SonicOS 6.2 Content Filtering Service 4.0

Upgrade Guide

June 2017

This Upgrade Guide provides instructions for upgrading your network security appliance from previous versions of SonicWall™ Content Filtering Service (CFS) to the latest version of CFS 4.0. CFS 4.0 is available for appliances running SonicOS 6.2.6 or later.

Topics:

- Differences between CFS 4.0 and Previous Releases
- Automatic CFS Policy Migration
- CFS Policy Upgrade Example
- SonicWall Support

Differences between CFS 4.0 and Previous Releases

This section provides information about the new features of CFS 4.0 and the main differences between CFS 4.0 and previous releases.

Topics:

- Configuring CFS Policy
- New CFS Objects
- New CFS Policy
- Comparison of CFS 3.0 to CFS 4.0

Configuring CFS Policy

In previous releases, configuring CFS policy involved navigating many steps on several pages: CFS page, Zones page, Users/Groups page, and App Rules page. In particular, CFS 3.0 had two separate modes: **Users and Zones** and **App Rules**. In CFS 4.0, these two modes are merged so that all CFS policies can be configured from a single page on the interface.

New CFS Objects

CFS 4.0 uses an object based model. This is more consistent with other SonicWall configurations with the same ease of re-usability.

A new **Content Filter Objects** page has been added inside the Firewall menu. All CFS objects are listed in this page. To apply these objects, you can access the Content Filter page through the link **Security Services > Content Filter** in the Content Filter Objects page. In the Content Filter page, a link also jumps back to the Content Filter Objects page.

CFS 4.0 introduces three new objects:

- **CFS URI List Object**. This replaces the Custom Allowed List, Custom Forbidden List, Keywords List, CFS Allowed/Forbidden List in App Rules, and part of Restrict Web Features (per file extensions). Unlike CFS 3.0, CFS URI lists now support wildcard matching. Once defined, a CFS URI List Object can be easily re-used in any CFS Profile Object for whitelisting or blacklisting.
- **CFS Profile Object.** This is a new concept in CFS 4.0. A Profile Object defines the kind of operation triggered for each HTTP/HTTPS connection. The user can define the Allowed/Forbidden URI List here, and define the operations for each category (Allowed, Blocked, Confirm, Passphrase, and BWM). The original consent feature has also been moved into CFS Profile Object. This changes the consent feature from a global setting to a per-profile setting. The CFS Profile Object is like an old CFS policy, although it is only a part of a new CFS policy.
- **CFS Action Object.** Also a new concept in CFS 4.0, the CFS Action Object defines what happens after a packet is filtered by CFS. The administrator can define the detailed configurations for these actions: Block, Confirm, Passphrase and BWM. This action object is also part of a new CFS policy.

New CFS Policy

The new CFS policy engine allows administrators to define the following matching conditions for a CFS Policy: Source Zone, Destination Zone, Address Object, Users/Groups, Schedule, Enabled, CFS Profile, and CFS Action.

When a packet is processed, the following conditions are checked: Source Zone, Destination Zone, Address Object, Users, Schedule and Enabled state. If all of these conditions are matched, the packet is filtered by the corresponding CFS Profile. Then the CFS Action is invoked according to the filtering results.

CFS policies now follow a priority defined by the order set in the Content Filter page. CFS 3.0's least restrictive and most permissive policies follow a new, high-to-low priority model in CFS 4.0. When matching policies, a CFS Policy with higher priority is checked earlier. Priority is determined by position in the policy list, with the highest priority given to the policy at the top. As a general practice, the highest priority should be assigned to specific/granular policies and lower priority to more generic policies that apply to a broader set of users.

Since CFS 4.0 now supports three new actions, Passphrase, BWM, and Confirm, the new priority model enables administrators to more clearly visualize and manage the policy execution order and ultimately better design the overall policy set behavior. Administrators should verify that the upgraded policies follow the intended behavior. If discrepancies in policies are found, administrators should back up all firmware settings and configurations before editing and deleting the applicable policies. With this method, administrators can re-create the corresponding policies manually without having to touch the Match, Action, and Profile CFS Objects.

Comparison of CFS 3.0 to CFS 4.0

The following table compares the user experience for various aspects of the old and new CFS.

CFS 3.0	CFS 4.0
Configure CFS on CFS page, Zone page, User page, and App Rules page.	Centralized CFS configuration in one place.
Two modes (via Zones and via App Rules).	Merged functions in one mode.
Admin cannot predict the filtering results accurately after configuration.	Admin can exactly predict the filtering results.
Need to define duplicated filtering options.	Define URI List object, Profile object, and Action object, which can be reused in multiple policies.
Does not support wildcard matching.	Supports wildcard (*) matching for URI List.
Consent feature is global.	Consent feature is per policy.
BWM is only supported in App Rules mode.	BWM is fully supported.
Does not support Override-Confirm.	Supports Override-Confirm.
Only supports GET, POST, and HEAD commands for HTTP.	Supports GET, POST, PUT, CONNECT, OPTIONS, DELETE, REPORT, COPY, and MOVE commands.

CFS 3.0	CFS 4.0
Cannot enable/disable CFS globally.	Can enable/disable CFS globally.
Custom category is based on category.	Custom category is based on domain, which is more intuitive.
Websense configuration is mixed with CFS configuration.	Separate Websense configuration from CFS configuration helps prevent errors.

NOTE: If Content Filtering Service is not licensed through either Comprehensive Gateway Security Services (CGSS) or a Content Filtering Service Premium license, then CFS functions does not work.

Automatic CFS Policy Migration

When upgrading to CFS 4.0 for the first time, the firmware does its best to automatically migrate the policies from CFS 3.0. However, as the settings are somewhat different, the resulting policies may not exactly match the original policies. CFS 3.0 employed some settings that are no longer used and are discarded when migrating to CFS 4.0.

The automatic migration process uses complex logic to try to replicate the originally intended policies. Therefore, the policy migration process takes longer and the complete objects are configured differently than when they were configured in CFS 3.0. Network administrators should not assume that the automatically migrated policies in CFS 4.0 exactly match their original policies configured in the previous version and should instead examine and verify the results.

This section describes the actions taken during the automatic migration process.

Topics:

- Migration from Users and Zones Mode
- Migration from App Rules Mode
- Migration from Websense Mode
- Recommended Validation Process

Migration from Users and Zones Mode

Because policies were previously accumulated in CFS 3.0, it is difficult to assign a correct priority/order to these new policies under CFS 4.0. Therefore, you should verify and manually adjust the correct policy priority following the migration.

After these steps take place, a default CFS Policy is automatically generated and appended at the end of the list.

To migrate from Users and Zones mode:

1 For each old CFS policy:

   a Generate a new CFS Profile Object.

   b Migrate old **Allowed URI List** objects:

   - If the Source of Allowed Domains of old policy is None, the Allowed URI List of the Profile Object is also None.
   - If the Source of Allowed Domains of the old policy is Global, CFS 4.0 generates a new CFS URI List from the old global allowed list. It then assigns this new CFS URI List to the Allowed URI List of the Profile Object.

- If the Source of Allowed Domains of the old policy is Per Policy, CFS 4.0 generates a new CFS URI List from the old custom allowed list. It then assigns this new CFS URI List to the Allowed URI List of the Profile Object.

c Migrate old Forbidden Domains and Keywords. The logic follows that of Allowed Domains.

d Generate a new CFS Action Object. The old global blocking page is assigned to this new Action Object. Since previous CFS versions do not have Confirm, Passphrase and BWM options, the values inside new Action Object are the default values.

After all the old polices have been migrated, new CFS URI List Objects, CFS Profile Objects and CFS Action Objects are generated and mapped to the old policy ID in order to keep their relationship.

2 If the old CFS uses the CFS Policy per IP Address Range feature, generate a new CFS policy for each row inside the old CFS Policy per IP Address Range Table. For each new CFS policy:

- The Source Zone and Destination Zone are set to **All**.
- The Source Address is the same value as the CFS 3.0 IP range.
- The Users/Groups are set to **All**.
- The Schedule keeps same value as in the CFS 3.0 policy.
- The CFS Profile Object is the Profile object generated in Step 1.
- The CFS Action Object is Action object generated in Step 1.

3 For each user group with CFS enabled, a new CFS Policy is generated. For each new CFS Policy:

- The Source Zone and Dest Zone are set to **All**.
- The Source Address is set to **Any**.
- The Users/Groups are the same CFS 3.0 user groups.
- The Schedule is same value as in the CFS 3.0 policy.
- The CFS Profile Object is the Profile object generated in Step 1.
- The CFS Action Object is the Action object generated in Step 1.

NOTE: After upgrading, the user groups under the same policy as the group Everyone in CFS 3.0 are merged into one policy with the Everyone group.

4 For each zone with CFS enabled, a new CFS Policy is generated. For each new CFS Policy:

- The Source Zone is set to the CFS 3.0 zone.
- The Destination Zone is set to **All**.
- The Source Address is set to **Any**.
- The Users/Groups are set to **Any**.
- The Schedule is the same value as in the CFS 3.0 policy.
- The CFS Profile Object is the Profile object generated in Step 1.
- The CFS Action Object is the Action object generated in Step 1.

Migration from App Rules Mode

For each App Rule whose Policy Type is CFS and Action is CFS Block Page or HTTP Block Page or BWM, CFS 4.0 executes the following steps to complete the policy upgrading process.

To migrate from App Rules mode:

1 CFS URI List Objects are generated from Allow/Excluded and Forbidden/Included lists of current App Rule.

2 The CFS Profile Object is generated according to current App Rule and its Match Object.

NOTE: Depending on the selected categories in the current App Rule's Match Object, they are set as either Block or BWM in the Profile Object.

3 The CFS Action Object is generated according to the following criteria:

- If the action of a current App Rule is a CFS Block Page, the old global CFS blocking page content is the block page content of this Action Object.
- If the action of a current App Rule is HTTP Block Page, the block page of current App Rule is the block content of this Action Object.
- If the action of a current App Rule is BWM, the BWM values are used for this Action Object.

4 The App Rule name is used as the Policy name. To generate a CFS Policy, the following should take place:

- The Zone of the CFS 3.0 App Rule is set to **Source Zone**.
- The Destination Zone is set to **All.**
- The Source Address is set to the address of the CFS 3.0 App Rule.
- The Users/Groups are set to the included Users/Groups of the CFS 3.0 App Rule.
- The Schedule is set to the Schedule of the CFS 3.0 App Rule.
- The CFS Profile Object generated above is assigned to the CFS Profile.
- The CFS Action Object generated above is set to CFS Action.

NOTE: After all App Rules have been migrated to CFS Policies, CFS attempts to keep the same priorities, generating a Default CFS Policy at the end of the list.

Migration from Websense Mode

There are no significant changes for Websense between CFS 4.0 and the previous releases, so the upgrading process for Websense is simple and is not discussed in this document.

Recommended Validation Process

Following the migration process, some of the generated CFS objects and policies might be duplicated and the priority order of some new policies might be wrong. Hence, administrators should clean and adjust the priorities.

The best practice for the migration is to keep the automatically generated CFS URI List Objects, which contain the whitelist and blacklist defined in the firewall, and keep the generated CFS Action Objects, which contain the customized blocking pages. Remove the generated CFS Policies and the generated CFS Profile Objects.

After cleaning, create the CFS Profile Objects and CFS Policies from scratch, providing descriptive names for each object. Normally, this is faster than adjusting the auto generated objects and making them work as expected. Fewer objects are duplicated also.

CFS Policy Upgrade Example

This section discusses the differences in policy settings between CFS 3.0 and CFS 4.0 via an sample situation.

Consider the case of an office with three groups: engineering, sales, and HR. Each group has different CFS policies to control access to websites.

In the previous CFS release, the IT administrator created 3 different CFS policies, and assigned each policy to a group from the Users menu. A default CFS policy was also used, which was assigned to the LAN zone.

For each HTTP connection, CFS 3.0 checked which group that current user belonged to, then accumulated the corresponding CFS policy with the default CFS policy to filter the connection. If the user did not belong to any group, then the default CFS policy was applied to the connection.

In the upgraded CFS 4.0, CFS generates three CFS Policies with the correct CFS Profile and CFS Action, and links the new policies with the correct groups. The default policy is auto generated too, which by default is at the end of the policy table.

In the previous CFS, if one employee belonged to multiple groups and each group had a different CFS policy, these policies were accumulated with complicated algorithms, and different algorithms for different settings inside the policy. This policy accumulation introduced many implicit filtering results. Thus, IT admin could not clearly distinguish what the filtering behaviors were after completing the configurations. It was also very difficult to troubleshoot when unexpected filtering behaviors appeared.

In CFS 4.0, the configuration is clear and explicit, without any implicit or hidden logic. Each connection only hits one CFS policy at most. Policy accumulation is no longer allowed. Once the connection hits one policy inside the policy table, that policy is the only one applied to this connection.

This behavior has a trade-off. For example, for the employee belonging to multiple groups, in CFS 4.0, the IT administrator needs to create a special small group for him, then create a CFS Policy for this group, and make sure this policy has higher priority than other bigger groups so that this policy is hit earlier.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid support maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, visit https://support.sonicwall.com/contact-support.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 6/20/17

232-003342-01 Rev A