SonicWALL Content Security Manager 2100 Content Filter SonicOS Secure Content 2.0.0.1 Release Notes

SonicWALL, Inc.
November 7, 2005

CONTENTS

PLATFORM COMPATIBILITY

SonicOS Secure Content (SonicOS SC) Version 2.0.0.1 is a supported firmware release for the SonicWALL® Content Security Manager 2100 Content Filter (SonicWALL CSM 2100 CF) security appliance.

ENHANCEMENTS

SonicOS SC 2.0 New Feature Highlights

- **Gateway Anti-Virus and Anti-Spyware**—SonicOS SC 2.0 introduces Gateway Anti-Virus and Anti-Spyware, offering protection against today's most insidious network threats. Automatic security updates provide constant and immediate protection against new security threats in real-time.
- **Application Filter Policies by Users and Groups**—The SonicOS SC 2.0 deep packet inspection engine provides accurate and reliable management of dynamic applications such as IM, P2P, remote access and streaming multimedia content with a highly configurable per-users and per-group control method. Administrators can now also define custom application filters by port.
- **Setup Wizards and Diagnostic Tools**—The SonicOS SC 2.0 Setup Wizard assists with the initial configuration of the SonicWALL CSM 2100 CF, while the Diagnostic tool helps to assure proper network settings and configuration. Additional diagnostic and status reporting enhancements include a display of Microsoft Active Directory authenticated users with IP address and assigned policies, and improved log messages for Active Directory Connector user and host resolution events about hosts (IP addresses) on which SonicWALL ADConnector is not able to resolve user information. Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- **High Availability/Failover Support**—HA capabilities for service continuity, including configurable monitoring, synchronization, and failover behavior.
- **Policy Configuration by IP Address**—The SonicOS SC 2.0 supports the ability to apply policies by IP addresses.

P/N 232-000583-04
Rev A 11/05

SonicWALL CSM 2100 CF

The SonicWALL CSM 2100 CF is an appliance-based Internet filtering solution that integrates real-time gateway anti-virus, anti-spyware and Internet filtering to deliver maximum network protection from today's sophisticated Internet threats. Combining dynamic threat management capabilities with precise control over Internet usage in an affordable, appliance-based solution, the SonicWALL CSM 2100 CF boosts network security and employee productivity, optimizes network utilization and mitigates legal liabilities. This unique solution integrates seamlessly into virtually any network topology for powerful, scalable and cost-effective threat protection.

Utilizing the high-performance SonicWALL deep packet inspection architecture, the SonicWALL CSM 2100 CF eliminates malicious Internet threats before they can infect the network. At the same time, the SonicWALL CSM 2100 CF provides granular controls that enable network administrators to manage access to Web sites containing inappropriate, unproductive and potentially illegal Web content. To complete the solution, the SonicWALL CSM 2100 CF includes advanced graphical reporting and analysis tools, offering administrators granular insight into network usage.

SonicWALL CSM 2100 CF Features

The SonicWALL Content Security Manager 2100 CF integrates real-time gateway anti-virus, anti-spyware and Internet filtering to deliver maximum network protection from today's sophisticated Internet threats. The following list provides feature highlights:

- **Real-time Gateway Anti-Virus and Anti-Spyware Scanning**—over a multitude of widely-used ports and protocols including HTTP, SMTP, POP3, FTP and NetBIOS delivers complete protection by eliminating viruses, worms, Trojans, spyware and other Internet threats at the gateway before they can infect the network.
- **Powerful Internet Filtering**—provides granular, policy-based controls to manage access to inappropriate, unproductive and potentially illegal Web content.
- **Instant Messaging** (**IM**)**, Peer-to-Peer** (**P2P**)**, and Multimedia Controls**—improves network performance, enhances security and protects against legal liabilities.
- **Granular Policy Control Using Single Sign-on**—streamlines user authentication and the management of access to network resources and online content.
- **Powerful Web-based Reporting**—provides greater insight into network usage through custom reports that can be viewed in multiple formats.
- **Seamless Integration Behind Virtually Any Network Firewall**—enables organizations to leverage the existing network infrastructure without the need to purchase additional hardware.
- **High Availability**—ensures the network is always protected and productivity remains uninterrupted by automatically failing over to a secondary SonicWALL CSM 2100 CF should the primary unit fail.

P/N 232-000583-04
Rev A 11/05

MODIFICATIONS

The following section describes changes to the Management Interface after upgrading from SonicOS SC 1.0 to SonicOS SC 2.0.

SonicOS SC 1.0 Software	SonicOS SC 2.0 Software
Default Categories	Predefined Categories
Untrusted URLs	Forbidden URLs
Untrusted Keywords	Forbidden Keywords
Trusted URLs	Allowed URLs
Privacy Threats	Miscellaneous (Web Risks, Forbidden File Types and Trusted Sites)

New Modifications to Policies (previously named "Policy Groups")

- Schedules are now associated with specific policies and not categories. When migrating policies from SonicOS SC 1.0 to SonicOS SC 2.0 all the schedules are reset to 'Always On'. You must re-apply the correct schedules in each policy to apply them at correct times. For information on configuring Schedules, refer to the **Applying Schedules to Custom Policies** section on page 13 of this document.
- You can now include Application Filters in individual policies. On the policy configuration pop-up window there is the new tab **Application Filters**. User can click on the **Edit** icon for every policy, navigate to the Application Filter tab and select the application filter category sets you would like to control.
- Note that all changes can be cancelled until the policy configuration pop-up window is closed by pressing the 'OK' button.

New Modifications to Web Filters -> Category Sets (previously named "Policies")

- Schedule is removed from Category Set Settings tab.
- A new action 'Continue' has been added for predefined categories providing administrators the option to allow users to opt-in to view (and log the viewing of) certain types of content.

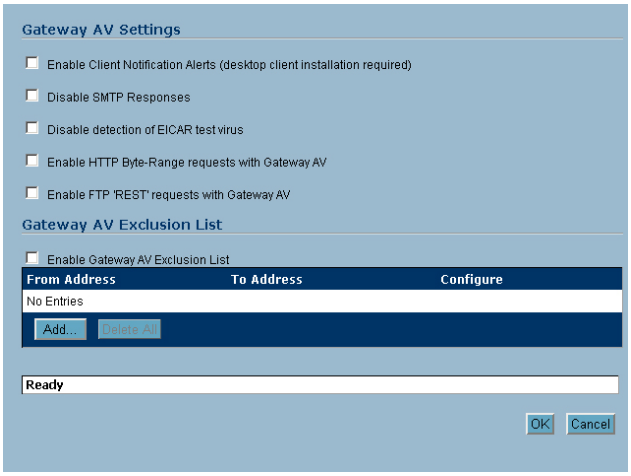
Application Filters > Category Sets

- Each Application Category Set can include Port filters, Instant Messenger, Multimedia and P2P application filters. Every item can be selected with 'block' or 'log' option.
- Every Application Filter Category Set can be included in a policy, the same way as Web Filter Category Set can.
- In addition to predefined non-editable Port Filters, you can add custom port filters. All these filters can be used in Application Filter Category Sets.

P/N 232-000583-04
Rev A 11/05

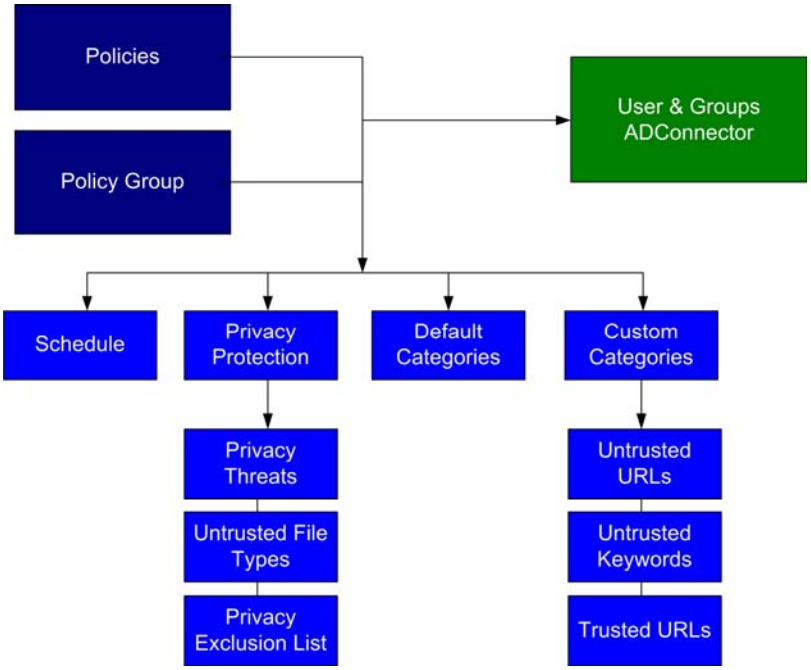
Internet Security > Gateway Anti-Virus > Gateway AV Settings

- The 'Enable HTTP Byte-Range requests with Gateway AV' checkbox has been added to the Gateway AV settings page. Allows HTTP Byte Range requests issued by HTTP clients. This checkbox is disabled by default.
- The 'Enable FTP 'Rest' Requests with Gateway AV' checkbox has been added to the Gateway AV settings page. Allows usage of RESTART FTP command by FTP clients. This checkbox is disabled by default.

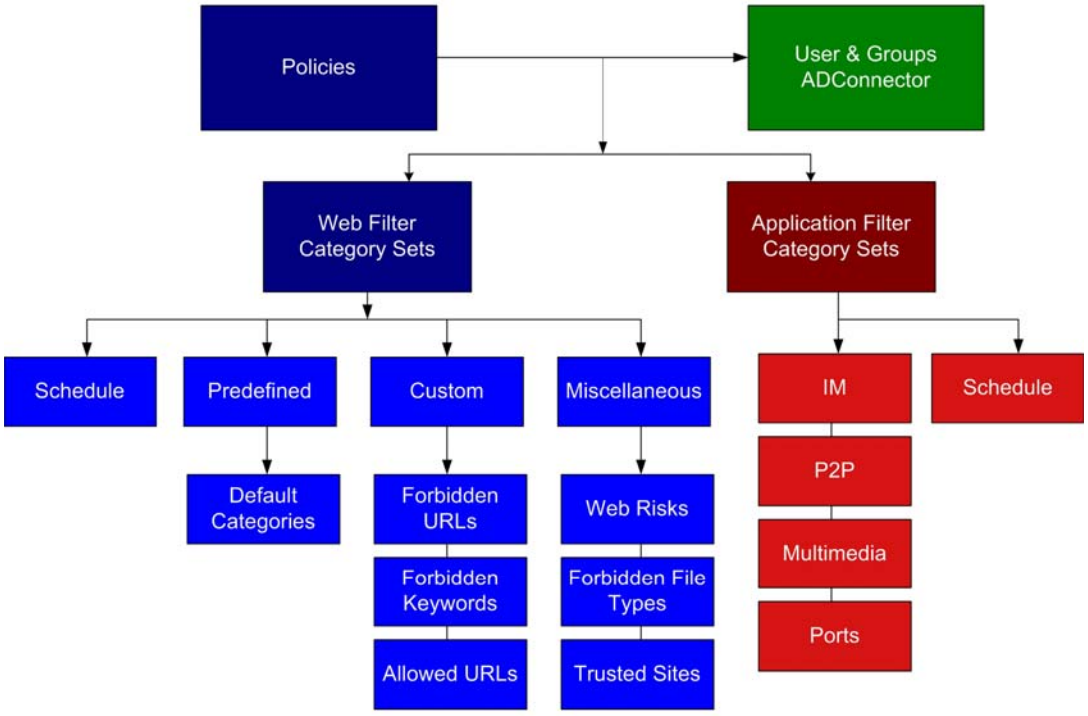


P/N 232-000583-04
Rev A 11/05

Policy Hierarchy and Structure Schematic for SonicOS SC 1.0 Software (Old Version)



Policy Hierarchy and Structure Schematic for SonicOS SC 2.0 Software (Current Version)



P/N 232-000583-04
Rev A 11/05

RELEASE CAVEATS

Flowing are formal notes and prerequisite warnings for the SonicOS SC 2.0.0.0 release:

- SonicWALL ADConnector requires you to open a network access rule to allow inbound TCP port 445 on the computer with the personal firewall installed.
- The SonicWALL ADConnector is unable to send data to the Content Security Manager using the following share secret keys:

```
1111111111111111
FEFEFEFEFEFEFEFE
1F1F1F1F1F1F1F1F
E0E0E0E0E0E0E0E0
01FE01FE01FE01FE
FE01FE01FE01FE01
1FE01FE01FE01FE0
E01FE01FE01FE01F
01E001E001E001E0
```

- The SonicWALL ADConnector will not correctly identify user sessions in Terminal Services and Citrix Terminal environments where multiple users are logged on the same computer.
- SonicWALL ViewPoint 2.8.5 or higher is supported on the SonicWALL CSM 2100 CF security appliance.

KNOWN ISSUES

- **37748**: **Symptom**: Unable to upgrade the firmware on the SonicWALL CSM 2100 CF security appliance, and in a few cases you may receive the following error message:

  Invalid firmware filename.

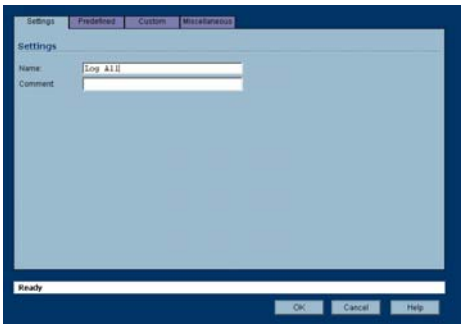
  Condition: Occurs when upgrading an existing network deployed SonicWALL CSM 2100 CF security appliance. **Workaround**: Perform a hard reboot on the SonicWALL CSM 2100 CF security appliance before upgrading the firmware.

- **37629**: **Symptom**: In a few Active Directory deployments, Policy's inherited by an object take over 10 seconds to display in the detail screen (right hand pane) after the Administrator clicks on an object in the Tree. **Condition**: This happens when the object is a member of multiple security groups that need to be parsed for policy inheritance. **Workaround**: The user has to wait for the software to complete its response.
- **37656**: The management interface (X2) must be configured for a different IP subnet from X0/X1, and must be located on a different physical segment. Failure to do so could result in routing anomalies.
- **37617**: **Symptom**: The user is unable to distinguish which SonicWALL CSM 2100 CF security appliance owns a policy being assigned to an object. **Condition**: Occurs when Multiple SonicWALL CSM 2100 CF security appliances are being managed by the same SonicWALL ADConnector. **Workaround**: When creating policies, use names that are identified by the SonicWALL CSM 2100 CF security appliance the policy is being created from. This is not an issue in installations where identical policies exist on all SonicWALL CSM 2100 CF security appliances being managed.
- **37535**: **Symptom**: Policy schedules set to “Always Block” after firmware upgrade from 1.x to 2.x. **Condition:** Schedule has been changed from custom to default which "always block". However, the schedule objects are not lost during upgrade. **Workaround**: You will need to change the schedule assignment again.

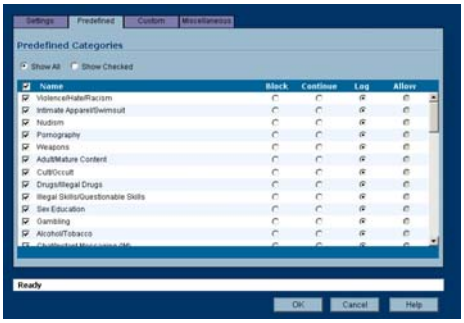
P/N 232-000583-04
Rev A 11/05

- **37317: Symptom**: After completion of installation program, the service does not start automatically. **Condition**: This happens when the installation program is completed. **Workaround**: Open the Service Control Manager, verify username and password and start the service.
- **35675**: **Symptom**: If a 250 character URL is added under 'Users' > 'Settings' > 'Global User Settings,' user is unable to remove URLs that bypass user authentication. **Condition**: Web sites with URLs longer than 250 characters may bypass user authentication in rules.
- **33904**: **Symptom**: SonicWALL ViewPoint reports display "N/A" for categories of Web sites in Web Usage reports. **Condition**: By default, the Content Security Manager categorizes Web sites only for the filter list. **Workaround**: Create a "Log All" policy to capture the category information for all Web traffic. Perform the following steps:

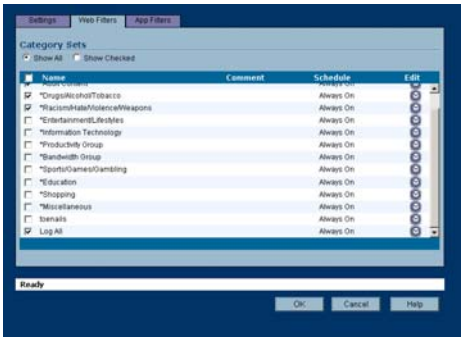
    1. In Web Filters > Category Sets, create a Web Category Set called "Log All" as depicted below:



    2. Check all the categories and change the action to log for each as depicted below:



    3. Save the Policy by clicking the **OK** button.
    4. In 'Policies' > 'Policy List', add the newly created "Log All" Policy to each policy in the Policy List.



P/N 232-000583-04
Rev A 11/05

- **39419**: **Symptom**: The SonicWALL CSM 2100 CF displays the time stamps for all log messages in UTC format. **Condition**: Occurs when the SonicWALL CSM 2100 CF is configured to display log message time stamps in local time format.
- **39422**: **Symptom**: The Firmware Management checkbox is greyed out; thus, users cannot disable the Firmware Management option. **Condition**: Can be seen when going to the "System > Settings" window.

RESOLVED KNOWN ISSUES

- **37987**: **Symptom**: Adding a second range of host IP addresses replaces the original range of host IP addresses, and lines without Comment fields are truncated. **Condition**: Occurs when adding host IP addresses under "Users and Hosts > Hosts."
- **38772**: **Symptom**: The performance of the SonicWALL CSM 2100 CF is degraded when both CFS and DRTR are enabled. **Condition**: Occurs when CFS and DRTR are enabled at the same time.
- **38435**: **Symptom**: Policies reset themselves back to their default value. **Condition**: Occurs randomly every few hours.
- **39110**: The SonicWALL CSM 2100 CF does not download the latest GAV signature.
- **38017**: **Symptom**: The SonicWALL CSM 2100 CF sends ADC requests for IP addresses that are already in the web filter exclusion list. **Condition**: Occurs when a user attempts to access a site that has already been added to the web filter exclusion list.
- **38805**: **Symptom**: The SonicWALL CSM 2100 CF does not allow primary and secondary management IP addresses to be configured. **Condition**: Occurs when trying to configure the X2 primary and secondary management IP addresses under "Hardware Failover > Monitoring."
- **39110**: The Gateway Anti-Virus (GAV) signature was occasionally not immediately updated. Clicking on the Update button did not obtain the most recent GAV signature.
- **39101**: When you defined a host range on a CSM and applied a policy to the range, the CSM filtering did not apply to the range. If you specified a single host in the range, it filtered properly.
- **38017**: Active Directory Connector (ADC) requests made to a host are sent even if the host is in an exclusion list.
- **38672**: Strings in the French language that contained characters with accent marks did not appear correctly in the French localized version of the CSM interface. This sometimes made messages that appear in the SysLog unreadable.
- **38191**: After resetting license information on the diagnostics page and rebooting the device, you cannot register the device from the status page.
- **38331**: After configuring the IP address in the wizard for the CSM 2100CF on the first session with the device, the wizard window freezes after you click **Apply** in the Change in Progress page.
- **37675**: Feature. Add a checkbox for web filter IP address exclusion list so it is like Anti-Spyware IP address exclusion lists.

P/N 232-000583-04
Rev A 11/05

- **37748**: When trying to upload new firmware on a CSM 2100 CF when the device resides behind a firewall, the device always rejects the new firmware and does not load it. This problem was caused by large chunk memory allocation.

- **37987**: When adding a range of addresses assigned to a series of hosts, the new range incorrectly replaces any existing range that was applied to hosts.

- **37795**: The User Group Configuration popup window incorrectly displayed the field Policy Group. It should just read Policy.

- **37792**: The Settings page displays the word heartbeat in two different ways in two different fields: **Heartbeat Interval (seconds)** and **Failover Trigger Level (missed heart beats)**.

- **38652**: The label for the Adult Content field on the **Web Filters > Category Settings** page was misspelled.

- **38805**: The High Availability (HA) Monitoring list did not display the management interface.

- **38602**: You cannot log into or ping the CSM 2100 CF user interface environment from the local area network.

- **37536**: The 'Block Nothing' default policy is no longer available in SonicOS SC 2.x.

P/N 232-000583-04
Rev A 11/05

UPGRADING SONICWALL CSM 2100 CF SECURITY APPLIANCES TO SONICOS SC 2.0 SOFTWARE

This document provides procedures to upgrade a **SonicWALL CSM 2100 CF** from **SonicOS CF 1.0** to **SonicOS SC 2.0**. The following sections describe the installation process:

- **Upgrade Prerequisites**
- **Installing SonicOS SC 2.0 Firmware**
- **Creating Web Filter Custom Categories**
- **Creating Web Filter Custom Category Sets**
- **Creating a Web Filter Custom Policy List**
- **Applying Schedules to Custom Policies**

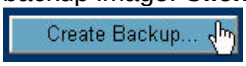
Before starting this upgrade process, you must have a copy of the SonicOS SC 2.0 firmware downloaded and saved to your local host. The firmware is available for download to all users through the firmware download page located at **https://www.mysonicwall.com**.

Upgrade Prerequisites

The following steps take you through the process of creating a backup image of your current firmware. By completing these steps, you can then revert to this backup of the SonicOS Standard firmware as a backout strategy.

1. In the SonicOS management interface, navigate to the **System > Settings** page.

2. At the bottom of the page, select **Create Backup**. You will be prompted to overwrite your existing backup image. **Click OK**.



3. To export your current configuration settings to a preferences file from the SonicOS **System > Settings** page, select **Export Settings** and save the preferences file to your local host.

P/N 232-000583-04
Rev A 11/05

Installing SonicOS SC 2.0 Firmware

Now you are ready to upload and boot to the SonicOS SC 2.0 firmware. Before you start, you should have a copy of the SonicOS SC 2.0 firmware saved to your local host. If you do not yet have a copy of the firmware on your local host, you must download the proper firmware from **https://www.mysonicwall.com**.

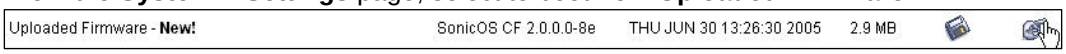
1. In the SonicOS management interface, navigate to the **System > Settings** page.
2. At the bottom of the page, select **Upload New Firmware**.

3. Navigate to your downloaded firmware by clicking the **Browse** button.

4. Once you have located the firmware, click the **Upload** button.

Please wait while the firmware is being uploaded to your SonicWALL. This process may take up to a minute. When the upload is complete, the status bar at the bottom will read **Firmware uploaded successfully**.

5. From the **System > Settings** page, select to boot from **Uploaded Firmware**.

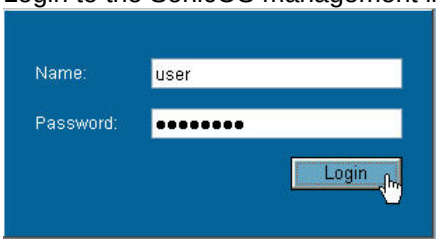


Your SonicWALL will restart. Please wait while this process is taking place.

***Warning**: The process of booting to the new uploaded firmware may take a few minutes, **DO NOT power down the unit** while this process is taking place.*

After reboot is complete, you will be taken to the SonicOS management interface login screen.

6. Login to the SonicOS management interface with your user name and password.

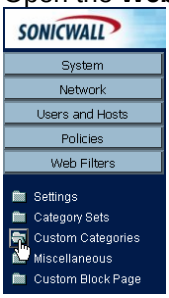


P/N 232-000583-04
Rev A 11/05

Creating Web Filter Custom Categories

To create a Custom Category:

1. Open the **Web Filters > Custom Categories** page in the administrative interface:



2. Select the type of category you want to add, **Forbidden URLs**, **Forbidden Keywords**, or **Allowed URLs**, and click **Add**.

3. Add the new custom category in the **Add Forbidden URL**, **Add Forbidden Keyword**, or **Add Allowed URLs** page.
   - **Name**: The name of the Custom Category.
   - **Comment**: A brief explanation of the Custom Category.
   - **Entry**: The value of the Custom Category. Enter a value and click **Add** to add it to the list. You can add several entries to a single Custom Category.

4. Click **OK** to add the Custom Category.

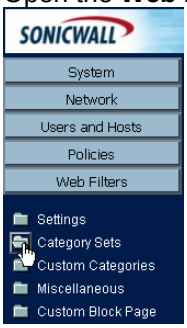
P/N 232-000583-04
Rev A 11/05

Creating Web Filter Custom Category Sets

A Category Set is a combination of predefined categories, custom categories, and other privacy threats that you combine together into a policy list and block, log, or allow. “Web Filter Category Sets” replaced Sonic OS SC 1.0’s “Policies.”

To create a custom Category Set:

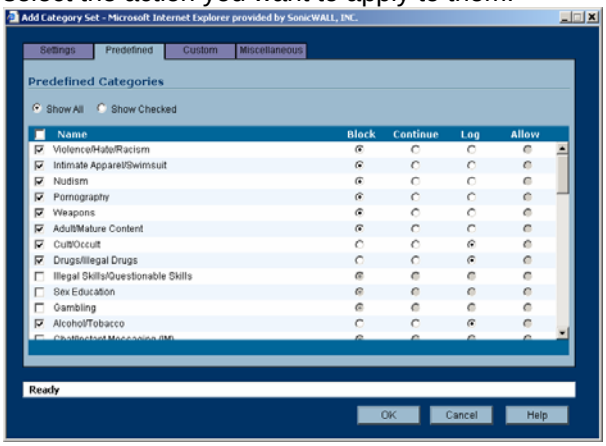
1. Open the **Web Filters > Category Sets** page in the administrative interface.



2. Select a Category Set to modify  , or click **Add** at the bottom of the page.

3. In the **Settings** tab of the **Add Category Set** page, enter a name and brief description for the Category Set.

4. In the **Predefined** tab, select the predefined web content categories you want to include and select the action you want to apply to them.



5. In the **Custom** tab, select custom categories you have added and select the action you want to apply to them.

6. In the **Miscellaneous** tab, select privacy threats and select actions to apply to them.

P/N 232-000583-04
Rev A 11/05

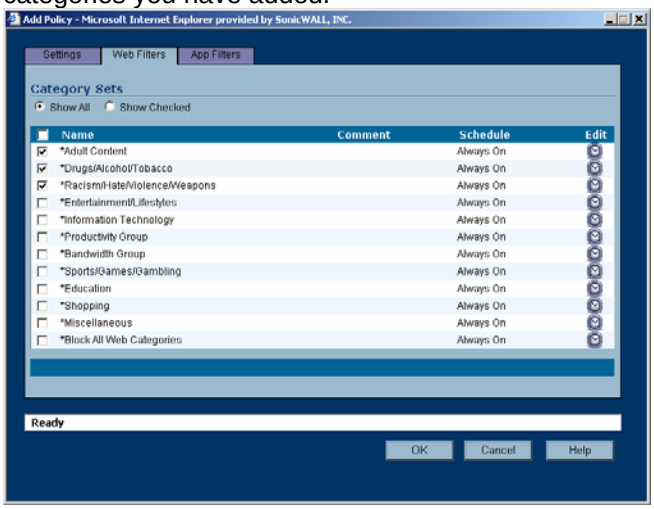
Creating a Web Filter Custom Policy List

Policy Lists are lists of category sets you collect together to apply as a single content filter to users, user groups, and network hosts. Policy Lists in SonicOS SC 2.0 replace Policy Groups in SonicOS SC 1.0. To add a custom policy list:

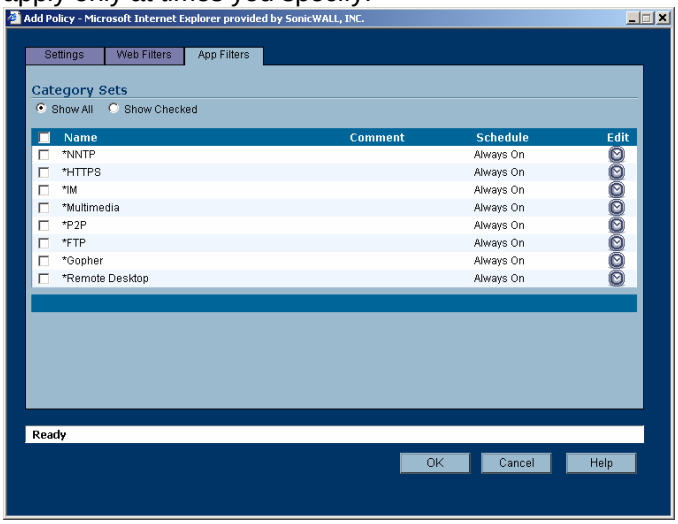
1. Open the **Policies > Policy Lists** page in the Admin UI.

2. In the **Settings** tab of the **Add Policy** page, enter a name and brief description/comment for the Policy List.

3. In the **Web Filters** tab, select the Category Sets you want to add. These can include any custom categories you have added.



4. In the **App Filters** tab, select application filters to add. You can change the schedule to have it apply only at times you specify.



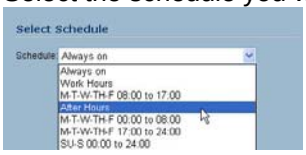
P/N 232-000583-04
Rev A 11/05

Applying Schedules to Custom Policies

With SonicOS SC 2.0, you now have the ability to apply schedules to individual policies. To apply a schedule to a Custom Policy:

1. Open the **Policies > Policy List** page in the administrative interface:

2. Select a Policy List to modify and click the **edit** icon .
3. To apply a schedule to a web filter, click on the **Web Filters** tab. To apply a schedule to an application click on the **App Filters** tab.
4. Click the **edit** button for the desired category set.
5. Select the schedule you wish to use from the pull-down menu provided.



6. Click the **OK** button.
7. To apply changes, click the **OK** button in the Edit Policy window.

Document version: November 7, 2005

P/N 232-000583-04
Rev A 11/05