

SonicWALL ***Content Filtering Service***

User's Guide



Table of Contents

Copyright Notice	3
Limited Warranty	3
SonicWALL Technical Support	4
Introduction	5
Activating Content Filtering Service from the Security Services Tab	6
Activating SonicWALL Content Filtering Service using mySonicWALL.com	8
What is mySonicWALL.com?	8
What Can I Do with mySonicWALL.com?	8
How do I Get Started with mySonicWALL.com?	8
Activating the Content Filtering Service Subscription	8
Managing Content Filtering	10
Accessing the SonicWALL using a Web Browser	10
Configuring SonicWALL Content Filtering Service	11
Content Filter Type	11
Restrict Web Features	12
Block:	12
Message to display when a site is blocked	12
Configuring CFS Settings	13
Settings	13
URL Cache	14
URL List	14
Select Categories to block	14
Customizing the Content Filtering List	15
Custom Filter	15
Allowed Domains	16
Forbidden Domains	16
Keywords	16
Deleting Allowed Domains, Forbidden Domains, or Keywords	16
Time of Day	17
Consent	17
Web Usage Consent Page	18
Mandatory Filtered IP Addresses	19
Users	20
Global User Settings	20
Users	21
Adding and Removing a User	22

Copyright Notice

© 2003 SonicWALL, Inc. All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein can be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

Limited Warranty

SonicWALL, Inc. warrants that SonicWALL Network Anti-Virus will perform in accordance to the accompanying written materials for a period of ninety (90) days from the date of receipt.

SonicWALL Inc.'s and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the PRODUCT has resulted from accident, abuse, or misapplication. Any replacement PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

In no event shall SonicWALL or its suppliers be liable for any damages whatsoever (including, without limitation, special, incidental, indirect, or consequential damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the PRODUCT.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. Where liability may not be limited under applicable law, SonicWALL's liability shall be limited to the amount you paid for the Product. This warranty gives you specific legal rights, and you may have other rights which vary from state to state.

By using this Product, you agree to these limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED.

No dealer, agent, or employee of SonicWALL is authorized to make any extension or addition to this warranty.

Phone: 1-408-752-7819

Fax: 1-408-745-9300

Support: <http://www.sonicwall.com/support/>

This warranty does not apply if the SonicWALL is damaged by accident, abuse, misuse, misapplication, or is modified without the written permission of SonicWALL, Inc.

In no event shall SonicWALL, Inc. or its suppliers be liable for any damages, whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or other pecuniary loss) arising out of the use of the SonicWALL, or the inability to use the SonicWALL.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. Where liability may not be limited under applicable law, SonicWALL liability is limited to the amount paid for the product. This warranty gives you specific legal rights, and you may have other rights which vary from state to state. By using the SonicWALL Internet Security Appliance, you agree to the limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESSED OR IMPLIED.

No dealer, agent, or employee of SonicWALL, Inc. is authorized to make any extension or addition to this warranty.

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <<http://www.sonicwall.com/support>>. Resources are available to help you resolve most technical issues, as well as a way to contact one of the SonicWALL Technical Support engineers.

Phone: (408) 745-9600

Fax: (408) 745-9300

Web: <http://www.sonicwall.com>

E-mail: sales@sonicwall.com

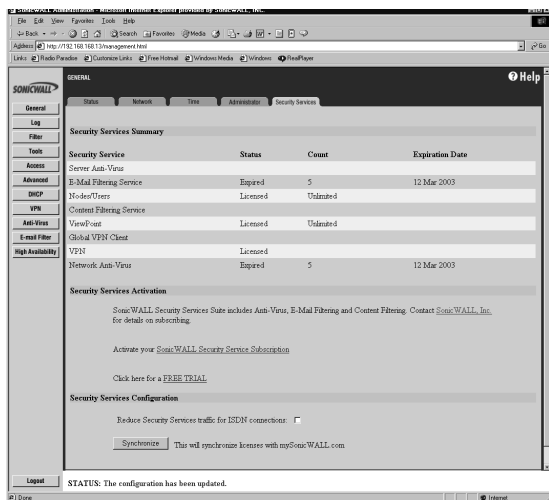
Introduction

The SonicWALL Content Filtering Service helps organizations increase productivity and reduce legal and privacy risks by automatically enforcing acceptable use policies while minimizing administration overhead. Integrated with SonicWALL's line of Internet security appliances, the SonicWALL Content Filtering Service enables organizations such as businesses, schools and libraries to maintain Internet access policies tailored to their specific needs.

With SonicWALL Content Filtering Service, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. The SonicWALL Content Filtering Service automatically updates the filters, making maintenance substantially simpler and less time consuming. SonicWALL Content Filtering can be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL, a customized message is displayed on the user's screen. SonicWALL Internet security appliances can also be configured to log attempts to access sites on the SonicWALL Content Filter List, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

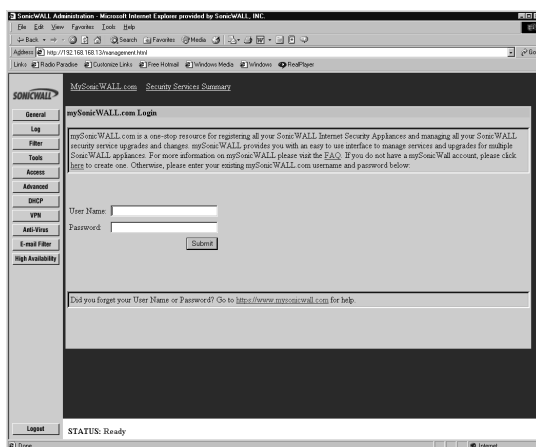
Activating Content Filtering Service from the Security Services Tab

You can also activate your Content Filtering Service from the **Security Services** tab. Click **General**, and then **Security Services**.



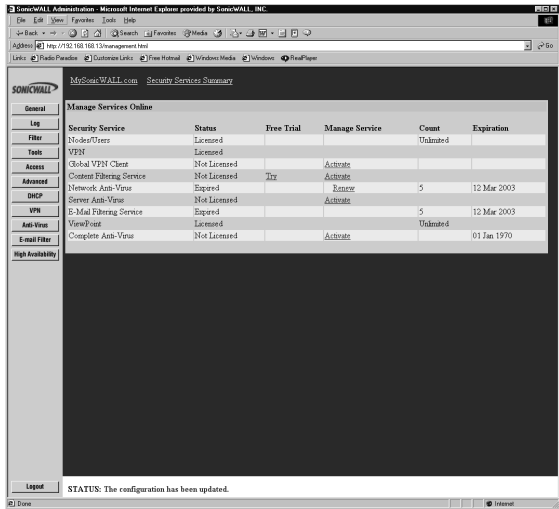
Tip! If you have already activated your subscription, proceed to **Configuring Content Filtering**.

In the **Security Services Activation** section, click the link **Activate Your SonicWALL Security Service Subscription**. The **mySonicWALL.com Login** page is displayed.



Type your mySonicWALL.com user name and password in the **User Name** and **Password** fields. If you do not have a mysonicWALL.com account, click the link [here](#) to go to the registration page and create your account.

When you log into your mySonicWALL.com account, the **Manage Services Online** page is displayed.



Click **Activate** and type your activation key from the back of this manual into the **Activation Key** field. Click **Submit**.

Activating SonicWALL Content Filtering Service using mySonicWALL.com

Before you can configure the SonicWALL **Content Filtering Service**, the subscription requires you to register your SonicWALL Internet Security Appliance at <<http://www.mysonicwall.com>>. At this web site, you can create a user account to activate and manage services for all of your SonicWALL Internet Security Appliances.

For the latest version of this manual and other SonicWALL documentation, go to <<http://www.sonicwall.com/support/documentation.html>>

What is mySonicWALL.com?

mySonicWALL.com delivers a convenient, centralized way to register all your SonicWALL Internet Security Appliances and Security Services and eliminates the hassle of registering individual SonicWALL appliances and upgrades. Using mySonicWALL.com allows you to have a single user profile where you can manage all your product registrations and security services.

What Can I Do with mySonicWALL.com?

You can use mySonicWALL.com to do the following:

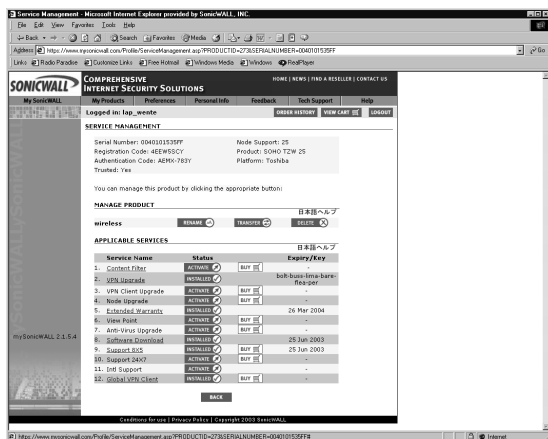
- **Register** all your SonicWALL appliances and services in one place.
- **Access** firmware and security service updates.
- **Get** SonicWALL alerts on services, firmware, and products.
- **Check** status of your SonicWALL services and upgrades linked to each registered SonicWALL Internet security appliance.
- **Manage** (activate, change or delete) your SonicWALL security services online.

How do I Get Started with mySonicWALL.com?

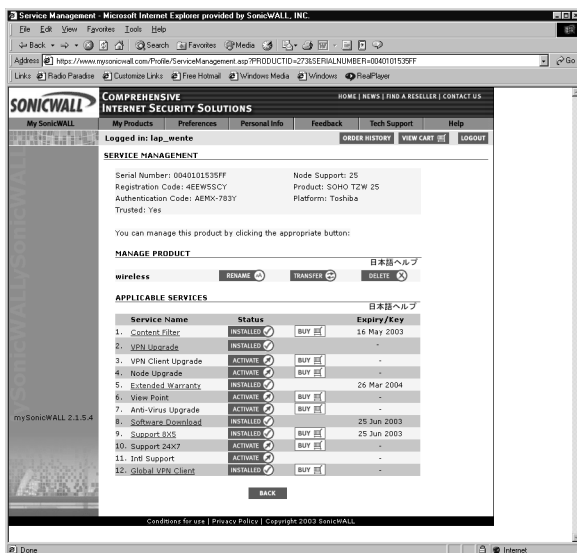
The first step to using mySonicWALL.com is creating a user account. Go to <<http://www.mysonicwall.com>> and follow the instructions for setting up a new user account.

Activating the Content Filtering Service Subscription

To activate the **Content Filtering Service** subscription, you must first register your activation key on the SonicWALL website at the SonicWALL registration site <<http://www.mysonicwall.com>>. Follow the instructions below to activate the Content Filtering Service subscription. Log into your user account, and select the SonicWALL appliance to activate the Content Filtering Service subscription. Click **Activate** next to **Content Filtering** in the list of **Applicable Services**



1. Type the **Activation Key** in the **Activation Key** field, and click **Submit**.
2. Your **Content Filtering Service** subscription is activated.



Managing Content Filtering

This section contains detailed information on the configuration of the SonicWALL **Content Filtering** feature. A Web browser is used to access the SonicWALL Management interface, and the commands and functions of Content Filtering.

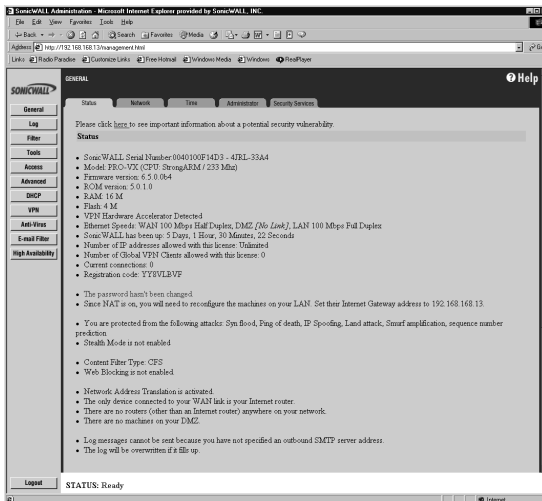
The following sections are in this chapter:

- **Accessing the SonicWALL using a Web browser**
- **Enabling Content Filtering and Blocking**
- **Customizing Content Filtering**
- **Blocking URLs with Keywords**

Accessing the SonicWALL using a Web Browser

Open a Web browser and enter the SonicWALL IP address into the **Address** field, then press **Enter**. When the **Password** dialogue box appears, enter **admin** into the **User Name** field, and enter the administrator password in the **Password** field. Click **Login** to open the Management Station interface.

Click **General** on the left side of the Management interface, and then **Status**.

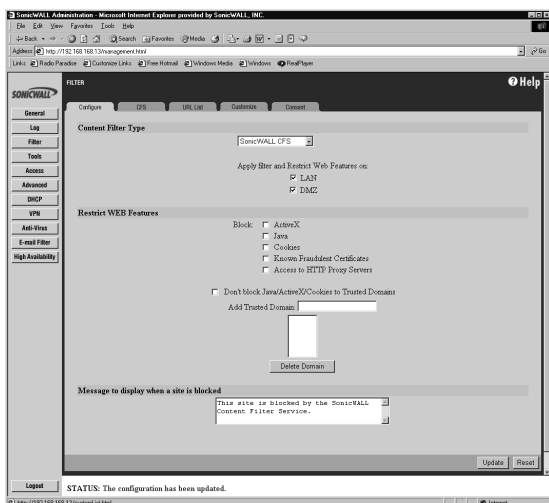


The active tab, **Status**, displays the current status of the SonicWALL. It contains an overview of the SonicWALL settings and configurations as well as any messages generated by the SonicWALL. Be sure to review the **Status** tab after making changes to the SonicWALL to verify that changes are updated by the SonicWALL.

If the message, “This SonicWALL is not yet registered.”, is displayed, you must complete the online registration process using the web-based registration form located at <<http://www.mysonicwall.com>> to register your SonicWALL. After the SonicWALL is registered, you can activate your Content Filtering List subscription by clicking **Activate**, and entering your **Activation Key** from the back of this manual. Your SonicWALL can now be managed from the central registration Web site.

Configuring SonicWALL Content Filtering Service

Click **Filter** on the left side of the browser window, and then click on the **Configure** tab.



Note: Content Filtering applies only to HTTP requests from devices behind the SonicWALL LAN, DMZ, or both.

Content Filter Type

SonicWALL CFS - Selecting **SonicWALL CFS** for the **Content Filter List Type** allows you use the CFS database and completely customize your Content Filter feature including allowed and forbidden domains as well as content filtering using keywords.

Restrict Web Features

Block:

- **ActiveX**

ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.

- **Java**

Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.

- **Cookies**

Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.

- **Known Fraudulent Certificates**

Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL blocks the Web content and the files that use these fraudulent certificates.

Known fraudulent certificates blocked by SonicWALL include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

- **Access to HTTP Proxy Servers**

When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.

- **Don't Block Java/ActiveX/Cookies to Trusted Domains**

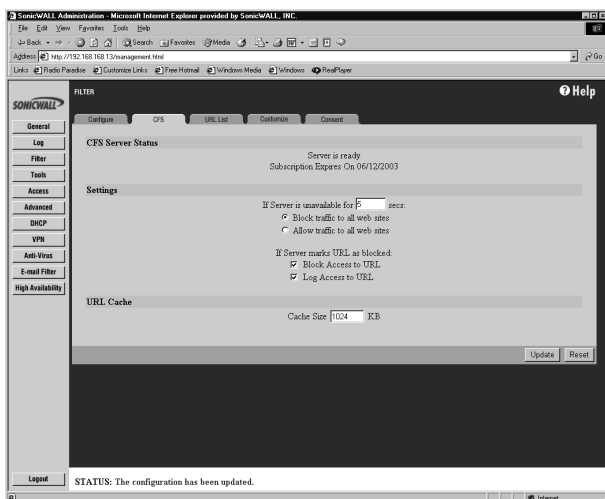
Select this option if you have trusted domains using Java, ActiveX, and Cookies. To add a trusted domain, enter the domain name into the **Add Trusted Domain** field. Click **Update** to add the domain to the list of trusted domains. To delete a domain, select it from the list, and then click **Delete**.

Message to display when a site is blocked

Enter your customized text to display to the user when access to a blocked site is attempted. The default message is **Web Site blocked by SonicWALL Filter**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.

Configuring CFS Settings

The **CFS** page allows you to see the status of the CFS Server and the expiration date of your subscription. You can also determine how the SonicWALL responds when the Content Filtering Service is unavailable.



Settings

If you have enabled blocking by **Categories** and the CFS Server is unavailable for a designated period of time (default value is 5 seconds), there are two options available:

- **Block traffic to all web sites except for Allowed Domains**

Selecting this option blocks traffic to all web sites until the CFS Server is available.

- **Allow traffic to all web sites**

Selecting this option allows traffic to all web sites. However, **Forbidden Domains** and **Keywords**, if enabled, are still blocked.

If you have enabled blocking by **Categories** and the URL is blocked by the server, there are two options available:

- **Block Access to URL**

Selecting this option prevents the browser from displaying the requested URL to the user.

- **Log Access to URL**

Selecting this option records the requested URL in the log file.

URL Cache

Configure the size of the **URL Cache** in KB.

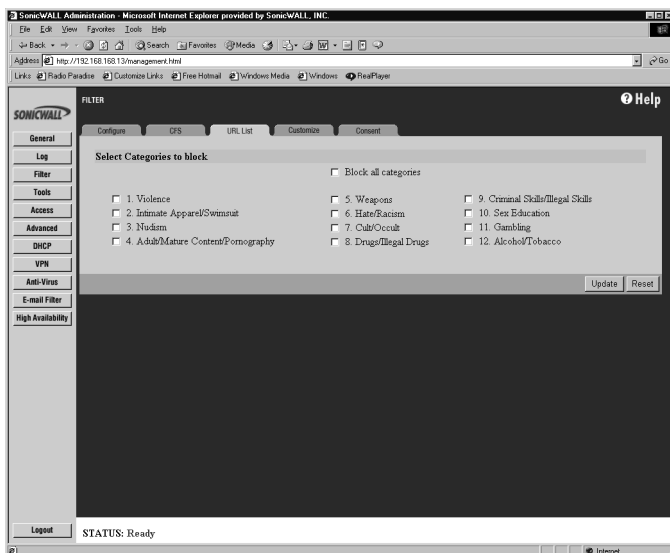
Model	Cache Size	Approximate Number of Sites
XPRS, PRO, SOHO2, TELE2, SOHO3, TELE3, and PRO-Vx	128	2,000
PRO 230, PRO 330, PRO 100, PRO 200, PRO 300, PRO2, PRO-VX2	256	4,000
GX250, GX650	1024	16,000



TIP! A larger **URL Cache** size can increase in noticeable improvements in Internet browsing response times.

URL List

To access **URL List**, click **Filter**, and then **URL List**.



Select Categories to block

- **Block all categories**

The SonicWALL uses a **URL List** database to block access to objectional Web sites. Objectional Web sites are classified based upon input from a wide range of social, political, and civic organizations. Select the **Block all categories** check box to block all of these categories. Alternatively, you can select categories individually by selecting the appropriate check box.

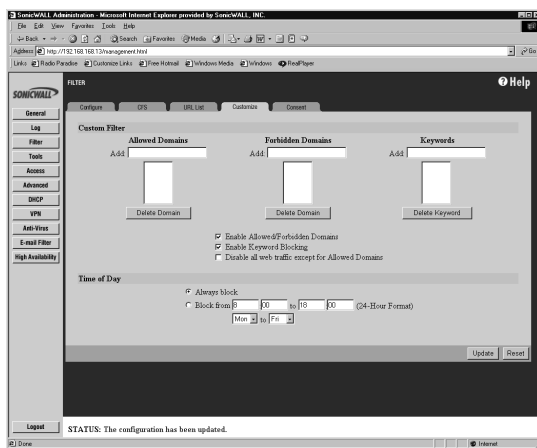
The following is a list of the **Content Filtering Service** categories:

- | | |
|-------------------------------------|-----------------------------------|
| 1. Violence | 7. Cult/Occult |
| 2. Intimate Apparel/Swimsuit | 8. Drugs/Illegal Drugs |
| 3. Nudism | 9. Criminal Skills/Illegal Skills |
| 4. Adult/Mature Content/Pornography | 10. Sex Education |
| 5. Weapons | 11. Gambling |
| 6. Hate/Racism | 12. Alcohol & Tobacco |

Visit <http://www.sonicwall.com/products/contentfiltering.html#filters> for a detailed description of the criteria used to define Content Filtering Service categories.

Customizing the Content Filtering List

The **Customize** tab allows you to customize Content Filtering by manually entering domain names or keywords to be blocked or allowed through the SonicWALL.



Custom Filter

You can customize your URL list to include **Allowed Domains**, **Forbidden Domains**, and **Keywords**. By customizing your URL list, you can include specific domains to be allowed (accessed), forbidden (blocked), and include specific keywords to be used to block sites.

• Enable Allowed/Forbidden Domains

To deactivate **Custom Filter** customization, clear the **Enable Allowed/Forbidden Domains**, and click **Update**. This option allows you to enable and disable customization without removing and re-entering custom domains.

- **Enable Keyword Blocking**

Select the **Enable Keyword Blocking** if you want to block Web traffic based on your list of customized keywords.

- **Disable all web traffic except for Allowed Domains**

When the **Disable Web traffic except for Allowed Domains** check box is selected, the SonicWALL only allows Web access to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectional material.

Allowed Domains

To allow access to a Web site that is blocked by the Content Filtering Service, type the host name, such as “www.ok-site.com”, into the **Allowed Domains** fields. 256 entries can be added to the **Allowed Domains** list.

An Allowed Domain is not the same as a Trusted Domain. You may allow access to a domain (Allowed Domain), but block ActiveX, Java, cookies, etc.

Forbidden Domains

To block a Web site that is not blocked by the Content Filtering Service, type the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 256 entries can be added to the **Forbidden Domains** list.

Alert! Do not include the prefix “http://” in either the Allowed Domains or Forbidden Domains the fields. All subdomains are affected. For example, entering “yahoo.com” applies to “mail.yahoo.com” and “my.yahoo.com”.

Keywords

To enable blocking using **Keywords**, select the **Enable Keyword Blocking** check box.

Type the keyword to block in the **Add Keyword** field, and click **Update**. Once the keyword has been added, a message confirming the update is displayed at the bottom of the browser window.



TIP! Customized domains do not have to be re-entered when the Content Filtering Service is updated each week and do not require a URL list subscription.

Deleting Allowed Domains, Forbidden Domains, or Keywords

To remove an **Allowed Domain**, select it from the appropriate list, and click **Delete Domain**. Once the domain has been deleted, a message is displayed at the bottom of the Web browser window.

To remove a **Forbidden Domain**, select it from the appropriate list, and click **Delete Domain**. Once the domain has been deleted, a message is displayed at the bottom of the Web browser window.

To remove a keyword, select it from the list and click **Delete Keyword**. Once the keyword has been removed, a message confirming the update is displayed at the bottom of the browser window.

Time of Day

The **Time of Day** feature allows you to define specific times when Content Filtering Service is enforced. For example, you could configure the SonicWALL to filter employee Internet access during normal business hours, but allow unrestricted access at night and on weekends.



TIP! *Time of Day restrictions only apply to the Content Filtering Service, Customized blocking and Keyword blocking. Consent and Restrict Web Features are not affected.*

- **Always Block**

When selected, **Content Filtering** is enforced at all times.

- **Block Between**

When selected, **Content Filtering** is enforced during the time and days specified. Enter the time period, in 24-hour format, and select the starting and ending day of the week that Content Filtering is enforced.

Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. **Consent** can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed. Click **Filter** on the left side of the browser window, and then click the **Consent** tab.

The screenshot shows the SonicWALL Administration console in a Microsoft Internet Explorer browser window. The browser's address bar shows the URL `http://192.168.1.3/management.html`. The console has a left-hand navigation menu with tabs for General, Log, Filter, Tools, Access, Advanced, DHCP, VPN, Anti-Virus, E-mail Filter, and High Availability. The 'Filter' tab is selected, and within it, the 'Consent' sub-tab is active. The main content area is titled 'Web Usage Consent Page' and contains several configuration fields: 'Require Consent' (a checkbox), 'Maximum web usage is' (a text box with '0' and a 'minutes' label), 'User Idle Timeout is 5 minutes (configure here)', 'Consent page URL (Optional Filtering)', '*Consent Accepted* URL (Filtering Off)', '*Consent Accepted* URL (Filtering On)', 'Mandatory Filtered IP Addresses', 'Consent page URL (Mandatory Filtering)', and 'Add New Address' (a text box). There is a 'Delete Address' button below the 'Add New Address' field. At the bottom right of the configuration area are 'Update' and 'Reset' buttons. At the bottom left of the console is a 'Logout' button. A status bar at the very bottom of the console displays the message: 'STATUS: The configuration has been updated.'

Web Usage Consent Page

- **Require Consent**

Select the **Require Consent** check box to enable the **Consent** features.

- **Maximum Web usage**

In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.

- **User Idle Timeout is 5 minutes (configure [here](#))**

After a period of Web browser inactivity, the SonicWALL requires the user to agree to the terms outlined in the **Consent** page before any additional Web browsing is allowed. To configure the value, follow the link to the **Users** window and enter the desired value in the **User Idle Timeout** section.

- **Consent page URL (Optional Filtering)**

When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. You must create this Web (HTML) page. It can contain the text from, or links to an Acceptable Use Policy (AUP).

This page must contain links to two pages contained in the SonicWALL, which, when selected, tell the SonicWALL if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of "192.168.168.168".

- **"Consent Accepted" URL (Filtering Off)**

When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Type the URL of this page in the **"Consent Accepted" (Filtering Off)** field. This page must reside on a Web server and be accessible as a URL by users on the LAN.

- **"Consent Accepted" URL (Filtering On)**

When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Type the URL of this page in the **"Consent Accepted" (Filtering On)** field. This page must reside on a Web server and be accessible as a URL by users on the LAN.

Mandatory Filtered IP Addresses

- **Consent page URL (Mandatory Filtering)**

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the web browser is opened. It can contain the text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL that tells the SonicWALL that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of "192.168.168.168".

Enter the URL of this page in the **Consent** page URL (Mandatory Filtering) field and click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

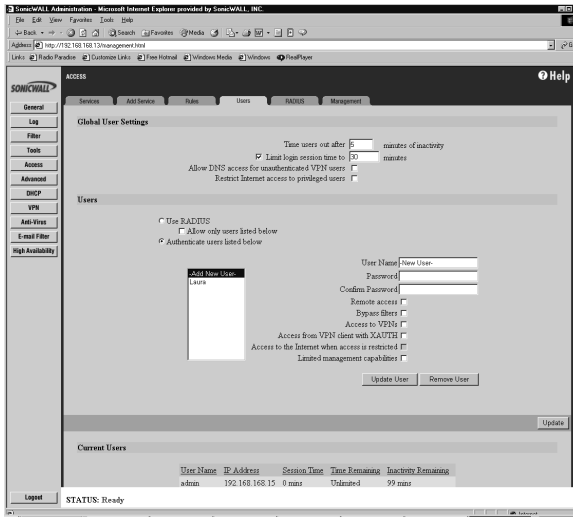
- **Add New Address**

The SonicWALL can be configured to enforce content filtering for certain computers on the LAN. Enter the IP addresses of these computers in the **Add New Address** field and click **Submit** button. Up to 128 IP addresses can be entered.

To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete Address**.

Users

Extensive features are available on the **Users** tab in the **Access** section of the Management interface. User level access can be configured for authentication, access to the network, and bypassing content filtering. Authentication can be performed using a local user database, RADIUS, or a combination of the two applications.




Global User Settings

- **Time users out after 5 minutes of inactivity** - Enter the number of allowable inactivity minutes before a user is automatically logged out of the network via the SonicWALL.
- **Limit login session time to** - Limit the length of time, in minutes, that a user is allowed to be logged into the network via the SonicWALL. When a user logs into the SonicWALL using a username and password, the user can also set the maximum login session time, but LAN it cannot be longer than the time configured by the administrator. If **Limit login session time to** is not selected, then the user has unlimited login session time on the SonicWALL.
- **Allow DNS access for unauthenticated VPN users** - Enabling this check box allows unauthenticated DNS traffic to access the DNS server over a VPN tunnel with authentication enforcement. Use this checkbox if you allow unauthenticated users to access the DNS server on your LAN.
- **Restrict Internet access to privileged users** - selecting this feature only allows Internet access to users configured on the SonicWALL.

Users

- **Use RADIUS** - Select **Use Radius** if you have configured RADIUS to authenticate users accessing the network through the SonicWALL. If you have more than 100 users requiring authentication, you must use a RADIUS server. If you select **Use RADIUS**, users must log into the SonicWALL using HTTPS in order to encrypt the password sent to the SonicWALL. If a user attempts to log into the SonicWALL using HTTP, the browser is automatically redirected to HTTPS.
- **Allow only users listed below** - Enable this setting if you have a subset of RADIUS users accessing the SonicWALL. The user names must be added to the internal SonicWALL user database before they can be authenticated using RADIUS.
- **Authenticate users listed below** - Selecting this option allows you to configure users in the local database. To add new users, fill out the **User Name**, **Password**, and **Confirm Password** fields, then select from the list of privileges allowed for the user:
 - **Remote Access** - Enable this check box if the user accesses LAN resources through the firewall from a remote location on the Internet.


 **Alert** *By enabling Remote Access, you allow unencrypted traffic over the Internet.*

- **Bypass Filters** - Select **Bypass Filters** if the user has unlimited access to the Internet from the LAN, bypassing Web, News, Java, and ActiveX blocking as well as any content filtering configured on the SonicWALL.
- **Access to VPNs** - Select the check box if the user can send information over the VPN Security Associations with authentication enforcement.
- **Access from the VPN Client with XAUTH** - Select the check box if the user requires XAUTH for authentication and accesses the firewall via a VPN client.
- **Access to the Internet when access is restricted** - select the checkbox to allow individual users access to the Internet if you have selected **Restrict Internet Access to privileged users**.
- **Limited Management Capabilities** - By selecting this check box, the user has limited local management access to the SonicWALL Management interface. The access is limited to the following pages:
 - General** - Status, Network, Time
 - Log** - View Log, Log Settings, Log Reports
 - Tools** - Restart, Diagnostics minus Tech Support Report



Tip! *The SonicWALL supports up to 100 users requiring authentication in the local database.*

Adding and Removing a User

 **Alert** *You must add a user to the Local Database to enforce access privileges.*

To add a new user, complete the following steps.

1. Log into the Management interface, click **Access**, then **Users**.
2. Highlight **-Add New User-** in the **Current User** list box.
3. Enter the name of a user into the **User Name** field.
4. Enter the user password in the **Password** and **Confirm Password** field. The password is case-sensitive.
5. Choose the privileges to be enabled for the user by selecting the appropriate check boxes.
6. Click **Update** to add the user to the SonicWALL database.
7. To remove a user, highlight the **User Name**, and click **Remove User**.

Content Filter Subscription Activation Key



SonicWALL, Inc.
1143 Borregas Drive
Sunnyvale, CA 94089-1209
Phone: 408-745-9600
Fax: 408-745-9300
E-mail: sales@sonicwall.com
Web: <http://www.sonicwall.com>

Part # 232-000266-01
Rev A. 05/03