

### About CFS Regions

A CFS region is a user-defined subset of switches for a given feature or application in its physical distribution scope. When a network spans a vast geography, you might need to localize or restrict the distribution of certain profiles among a set of switches based on their physical proximity. CFS regions allow you to create multiple islands of distribution within the network for a given CFS feature or application. CFS regions are designed to restrict the distribution of a feature's configuration to a specific set or grouping of switches in a network.



---

**Note** You can only configure a CFS region based on physical switches. You cannot configure a CFS region in a VSAN.

---

### Example Scenario

The Smart Call Home application triggers alerts to network administrators when a situation arises or something abnormal occurs. When the network covers many geographies, and there are multiple network administrators who are each responsible for a subset of switches in the network, the Smart Call Home application sends alerts to all network administrators regardless of their location. For the Smart Call Home application to send message alerts selectively to network administrators, the physical scope of the application has to be fine tuned or narrowed down. You can achieve this scenario by implementing CFS regions.

CFS regions are identified by numbers ranging from 0 through 200. Region 0 is reserved as the default region and contains every switch in the network. You can configure regions from 1 through 200. The default region maintains backward compatibility.

If the feature is moved, that is, assigned to a new region, its scope is restricted to that region; it ignores all other regions for distribution or merging purposes. The assignment of the region to a feature has precedence in distribution over its initial physical scope.

You can configure a CFS region to distribute configurations for multiple features. However, on a given switch, you can configure only one CFS region at a time to distribute the configuration for a given feature. Once you assign a feature to a CFS region, its configuration cannot be distributed within another CFS region.



## Managing CFS Regions

### Creating CFS Regions

You can create a CFS region.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>cfs region region-id</b>	Creates a region.

### Assigning Applications to CFS Regions

You can assign an application on a switch to a region.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>cfs region region-id</b>	Creates a region.
<b>Step 3</b>	switch(config-cfs-region)# <i>application</i>	<p>Adds application(s) to the region.</p> <p><b>Note</b> You can add any number of applications on the switch to a region. If you try adding an application to the same region more than once, you see the "Application already present in the same region" error message.</p>

#### Example

The following example shows how to assign applications to a region:

```
switch# configure terminal
switch(config)# cfs region 1
switch(config-cfs-region)# ntp
switch(config-cfs-region)# callhome
```

### Moving an Application to a Different CFS Region

You can move an application from one region to another region.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>cfs region</b> <i>region-id</i>	Enters CFS region configuration submode.
<b>Step 3</b>	switch(config-cfs-region)# <i>application</i>	Indicates application(s) to be moved from one region into another.  <b>Note</b> If you try moving an application to the same region more than once, you see the "Application already present in the same region" error message.

**Example**

The following example shows how to move an application into Region 2 that was originally assigned to Region 1:

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# ntp
```

**Removing an Application from a Region**

Removing an application from a region is the same as moving the application back to the default region (Region 0), which brings the entire network into the scope of distribution for the application.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>cfs region</b> <i>region-id</i>	Enters CFS region configuration submode.
<b>Step 3</b>	switch(config-cfs-region)# <b>no</b> <i>application</i>	Removes application(s) that belong to the region.

**Deleting CFS Regions**

Deleting a region nullifies the region definition. All the applications bound by the region are released back to the default region.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>no cfs region</b> <i>region-id</i>	Deletes the region.  <b>Note</b> You see the, "All the applications in the region will be moved to the default region" warning.

## Configuring CFS over IP

### Enabling CFS over IPv4

You can enable or disable CFS over IPv4.



**Note** CFS cannot distribute over both IPv4 and IPv6 from the same switch.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>cfs ipv4 distribute</b>	Globally enables CFS over IPv4 for all applications on the switch.
<b>Step 3</b>	(Optional) switch(config)# <b>no cfs ipv4 distribute</b>	Disables (default) CFS over IPv4 on the switch.

### Enabling CFS over IPv6

You can enable or disable CFS over IPv6.



**Note** CFS cannot distribute over both IPv4 and IPv6 from the same switch.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure</b>	Enters configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	switch(config)# <b>cfs ipv6 distribute</b>	Globally enables CFS over IPv6 for all applications on the switch.
<b>Step 3</b>	(Optional) switch(config)# <b>no cfs ipv6 distribute</b>	Disables (default) CFS over IPv6 on the switch.

## Verifying the CFS Over IP Configuration

The following example show how to verify the CFS over IP configuration:

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::eff:4653
```

## Configuring IP Multicast Addresses for CFS over IP

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP network. CFS protocol-specific distributions, such as the keeplive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.



**Note** CFS distributions for application data use directed unicast.

## Configuring IPv4 Multicast Address for CFS

You can configure a CFS over IP multicast address value for IPv4. The default IPv4 multicast address is 239.255.70.83.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>cfs ipv4 mcast-address</b> <i>ipv4-address</i>	Configures the IPv4 multicast address for CFS distribution over IPv4. The ranges of valid IPv4 addresses are 239.255.0.0 through 239.255.255.255 and 239.192/16 through 239.251/16.
<b>Step 3</b>	(Optional) switch(config)# <b>no cfs ipv4 mcast-address</b> <i>ipv4-address</i>	Reverts to the default IPv4 multicast address for CFS distribution over IPv4. The default IPv4 multicast address for CFS is 239.255.70.83.

## Configuring IPv6 Multicast Address for CFS

You can configure a CFS over IP multicast address value for IPv6. The default IPv6 multicast address is ff13:7743:4653.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>cfs ipv6 mcast-address</b> <i>ipv4-address</i>	Configures the IPv6 multicast address for CFS distribution over IPv6. The range of valid IPv6 addresses is ff15::/16 (ff15::0000:0000 through ff15::ffff:ffff) and ff18::/16 (ff18::0000:0000 through ff18::ffff:ffff).
<b>Step 3</b>	(Optional) switch(config)# <b>no cfs ipv6 mcast-address</b> <i>ipv4-address</i>	Reverts to the default IPv6 multicast address for CFS distribution over IPv6. The default IPv6 multicast address for CFS over IP is ff15::eff:4653.

## Verifying the IP Multicast Address Configuration for CFS over IP

The following example shows how to verify the IP multicast address configuration for CFS over IP:

```
switch# show cfs status
Fabric distribution Enabled
IP distribution Enabled mode ipv4
IPv4 multicast address : 10.1.10.100
IPv6 multicast address : ff13::e244:4754
```

## Default Settings for CFS

The following table lists the default settings for CFS configurations.

**Table 1: Default CFS Parameters**

Parameters	Default
CFS distribution on the switch	Enabled
Database changes	Implicitly enabled with the first configuration change
Application distribution	Differs based on application
Commit	Explicit configuration is required
CFS over IP	Disabled
IPv4 multicast address	239.255.70.83
IPv6 multicast address	ff15::eff:4653

The CISCO-CFS-MIB contains SNMP configuration information for any CFS-related functions. See the MIB reference for your platform.

## Enabling CFS to Distribute Smart Call Home Configurations

You can enable CFS to distribute Call Home configurations to all Cisco NX-OS devices in the network. The entire Call Home configuration is distributed except the device priority and the sysContact names.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>callhome</b>	Enters Call Home configuration mode.
<b>Step 3</b>	switch(config-callhome)# <b>distribute</b>	Enables CFS to distribute Smart Call Home configuration updates.
<b>Step 4</b>	(Optional) switch(config-callhome)# <b>show application-name status</b>	For the specified application, displays the CFS distribution status.
<b>Step 5</b>	(Optional) switch(config-callhome)# <b>copy running-config startup-config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# distribute
switch(config-callhome)# show callhome status
Distribution : Enabled
switch(config-callhome)# copy running-config startup-config
```

## Enabling CFS to Distribute Device Alias Configurations

You can enable CFS to distribute device alias configurations in order to consistently administer and maintain the device alias database across all Cisco NX-OS devices in the fabric.

### Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>device-alias distribute</b>	Enables CFS to distribute device alias configuration updates.

	Command or Action	Purpose
<b>Step 3</b>	(Optional) switch(config)# <b>show cfs application</b>	Displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

This example shows how to enable CFS to distribute device alias configurations:

```
switch(config)# device-alias distribute
switch(config)# show cfs application
-----
Application Enabled Scope
-----
device-alias Yes Physical-fc
switch(config)# copy running-config startup-config
[#####] 100%
```

## Enabling CFS to Distribute DPVM Configurations

You can enable CFS to distribute dynamic port VSAN membership (DPVM) configurations in order to consistently administer and maintain the DPVM database across all Cisco NX-OS devices in the fabric.

### Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the DPVM feature. To do so, use the **feature dpvm** command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>dpvm distribute</b>	Enables CFS to distribute DPVM configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show application-name status</b>	For the specified application, displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

**Example**

This example shows how to enable CFS to distribute DPVM configurations:

```
switch(config)# dpvm distribute
switch(config)# show dpvm status
Distribution is enabled.
switch(config)# copy running-config startup-config
[#####] 100%
```

## Enabling CFS to Distribute FC Domain Configurations

You can enable CFS to distribute Fibre Channel (FC) domain configurations in order to synchronize the configuration across the fabric from the console of a single Cisco NX-OS device and to ensure consistency in the allowed domain ID lists on all devices in the VSAN.

**Before you begin**

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>fcdomain distribute</b>	Enables CFS to distribute FC domain configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show application-name status</b>	For the specified application, displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

**Example**

This example shows how to enable CFS to distribute FC domain configurations:

```
switch(config)# fcdomain distribute
switch(config)# show fcdomain status
fcdomain distribution is enabled
switch(config)# copy running-config startup-config
[#####] 100%
```



## Enabling CFS to Distribute FC Port Security Configurations

You can enable CFS to distribute Fibre Channel (FC) port security configurations in order to provide a single point of configuration for the entire fabric in the VSAN and to enforce the port security policies throughout the fabric.

### Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you enable the FC port security feature. To do so, use the **feature fc-port-security** command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>fc-port-security distribute</b>	Enables CFS to distribute FC port security configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show cfs application</b>	Displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup-config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

This example shows how to enable CFS to distribute FC port security configurations:

```
switch(config)# fc-port-security distribute
switch(config)# show cfs application
-----
Application Enabled Scope
-----
fc-port-securi Yes Logical
switch(config)# copy running-config startup-config
[#####] 100%
```

## Enabling CFS to Distribute FC Timer Configurations

You can enable CFS to distribute Fibre Channel (FC) timer configurations for all Cisco NX-OS devices in the fabric.

### Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>ftimer distribute</b>	Enables CFS to distribute FC timer configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show application-name status</b>	For the specified application, displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup-config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

**Example**

This example shows how to enable CFS to distribute FC timer configurations:

```
switch(config)# ftimer distribute
switch(config)# show ftimer status
Distribution : Enabled
switch(config)# copy running-config startup-config
[#####] 100%
```

## Enabling CFS to Distribute IVR Configurations

You can enable CFS to distribute inter-VSAN routing (IVR) configurations in order to enable efficient IVR configuration management and to provide a single point of configuration for the entire fabric in the VSAN.

**Before you begin**

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

Make sure that you install the Advanced SAN Services license.

Make sure that you enable the IVR feature. To do so, use the **feature ivr** command.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>ivr distribute</b>	Enables CFS to distribute IVR configuration updates.  <b>Note</b> You must enable IVR distribution on all IVR-enabled switches in the fabric.

	Command or Action	Purpose
<b>Step 3</b>	(Optional) switch(config)# <b>show cfs application</b>	Displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

This example shows how to enable CFS to distribute IVR configurations:

```
switch(config)# ivr distribute
switch(config)# show cfs application
-----
Application Enabled Scope
-----
ivr Yes Physical-fc
switch(config)# copy running-config startup-config
[#####] 100%
```

## Enabling CFS to Distribute NTP Configurations

You can enable CFS to distribute NTP configurations to all Cisco NX-OS devices in the network.

### Before you begin

Make sure that you enable the NTP feature (using the **feature ntp** command).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>ntp distribute</b>	Enables CFS to distribute NTP configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show application-name status</b>	For the specified application, displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# show ntp status
```

```
Distribution : Enabled
switch(config)# copy running-config startup-config
```

## Enabling CFS to Distribute RADIUS Configurations

You can enable CFS to distribute RADIUS configurations to all Cisco NX-OS devices in the network.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>radius distribute</b>	Enables CFS to distribute RADIUS configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show application-name status</b>	For the specified application, displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

```
switch# configure terminal
switch(config)# radius distribute
switch(config)# show radius status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

## Enabling CFS to Distribute RSCN Configurations

You can enable CFS to distribute registered state change notification (RSCN) configurations to all Cisco NX-OS devices in the fabric.

### Before you begin

Make sure that you are in the storage VDC. To change to the storage VDC, use the **switchto vdc fcoe** command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>rscn distribute</b>	Enables CFS to distribute RSCN configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show cfs application</b>	Displays the CFS distribution status.

	Command or Action	Purpose
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

This example shows how to enable CFS to distribute RSCN configurations:

```
switch(config)# rscn distribute
switch(config)# show cfs application
-----
Application Enabled Scope
-----
rscn Yes Logical
switch(config)# copy running-config startup-config
[#####] 100%
```

## Enabling CFS to Distribute TACACS+ Configurations

You can enable CFS to distribute TACACS+ configurations to all Cisco NX-OS devices in the network.

### Before you begin

Make sure that you enable the TACACS+ feature (using the **feature tacacs+** command).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>tacacs+ distribute</b>	Enables CFS to distribute TACACS+ configuration updates.
<b>Step 3</b>	(Optional) switch(config)# <b>show application-name status</b>	For the specified application, displays the CFS distribution status.
<b>Step 4</b>	(Optional) switch(config)# <b>copy running-config startup config</b>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

### Example

```
switch# configure terminal
switch(config)# tacacs+ distribute
switch(config)# show tacacs+ status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

