Notes, Cautions, and Warnings

**NOTE:** A NOTE indicates important information that helps you make better use of your system.

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

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

© 2014 Dell Inc.

Trademarks: Dell™, the DELL logo, SonicWALL™, SonicWALL GMS™, Reassembly-Free Deep Packet Inspection™, Dynamic Security for the Global Network™, and all other SonicWALL product and service names and slogans are trademarks of Dell Inc.

Date 2014 - 05   P/N 232-002506-00   Rev. A
# Table of Contents

Content Filtering Client - Policy & Reporting Components ........................................ 5  
How Does Content Filtering Client - Policy & Reporting Work? ................................. 5  
How is the Client Installed on User Systems? .............................................................. 6  
How Does the Administrator Access Dell SonicWALL Content Filtering Client? ............ 6  
How Does the TreeControl Pane Work? ..................................................................... 7  
Viewing Status ............................................................................................................. 7  
Viewing Schedules ....................................................................................................... 8  
  - Adding a Schedule Group ...................................................................................... 8  
  - Editing a Schedule Group .................................................................................... 9  
  - Deleting a Schedule Group .................................................................................. 9  
Importing Certificates ................................................................................................. 10  
  - Searching for Certificates .................................................................................. 10  
  - Importing a Certificate ...................................................................................... 10  
  - Deleting a Certificate ......................................................................................... 10  
Configuring LDAP Settings ......................................................................................... 11  
  - Settings .............................................................................................................. 11  
  - Schema ............................................................................................................... 12  
  - Directory ............................................................................................................. 13  
  - Users & Groups .................................................................................................. 13  
  - Test ..................................................................................................................... 14  
Configuring User Groups ............................................................................................. 14  
  - Searching for a User Group. ............................................................................... 14  
  - Synchronizing LDAP ......................................................................................... 14  
  - Deleting User(s)/User Group(s) ....................................................................... 15  
Importing User Groups from LDAP ............................................................................ 15  
Importing Users from LDAP ......................................................................................... 17  
Importing User Groups from LDIF ............................................................................... 18  
Importing Users from LDIF .......................................................................................... 19  
Blocking/Unblocking Users ......................................................................................... 20  
Assigning Primary Groups ............................................................................................ 21  
Settings ....................................................................................................................... 23  
Custom List .................................................................................................................. 23  
Policies ......................................................................................................................... 24  
Configuring Content Filter Settings ........................................................................... 24  
Configuring Custom Lists ............................................................................................ 25  
  - Configuring Allowed Domains ......................................................................... 26  
  - Configuring Forbidden Domains ....................................................................... 27
Dell SonicWALL Content Filtering Client
Introduction

The Dell SonicWALL Content Filtering Client - Policy & Reporting Admin tool provides the interface to manage content filtering policies for clients on the network. Based on licensing on the client, the client pulls its policy from one of the registered policy servers.

The Policy Management interface provides benefits such as Global Management and User Access Control.

See the following sections:

- Content Filtering Client - Policy & Reporting Components on page 5
- How Does Content Filtering Client - Policy & Reporting Work? on page 5
- How is the Client Installed on User Systems? on page 6
- How Does the Administrator Access Dell SonicWALL Content Filtering Client? on page 6
- How Does the TreeControl Pane Work? on page 7

Content Filtering Client - Policy & Reporting Components

Content Filtering Client - Policy & Reporting Admin includes the following components:

- **Web Management Interface**—The Dell SonicWALL Content Filtering Client Web Management Interface is a Web-based interface that provides the system administrator the ability to configure, create, and apply global policies and generate activity reports for client machines connecting to the Dell SonicWALL network security appliance.

- **Policy Manager**—The policy manager for Dell SonicWALL Content Filtering Client provides an interface for administrators and permitted users to manage policies for the client machines. The policy manager is a part of the Web management interface.

- **Policy Server**—The policy server supports policy functions, including global management and user access credentials.

- **Reporting Server**—The reporting server provides summarization of raw data to be used in reports, and supports the various types of reports along with search and filtering functions.

How Does Content Filtering Client - Policy & Reporting Work?

The administrator can access the management interface directly through a MySonicWALL account. Single sign-on access allows the administrator to seamlessly move from one site or account to another without the need to remember multiple account details.

Dell SonicWALL Content Filtering Client features include dynamic updates of licensing on the firewall registered to use the content filtering client, policy application based on client licensing, notifications to administrators when the licensing expires, and alerting based on triggered thresholds.

---

Some of these features are available only when using a customer’s deployed Dell SonicWALL Global Management System (GMS) instead of the Cloud-based Content Filtering Client - Policy & Reporting Admin.
When deployed in the Cloud, the client is a customized, stripped down version of Dell SonicWALL Global Management System (GMS) providing just the client management function as a service. This means the server is optimized to perform at higher loads and also designed to be scalable when additional servers need to be added as the volume of clients requesting policies increases.

The Policy Manager is integrated with MySonicWALL and the Dell SonicWALL License Manager. Data is saved in the database and is used when a request for a policy is made to the Policy Server Web Services.

**How is the Client Installed on User Systems?**

A new Dell SonicWALL firewall is deployed on a network, registered, and licensed for Content Filtering. The feature is enabled as Enforced for Content Filtering. The administrator logs into the Policy Server and uses the Policy Manager interface to create one or more policies for client systems in the network. The administrator can also define user accounts on Dell SonicWALL Content Filtering Client with the necessary credentials to manage policies for one or more clients.

When a user tries to access the Internet and does not have the client installed, the user is taken to a Block page, which provides the information on where and how to download the client and install it.

Once the Dell SonicWALL Content Filtering Client software is installed, it contacts the Dell SonicWALL license manager to verify licensing. After a successful license check, the Dell SonicWALL license manager sends the URL of the Policy Server to the client software. The client contacts the server and downloads the policy, then uses the policy to determine the appropriate action for that user.

The software can also be installed on client systems by accessing a URL in Internet Explorer, and with an MSI package in conjunction with a domain group policy. In the final release, Dell SonicWALL software can also be installed on client systems from the command line.

**How Does the Administrator Access Dell SonicWALL Content Filtering Client?**

MySonicWALL provides links that the administrator or user can click to access the Dell SonicWALL Content Filtering Client management interface in order to create or manage client policies. Two links are provided:

- Firewall (unit) level link to manage that selected firewall
- Global level link to manage multiple firewalls under the MySonicWALL account

Single Sign-On is supported for MySonicWALL users when logging in to the Policy Server.

You can also access Dell SonicWALL Content Filtering Client from SonicOS. Administrators can click a link on the Security Services > Client CFS Enforcement page to access and manage the client. When the link is clicked, a MySonicWALL login screen (similar to the one used when licensing other services) prompts the user to log in using the MySonicWALL account. After successfully logging in, the user is forwarded from MySonicWALL to the Dell SonicWALL Content Filtering Client interface using Single Sign-On.

Logging in to Dell SonicWALL Content Filtering Client from MySonicWALL allows you to configure policies and reporting for all the Dell SonicWALL appliances that are registered to that MySonicWALL account.
When you log in to Dell SonicWALL Content Filtering Client from an individual firewall, the interface only displays configuration pages for the unit from which you logged in.

**How Does the TreeControl Pane Work?**

Dell SonicWALL Content Filtering Client uses a signed Java applet called the TreeControl to display the list of managed Dell SonicWALL appliances in the left pane. Normally, the TreeControl is only displayed when there is more than one unit. The TreeControl allows you to select a specific unit to view or work with, or to select the **GlobalView** to work with all units at the same time.

The GlobalView provides the Settings, Policies, and Client Groups pages, but does not provide the Status or Clients pages since those pertain to a single Dell SonicWALL appliance.

**Viewing Status**

The **System > Status** page displays when you first access Dell SonicWALL Content Filtering Client.

![System > Status](image)

The **System > Status** page displays the status information for the firewall from which you accessed the client. You can select which unit to display the Status page from MySonicWALL.

The status information includes the following:

- **General**—Displays the Serial Number.
- **Services**—Displays the following information:
  - License status (Current or Expired)
  - Expiration date of the license
  - Nodes or client machines currently in use with the Content Filtering Client installed
  - Total number of nodes licensed to install the Content Filtering Client

You can also synchronize the license of the unit with the license manager on this page by clicking **Synchronize with mySonicWALL.com**.
Viewing Schedules

The System > Schedules page displays the schedule groups configured on Dell SonicWALL Content Filtering Client. If you expand a specific schedule group, details of when the schedule is enforced displays.

Adding a Schedule Group

You can create a Schedule Group with multiple times in which the schedule is enforced.

To add a Schedule Group:

Step 1  Navigate to the System > Schedules page. Click the Add Schedule Group link.
Step 2  Enter the Name of the Schedule Group.
Step 3  Select the Day(s) for the schedule to be enforced.
Step 4  Specify the Start Time for the schedule to begin. Note this is in 24-hour format.
Step 5  Specify the Stop Time for the schedule to end. Note this is in 24-hour format.
Step 6  Click Add. This will save the newly created schedule, displaying the Day(s) and Time, in a list below. You can continue to create other schedules for this group by specifying the parameters, then clicking Add.
        You can also delete a schedule in the list by selecting the schedule and clicking Delete, or clicking Delete All to delete all schedules listed.
Step 7  Click OK to save a Schedule Group.
Editing a Schedule Group

To edit a schedule group that has already been created:

**Step 1** Navigate to the **System > Schedules** page.

**Step 2** Click the Configure icon of the existing schedule group you wish to edit. The Schedule Settings screen displays.

![Schedule Settings](image)

**Step 3** You can add a schedule by specifying the parameters and clicking **Add**. You can also delete a schedule in the list by selecting the existing schedule and clicking **Delete**, or clicking **Delete All** to delete all schedules listed.

**Step 4** Click **OK** to save changes made.

Deleting a Schedule Group

To delete a schedule group, navigate to the **System > Schedules** page. Select the checkbox next to the schedule group you wish to delete, then click the **Delete Schedule Group(s)** link. You can also click the Delete icon under the **Configure** column of the group you wish to delete.
Importing Certificates

The **System > Certificates** page allows administrators to perform a search for certificates. This page also allows administrators to import or delete certificates and certificate requests.

**Searching for Certificates**

To search for a user group, follow the steps listed below:

1. **Select the Certificates Name search field from the drop-down list.**
2. **To specify what part of the search field to match against, choose from the following:**
   - **Equals**—The entire field must match the text you provide.
   - **Starts with**—The field must start with the text you provide.
   - **Ends with**—The field must end with the text you provide.
   - **Contains**—The field must contain the text you provide.
3. **In the blank field, type in the text that you want to search for.**
4. **Click** **Search**.
5. **Click** **Clear** to return the search fields to their default values and clear the text field.

**Importing a Certificate**

Dell SonicWALL Content Filtering Client allows you to import a CA certificate on the **System > Certificates** page. You can import a CA certificate with a .p7b, .pem, .der, or .cer file extension.

To import a certificate, follow the steps listed:

1. **On the System > Certificates page, click the Import link.** The Import Certificate page displays.
2. **Click the Choose File button** to select a file to import from your local system.
3. **After selecting a file, click the Import button.** Note that the imported certificate may be available for use 24 hours after a successful import.

**Deleting a Certificate**

To delete a certificate, navigate to the **System > Schedules** page. Select the checkbox next to the schedule group you wish to delete, then click the Delete Schedule Group(s) link. You can also click the Delete icon under the Configure column of the group you wish to delete.
With the added support of Lightweight Directory Access Protocol (LDAP), administrators and permitted users are able to efficiently manage Users and Groups from the server. Administrators can configure their policies to apply to a specific User Directory LDAP Schema.

See the following sections:

- Configuring LDAP Settings on page 11
- Configuring User Groups on page 14

### Configuring LDAP Settings

To configure LDAP Settings, navigate to the LDAP > Settings page, located on the Policies tab. The section below provides the steps to configure LDAP Settings.

#### Settings

On the LDAP > Settings page, navigate to the Settings tab. Configure the following fields:

- **Name or IP address**—Enter the name or IP address for the LDAP Server.
- **Port Number**—Enter the TCP port number running the LDAP service. You can also choose one of the **Standard Port Choices** from the drop-down list. The default LDAP port is 389.
- **Server Timeout**—Specify the connection timeout period value in seconds. After this period of time, the client will stop attempting to connect to the server.
- Select the Authentication Method from the following choices:
  - **Anonymous login**—This option allows you to login without the LDAP server authenticating information, or “binding” to the server.
  - **Give login name/location in tree**—With this option selected, you will have to provide the user’s distinguished name under the Login User Name as well as the Login Password. Be aware that this is different from the user login ID. For example, John Doe may have a user login ID as ‘jdoe’. However, you would enter ‘John Doe’ in this field. When selecting this option, you will also need to provide User Tree for Login to Server, located on the LDAP > Settings > Directory tab.
  - **Give bind distinguished name**—With this option selected, you will have to provide the Bind Distinguished Name and Login Password. The bind distinguished name is the full distinguished name (DN) used to bind to the LDAP server.
- **Protocol Version**—Select the LDAP version from the drop-down list.
- **Use TLS (SSL)**—Select the Use TLS (SSL) checkbox to enable the authentication of servers and clients and encryption of messages on LDAP.
Click **Update** to save these settings.

![LDAP Server Settings](image)

**Schema**

On the **LDAP > Settings** page, navigate to the **Schema** tab. Select the **LDAP Schema** from the drop-down list. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values.

If the LDAP Schema you wish to use is not an option in the drop-down list, select **User Defined**. The following fields are available for you to configure:

**User Objects**

- **Object Class**—This defines which attribute represents the individual user account to which the next two files apply.
- **Login Name Attribute**—The LDAP attribute that corresponds to the User ID.
- **User Group Membership Attribute**—The LDAP attribute that lists the groups or mailing lists that the user is a member of.
- **Additional User Group ID Attribute**—The LDAP attribute that allows for a schema to set additional memberships for a user. If the **Use** checkbox for this field is selected, then when a user object is found with one or more instances of the specified attribute, a search for additional user groups matching the specified attribute is made in the LDAP directory. Note that this attribute may be inefficient to the load performance of your LDAP server.

**User Group Objects**

- **Object Class**—The object class of the group for the LDAP schema.
- **Member Attribute**—The LDAP attribute that corresponds to group members.
- **Additional User Group Match Attribute**—The LDAP attribute that allows for a schema to set additional memberships for a user group. If a group is found with this attribute set to the specified value, then the user will also be made a member of that group. Note that this attribute may be inefficient to the load performance of your LDAP server.
- **Read from Server**—Click this button to retrieve the LDAP schema from the LDAP server. You can then select to **Automatically update the schema configuration** or **Export details of the schema**. Click **OK**.

Click **Update** to save these settings.

### Directory

On the **LDAP > Settings** page, navigate to the **Directory** tab. Depending on the Authentication Method you specified on the **Settings** tab, you may have to enter the **Primary Domain** and **User Tree for Login to Server** fields.

If you selected **Anonymous Login** or **Give bind distinguished name**, you will only need to specify the **Primary Domain**.

If you selected **Give login name/location in tree**, specify the **Primary Domain** and the **User Tree for Login to Server** fields. This specifies the tree in the directory that includes the user object for the user that you configured on the **Settings** tab.

Click **Update** to save these settings.

### Users & Groups

On the **LDAP > Settings** page, navigate to the **Users & Groups** tab. The LDAP User Settings section allows you to **Mirror LDAP Users and User Groups Automatically** by selecting the checkbox, and then specifying the **Refresh Period** in hours.

Click **Update** to save these settings.
Test

On the LDAP > Settings page, navigate to the Test tab. This tab allows you to test the LDAP settings you have configured. Enter a valid LDAP User name and Password, then click the Test button. After clicking the Test button, the client will retrieve any messages from the LDAP Server, as well as returned user attributes in the appropriate fields.

Configuring User Groups

The LDAP > User Groups page allows you to conduct a search for User Groups, synchronize LDAP servers, or Import Users and Groups from the LDAP server or a Local Directory.

Searching for a User Group

The LDAP > User Groups Search is useful if you have a high number of user groups and need to find one or more with specific text in the Name, Mirrored From, User Name, or Type fields.

To search for a user group, follow the steps listed below:

Step 1  Select the user group field to be searched. You can select either the Name, Mirrored From, User Name, or Type fields.

Step 2  To specify what part of that field to match against, choose from the following:

• Equals—The entire field must match the text you provide.
• Starts with—The field must start with the text you provide.
• Ends with—The field must end with the text you provide.
• Contains—The field must contain the text you provide.

Step 3  In the blank field, type in the text that you want to search for.

Step 4  Click Search.

Step 5  Click Clear to return the search fields to their default values and clear the text field.

Synchronizing LDAP

The LDAP > User Groups page allows you to synchronize your LDAP to easily authenticate users. Click the Synchronize LDAP link to efficiently synchronize the list of User Groups you want added to the LDAP directory.

Note that synchronizing user groups from LDAP may do the following:

• Replicates any membership changes for user groups listed in the User Groups Mirrored from LDAP list.
• Removes any deleted user groups from the User Groups Mirrored from LDAP list.
• Removes client groups for the deleted user groups.
Deleting User(s)/User Group(s)

To delete user groups from the LDAP > User Groups page, select the check box corresponding to the User Group you wish to delete. Then, click the Delete User(s)/User Group(s) link or click the Delete icon for that group.

Importing User Groups from LDAP

To import user groups from your LDAP server, click the Import User Groups from LDAP link. A list of available user groups from the LDAP server displays. You can then select the groups to import and click the Save Selected button to add those user groups to the LDAP user groups.

To remove user group(s), select the group, then click the Remove from List button.
If there are no user groups found on the LDAP server, a list of possible reasons will display. See the image below.
Importing Users from LDAP

To import users from your LDAP server, click the **Import Users from LDAP** link. A list of available users from the LDAP server displays. You can then select the users to import and click the **Save selected** button to add those users to your LDAP users.

There are several ways to remove users:

- **All selected users**—Select the users from the list, then click the **All selected users** radio button. Click the **Remove from list** button.

- **Any user whose [Name/Description/Location] contains [field]**—Select either **Name**, **Description** or **Location** from the drop-down list, then specify the field. For example, you may select **Location**, then specify the field as “San Jose” to find all users that located in San Jose. Click the **Remove from list** button to remove these users from the list.

- **All users [at/ at or under]**—This option can be used to remove users under an email alias or similar groups, such as “engineering@sonicwall.com.” By clicking the **Remove from list** button, it will remove all users listed in the engineering@sonicwall.com group.
If there are no user groups found on the LDAP server, a list of possible reasons will display. See the image below.

![LDAP Users Search](image)

**Importing User Groups from LDIF**

The Content Filtering Client also supports importing from DAP Data Interchange Format (LDIF) files. LDIF is a standard plain text data interchange format for representing LDAP directory content. While LDAP is the recommended format to use, LDIF is a more secure method for administrators because they do not have to connect to a server to retrieve information, unlike LDAP.

LDIF files must contain schema attributes that are the same as the current LDAP schema settings. The following schema is configured for User Groups:

- LDAP Schema - Microsoft Active Directory
- Group Object class - group
- Member attribute - member

If you need to edit the User Groups, you will need to upload a new LDIF file with the changes.
To import an LDIF file, click the **Import User Groups from LDIF** link. Click the **Browse** button to select the LDIF file. Then, click **Import**.

### Importing Users from LDIF

Similarly to Importing User Groups from LDIF, you can Import Users from LDIF files. While LDAP is the recommended format to use, LDIF is a more secure method for administrators because they do not have to connect to a server to retrieve information, unlike LDAP. LDIF files must contain schema attributes that are the same as the current LDAP schema settings. The following schema is configured for User Groups:

- LDAP Schema - Microsoft Active Directory
- User Object class - user
- Login name attribute - sAMAccountName
- User group membership attribute - memberOf
- Use Additional User group membership attribute - false
- Group Object class - group
- Member attribute - member

**Note**

If you need to edit the Users, you will need to upload a new LDIF file with the changes.

To import an LDIF file, click the **Import Users from LDIF** link. Click the **Browse** button to select the LDIF file. Then, click **Import**.
Blocking/Unblocking Users

To block users:

**Step 1** Click the **Block/Unblock Users** link. The Block/Unblock Users dialog box displays.

**Step 2** Select the username you wish to block from the list of Available Users.

**Step 3** Then, click the > button to move the user to the Blocked Users list. Click **OK** to finish.
To unblock users:

**Step 1**  Click the **Block/Unblock Users** link. The Block/Unblock Users dialog box displays.

**Step 2**  Select the username you wish to unblock from the list of Blocked Users.

![Block/Unblock Users dialog box](image)

**Step 3**  Then, click the < button to move the user to the Available Users list. Click **OK** to finish.

![Block/Unblock Users dialog box](image)

### Assigning Primary Groups

The **LDAP > User Groups** page allows you to assign users to primary groups. Primary Groups are essential in organizing users and ensuring the proper policies are assigned to each user. In a typical situation, an individual user may belong to multiple groups, each of which has a variety of policies enforced. To ensure the correct policies are applied to this user, the administrator is recommended to assign the primary group to which the user should belong.

**Note**

If a user is not assigned to a Primary Group, Dell SonicWALL will assign the user to the Primary Group that is believed to be best suited.
To assign primary groups to users:

**Step 1** Click the **Assign Primary Group** link. A dialog window will display with your list of groups and users.

![Assign Primary Group to Users dialog window](image)

This may take several minutes to populate.

**Step 2** Select the **Primary Group** from the drop-down list at the top of the window. Based on the Primary Group selected, the **Users Not Having Selected Group as Primary** and **Users Having Selected Group as Primary** lists will populate.

![Assign Primary Group drop-down list](image)

**Step 3** Select a username from the list, then click the `<` button to add this user to the **Users Not Having Selected Group as Primary**. This user will not have the selected Primary Group as his/her primary group.

Select a username from the list, then click the `>` button to add this user to the **Users Having Selected Group as Primary**. This user will have the selected Primary Group as his/her primary group.

**Step 4** Click the **OK** button to finish and save changes.
Navigate to the **Content Filter** menu on the Dell SonicWALL client, located on the Policies tab. You can configure Enforcement settings, Custom List settings, and Policy settings.

See the following sections:

- **Settings** on page 23
- **Custom List** on page 23
- **Policies** on page 24
- **Configuring Content Filter Settings** on page 24
- **Configuring Custom Lists** on page 25

### Settings

From the **Content Filter > Settings** page, you can manage the following:

- **Enforcement Settings**—Select the checkbox to *Enable Content Filtering Client behind the Firewall*. Dell SonicWALL recommends enabling this checkbox when the Content Filtering Service is not active on your firewall, or if the Content Filtering Client policies are to override the firewall’s policies. Click the **Update** button to save changes.

- **Web Page to Display when Blocking**—Choose to display the default Web page when blocking or customize your own Web page.

- **CFS Settings**—Select the checkbox to *Enable HTTPS Content Filtering*. HTTPS Content Filtering is based on IP and hostname. HTTP Content Filtering may perform redirects to enforce authentication or provide a block page.

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

  - **Block Access to URL**—This option prevents the browser from displaying the requested URL to the user.
  - **Log Access to URL**—This option records the requested URL in the log.

### Custom List

From the **Content Filter > Custom List** page, you can manage the following:

- **Allowed Domains**—Add, import, or delete Allowed Domains that users are allowed to access with their Web browser.

- **Forbidden Domains**—Add, import, or delete Forbidden Domains that users are forbidden to access with their Web browser.

- **Keywords**—Add, import, or delete Keywords that the client system uses to offer protection against Web sites that have not explicitly been added to the Master Database or defined as a custom URL.
Policies

The Content Filter > Policies page allows you to search for, add, and delete policies that block objectionable Web sites.

- **Policies Search**—This function allows you to search for policies by Name that Equals, Starts with, Ends with, or Contains certain characters.

- **Policies**—Allows you to create, edit, and delete policies.

Configuring Content Filter Settings

To configure Content Filter settings, perform the following steps:

**Step 1** On the Policies tab, navigate to the Content Filter > Settings page and select the Enable Content Filtering Client behind the Firewall checkbox to enforce content filtering policies from behind the firewall.

**Step 2** Click Update.

**Step 3** You can choose to display the default Web page when blocking or customize your own Web page.
   - To display the default page, leave the field blank. Then, click Update.
   - To display a custom Web page, use the field to enter the HTML code. Then, click Update.

**Step 4** The CFS Settings section allows you to enable HTTPS Content Filtering, block traffic to sites when the server is unavailable, and set preferences for your URL cache. For more information, see Settings on page 23.
Configuring Custom Lists

The **Content Filter > Custom List** page is used to block or allow access to specific domain names. This enables an organization to block access to domains that are not in the content filter list, allow access to domains in the content filter list, or only allow access to specific domains.

Allowed domains are domains that users can access, regardless of whether they appear in the content filter list. Allowed domains are particularly useful for dedicated systems that are only allowed to access specific websites. Up to 256 entries are supported in the Allowed Domains list.

Forbidden domains are domains that users are not allowed to access. This is useful when a website disrupts a corporate or educational environment. To find out which websites are most frequently accessed, refer to the Top Web Site Hits section of the log report. Up to 256 entries are supported in the Forbidden Domains list.

Tip: Importing a .txt file with one domain per line is the easiest way to add multiple domains to a forbidden/allowed list.

From the Dell SonicWALL Custom List page, you can add, import or delete Allowed Domains, Forbidden Domains and Keywords.

On the **Policies** tab, navigate to the **Content Filter > Custom List** page.

See the following sections for information about configuring Custom Lists:

- Configuring Allowed Domains on page 26
- Configuring Forbidden Domains on page 27
- Configuring Keywords on page 29
Configuring Allowed Domains

The Content Filter > Custom List screen allows you to add, import, or delete allowed domains.

Adding Allowed Domains

To add an allowed domain, navigate to the Allowed Domains section and follow the steps listed:

**Step 1** Click Add New Allowed Domain. The domain pop-up displays.

![Add Allowed Domain](image)

**Step 2** Enter domain(s) that you would like to allow. To separate multiple domains, use a semicolon between each domain.

*Note* Enter the domain name only. For example, “yahoo.com.” Do not include “http://.” Entering “yahoo.com” will also allow access to www.yahoo.com, my.yahoo.com, sports.yahoo.com, and so on.

**Step 3** Click OK. When the client system refreshes, the additional allowed domains are displayed.

Importing Allowed Domains

To import a list of allowed domains, navigate to the Allowed Domains section and follow the steps listed:

**Step 1** Click the Import... link. The Import Allowed Domain Names screen displays.

![Import Allowed Domain Names](image)

**Step 2** Click Choose File to select a .txt file from your local system. Verify that the .txt file has one domain per line.
Step 3  Click the **Import** button. When the client system refreshes, the imported allowed domains display.

Deleting Allowed Domains

To delete an allowed domain, navigate to the **Allowed Domains** section and follow the steps listed:

**Step 1**  Select the **Domain** checkbox to delete all allowed domains. To delete an individual domain from the Allowed Domains list, select the checkbox of the domain you wish to remove.

**Step 2**  Click the **Delete Allowed Domain(s)** link. A dialog box displays to confirm deleting the selected entries.

**Step 3**  Click **OK**. The selected entries are deleted and removed from the Allowed Domain list.

Configuring Forbidden Domains

From the **Content Filter > Custom List** screen, navigate to the **Forbidden Domains** section to add, import, or delete forbidden domains.
Adding Forbidden Domains

To add Forbidden Domains, follow the steps listed:

**Step 1**  Click the **Add New Forbidden Domain** link. The Add Forbidden Domain pop-up displays.

**Step 2**  Enter domain(s) that you would like on the forbidden list. To separate multiple domains, use a semicolon between each domain.

**Step 3**  Click **OK**. When the system refreshes, the new added forbidden domains will be displayed.

Importing Forbidden Domains

To import a list of forbidden domains, navigate to the **Forbidden Domains** section and follow the steps listed:

**Step 1**  Click the **Import...** link. The **Import Forbidden Domain Names** screen displays.

**Step 2**  Click **Choose File** to select a .txt file from your local system. Verify that the .txt file has one domain per line.

**Step 3**  Click the **Import** button. When the system refreshes, the imported forbidden domains display.
Deleting Forbidden Domains

To delete a forbidden domain, navigate to the Forbidden Domains section and follow the steps listed:

**Step 1**  Select the **Domain** checkbox to delete all forbidden domains. To delete an individual domain from the Forbidden Domains list, select the checkbox of the domain you wish to remove.

![Forbidden Domains Table]

**Step 2**  Click the **Delete Forbidden Domain(s)** link. A dialog box displays to confirm deleting the selected entries.

**Step 3**  Click **OK**. The selected entries are deleted and removed from the Forbidden Domain list.

Configuring Keywords

From the Content Filter > Custom List screen, navigate to the Keywords section to add, import, or delete keywords.

Adding Keywords

To add Keywords, navigate to the Keywords section and follow the steps listed below:

**Step 1**  Click the **Add New Keyword** link. The keyword pop-up displays.

![Add Keyword Pop-up]

**Step 2**  Enter keyword(s) that you would like on the Keywords list. To separate multiple keywords, use a semicolon between each keyword.

**Step 3**  Click **OK**. When the system refreshes the newly added keywords display.
Importing Keywords

To import a list of keywords, navigate to the Keywords section and follow the steps listed:

**Step 1** Click the Import... link. The Import URL Keywords screen displays.

**Step 2** Click Choose File to select a .txt file from your local system. Verify that the .txt file has one keyword per line.

**Step 3** Click the Import button. When the system refreshes, the imported keywords display.

Deleting Keywords

To delete a keyword, navigate to the Keywords section and follow the steps listed:

**Step 1** Select the Keyword checkbox to delete all keywords. To delete an individual keyword from the list, select the checkbox of the keyword you wish to remove.

**Step 2** Click the Delete Keyword(s) link. A dialog box displays to confirm deleting the selected entries.

**Step 3** Click OK. The selected entries are deleted and removed from the Keywords list.
Content Filter Policies

Policies control content filtering behavior on client machines. You can add new policies by making a copy of the Default Policy or another policy, changing the settings, or by creating a completely new policy.

See the following sections:
- Searching for a Policy on page 31
- Cloning & Creating a New Content Filter Policy on page 31

Searching for a Policy

The Policies Search area at the top of the Content Filter > Policies page is useful if you have a high number of policies and need to find one or more with specific text in the Name field.

To search for a policy, follow the steps listed below:

Step 1 Select the policy field to be searched. You can select either the Name or Comment field.
Step 2 To specify what part of that field to match against, choose from the following:
- **Equals**—The entire field must match the text you provide.
- **Starts with**—The field must start with the text you provide.
- **Ends with**—The field must end with the text you provide.
- **Contains**—The field must contain the text you provide.
Step 3 In the blank field, type in the text that you want to search for.
Step 4 Click **Search**.
Step 5 Click **Clear** to return the search fields to their default values and clear the text field.

Cloning & Creating a New Content Filter Policy

The Content Filtering Client includes a Default Content Filter Policy that you can access from the Content Filter > Policies page. The Default Policy provides standard settings for content filtering on client machines. The Default Policy is configured to be moderately strict, and is suitable for use with most Content Filtering Clients. Note that the Default Policy cannot be edited or deleted.

You can create a new policy or clone a policy from an existing policy, such as the Default Policy. Dell SonicWALL recommends cloning the Default Policy or an existing policy, and then editing specific fields within the cloned policy as an efficient way to create a new policy that is similar to the existing policy.

On the Policies tab, the Content Filter > Policies page shows the Default Policy as the first policy.
To clone a policy or add a new policy, perform the following steps:

**Step 1**  
To clone an existing policy, click the Clone icon, located under the Configure column, in the row for the policy that you wish to clone.

To create a new policy, click **Add New Policy**.

**Step 2**  
The Add Policy window displays.

On the Policy tab, edit the **Name** field for the new policy. For a cloned policy, the fields are automatically populated, which can be changed.
Step 3  Click the URL List tab. The URL list of forbidden categories displays. If the policy is cloned, you can keep the default settings selected or select the boxes of the categories you would like to block. To select all categories listed, check the Select all Categories checkbox.

Step 4  Next, click the Settings tab. Configure the following settings:

- Under the Custom List Settings section, select the Source of Allowed Domains. This setting allows you to specify a list of allowed domains for the client to refer to when content is filtered. The Domains that match this list will be allowed. The following sources for the allowed domains list are available:
  - None—None of the Allowed Domain lists are referred to when content is filtered.
  - Global—Uses the list of Allowed Domains that was created in the Content Filtering > Custom List page. For more information, refer to Configuring Custom Lists on page 25.
  - Per Policy—Uses the Allowed Domains list created in the Custom List tab of this dialog window.

- Under the Custom List Settings section, select the Source of Forbidden Domains. This allows you to specify a list of forbidden domains for the client to refer to when content is filtered. The Domains that match this list will be blocked. The following sources for the forbidden domains list are available:
  - None—None of the Forbidden Domains lists are referred to when content is filtered.
  - Global—Uses the list of Forbidden Domains that was created in the Content Filtering > Custom List page. For more information, refer to Configuring Custom Lists on page 25.
  - Per Policy—Uses the Forbidden Domain list created in the Custom List tab of this dialog window.
Under the Custom List Settings section, select the source of the **Keywords**. This allows you to specify a list of keywords for the client to refer to when content is filtered. The Keywords that match this list will be blocked. The following sources for the keywords list are available:

- **None**—None of the Keyword lists are referred to when content is filtered.
- **Global**—Uses the list of Keywords that was created in the Content Filtering >Custom List page. For more information, refer to Configuring Custom Lists on page 25.
- **Per Policy**—Uses the Keywords list that is created in the Custom List tab of this dialog window.

**Step 5** Under Safe Search Enforcement Settings, select the checkbox to **Enable Safe Search Enforcement**. This setting enables safe browsing options for certain search engines, such as Google and Yahoo. Safe Search is a setting that filters out explicit adult content from Web and image search results.

**Step 6** Under the YouTube for Schools section, select the **Enable YouTube for Schools** checkbox and enter the **School ID**. This feature filters content per your school ID and determines which content is acceptable for students.

**Step 7** To configure the time schedule for Content Filtering enforcement, select one of the options from the drop-down list under **Filter Forbidden URLs by time of day**.

**Step 8** Navigate to the **Custom List** tab. You will use this screen if you selected “Per Policy” as the source of allowed domains, forbidden domains, or keywords in the **Settings** tab.
Step 9 In the **Content** text-field, enter the allowed domain, forbidden domain, or keyword, and then click the **Add** button. This adds your entry into the respective list.

Step 10 To edit an existing domain or keyword in the lists, select the desired row, edit the domain or keyword in the text field, and then click the **Update** button.

Step 11 To remove a domain or keyword from the lists, select the desired row, and then click the **Remove** button. You can also remove all the domains or keywords from a list by clicking the **Remove All** button.

Step 12 Click **OK**.

---

**Note** Items added to the Custom List tab (Allowed Domains, Forbidden Domains, or Keywords) are applied only when the Settings tab has "Per Policy" selected for Custom List Settings.
Navigate to the **Enforcement** menu on the Dell SonicWALL Content Filtering Client, located on the Policies tab. You can configure enforcement policies, as well as settings for Client Groups and Clients.

This chapter includes the following sections:

- Cloning & Creating a New Enforcement Policy on page 37
- Configuring Client Groups on page 39
- Configuring Clients on page 42

## Cloning & Creating a New Enforcement Policy

Content Filtering Client includes a Default Desktop Policy and a Default Mobile Policy that you can access from the **Enforcement > Policies** page. The Default Desktop and Default Mobile policies provide standard settings for content filters. These policies are configured to be moderately strict, and is suitable for use with most Content Filtering Clients. They cannot be edited or deleted.

You can create a new policy or clone a policy from an existing policy, such as the Default Desktop Policy. Dell SonicWALL recommends cloning the Default Desktop Policy or an existing policy, and then editing specific fields within the cloned policy as an effective way to create a new policy that is similar to the existing policy.

Note that the client does not assign a content filtering policy to the Default Desktop Policy. Content filtering policies are assigned only to the Default Mobile Policy.

> When all settings are left as the default settings, all desktop devices will acquire the policies as defined in the Default Desktop Policy. Likewise, all mobile devices, such as a laptop, will acquire the policies defined in the Default Mobile Policy.

To clone a policy or add a new policy, navigate to the **Enforcement > Policies** page, and perform the following steps:

### Step 1

To clone an existing policy, click the Clone icon under Configure in the row for the policy that you want to clone.
To create a new policy, click **Add New Policy**.

**Step 2** The Add Policy dialog window displays.

On the **General** tab, edit the **Name** and **Comment** fields for the new policy. For a cloned policy, the fields are already populated with text indicating the cloning, which can be changed.

**Step 3** On the Agent Version Settings section, select the desired **Agent Version** (specific release) from the drop-down list. This allows the policy to be configured for a specific Agent version. You can select **Stable**, **Latest**, or possibly a specific release.
Step 4  Next, navigate to the **Content Filter** tab.

![Content Filter tab](image)

Step 5  Select the **Default** Local Policy from the drop-down menu.

Step 6  Select a **Scheduled** Policy from the drop-down list. A scheduled policy is a policy that has Schedule associated to it. The policy is used for enforcement during the scheduled time interval configured. Note that only policies with a schedule set appear in this drop-down list.

Step 7  Click **OK**.

### Configuring Client Groups

Administrators can configure client groups on the **Enforcement > Client Groups** page. You can edit existing client groups or create new client groups. The Default Client Group can be edited, but cannot be deleted. All clients requesting a policy for the first time are automatically added to the Default Client Group and are served with the policy defined for this group. The administrator can move a client to a different client group after the client is initially added to the Default Client Group.

**Note**

All desktop devices will acquire the policies as defined in the Default Desktop Policy. All mobile devices, such as a laptop, will acquire the policies defined in the Default Mobile Policy. If you would like to modify the service associated with the client defined default policy, you must clone the Default Desktop or Mobile Policy, then add/remove the services that the default client groups contain.

The **Enforcement > Client Groups** page is available on the Policies tab.
See the following sections for information about configuring client groups:

- Searching for Client Groups on page 40
- Adding or Editing Client Groups on page 41
- Deleting Client Groups on page 41

User Groups from LDAP & LDIF

If you imported User Groups using LDAP or LDIF on the LDAP > User Groups page, those user groups will appear on this page for Policy assignment. User groups imported with LDAP or LDIF have different adding and deleting caveats than groups that are added from the Enforcement > Client Groups page.

To add a new User Group based Client Group, you will have to navigate to the LDAP > User Group page and import the User Group from LDAP or LDIF. To delete a User Group based Client Group, you will need to move the Clients to an available Client Group before deleting.

Searching for Client Groups

The Client Groups Search section on the Enforcement > Client Groups page provides a way to search the list of client groups. This is useful if you have a large number of client groups and need to find one or more with specific text.

To search for a client group:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select the client group field to be searched. You can select the Name, Type, Local Policy, Remote Policy, or Comment field from the drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To specify what part of that field to match against, choose among the following operators:</td>
</tr>
<tr>
<td></td>
<td>• Equals—The entire field must match the text you provide.</td>
</tr>
<tr>
<td></td>
<td>• Starts with—The field must start with the text you provide.</td>
</tr>
<tr>
<td></td>
<td>• Ends with—The field must end with the text you provide.</td>
</tr>
<tr>
<td></td>
<td>• Contains—The field must contain the text you provide.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the blank field, type in the text that you want to search for.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Search.</td>
</tr>
<tr>
<td></td>
<td>Click Clear to return the search fields to their default values and clear the text field.</td>
</tr>
</tbody>
</table>
Adding or Editing Client Groups

To add or edit a client group, perform the following steps:

**Step 1** On the **Policies** tab, navigate to the **Enforcement > Client Groups** page.

**Step 2** To add a new client group, click **Add New Client Group**. To edit an existing client group, click the Edit icon in the Configure column for the client group you want to edit.

**Step 3** The Add Client Group window displays. Type a descriptive name into the **Group Name** field.

![Client Group Settings Window](image)

**Step 4** In the **Comment** field, enter a descriptive comment.

**Step 5** Select a policy for the group from the **Desktop Policy** drop-down list. All existing policies are available for selection.

**Step 6** Select a policy for the group from the **Mobile Policy** drop-down list. All existing policies are available for selection.

**Step 7** Click **OK** to complete.

Deleting Client Groups

You can delete one or more host-based client groups on the **Enforcement > Client Groups** page.

To delete one or more client groups:

**Step 1** Navigate to the **Enforcement > Client Groups** page.

**Step 2** To delete all client groups except the default, select all checkboxes by selecting the checkbox next to the **Name** column heading, then click **Delete Client Group(s)**.

**Step 3** To delete multiple client groups, select the checkbox next to each one you want to delete, then click **Delete Client Group(s)**.

**Step 4** To delete a single client group, click the trash can icon in the same row. Or, select the checkbox next to it and then click **Delete Client Group(s)**.

**Note** The Default Client Group and User Group-based Client Groups cannot be deleted, and will have a grayed-out icon Trash icon.
Configuring Clients

Administrators can configure clients on the Enforcement > Clients page. You can delete clients, move clients from one client group to another, and block or unblock clients. You can also use the Search function to search for clients.

Administrators can select a custom policy for the Default Client Group, or leave the Default Policy configured. The administrator can move a client to a different client group after the client is initially added to the Default Client Group.

Searching for Clients

The Clients Search area at the top of the page provides a way to search the list of clients. This is useful if you have a number of clients and need to find one or more with a specific value in the Host Name, Host IP, Client Group, or Last Contacted field.

To search for a client:

**Step 1** Navigate to the Enforcement > Clients page and select the client field to be searched. You can select the Host Name, Client Group, Client Version, Allowed, and Client Users field.

**Step 2** To specify what part of that field to match against, choose among the following operators:

- **Equals** – The entire field must match the text you provide.
- **Starts with** – The field must start with the text you provide.
- **Ends with** – The field must end with the text you provide.
- **Contains** – The field must contain the text you provide.

**Step 3** In the blank field, type in the text or value that you want to search for.

**Step 4** Click Search.

**Step 5** Click Clear to return the search fields to their default values and clear the text field.
Deleting Clients

You can delete one or more clients from the Clients table on the Enforcement > Clients page. To delete one or more clients:

**Step 1** On the Policies tab, navigate to the Enforcement > Clients page.

**Step 2** To delete all clients, select the checkbox next to the Host Name column heading, then click Delete Client(s).

**Step 3** To delete multiple clients, select the checkbox next to each one you want to delete, then click Delete Client(s).

**Step 4** To delete a single client, click the trash can icon in the same row. Or, select the checkbox next to it and then click Delete Client(s).

**Step 5** Click OK in the confirmation dialog box.

Blocking Multiple Clients

The administrator can prevent clients from accessing the Internet by using the Block Client(s) function.

To block multiple clients, follow the steps below:

**Step 1** Navigate to the Enforcement > Clients page.

**Step 2** Select the checkbox next to the clients you want to block.

**Step 3** Click the Block Client(s) link at the bottom of the page.

**Step 4** You will be asked to confirm blocking these clients. Click Yes. The client now displays as blocked on the Enforcement > Clients page.

This allows the client to recover the licenses back into the pool. After a blocked client gets a policy update from client, Dell SonicWALL Content Filtering Client will wipe all content filter policies from the client machine. From this point on, there is no content filter protection on the client machine. If this client is behind a firewall that is enforcing client content filtering, then this client is not allowed to access the Internet.
Blocking a Single Client

There are two methods to block a single client. You can either follow the steps listed for Blocking Multiple Clients on page 43, or you can follow the steps below:

**Step 1** Navigate to the Enforcement > Clients page.
**Step 2** Click the configure icon of the client you wish to block. The client settings window displays.
**Step 3** Click the Block checkbox. Then, click OK.

This allows the client to recover a license back into the pool. After a blocked client gets a policy update from client, Dell SonicWALL Content Filtering Client will wipe all content filter policies from the client machine. From this point on, there is no content filter protection on the client machine. If this client is behind a firewall that is enforcing client content filtering, then this client is not allowed to access the Internet.

Unblocking Clients

Unblocking clients allows the client to receive content filter protection. Unblocking the client will also allow access to the Internet if it is a client behind a firewall enforcing client content filtering.

To unblock one or multiple clients, follow the steps listed below:

**Step 1** Navigate to the Enforcement > Clients page.
**Step 2** Select the checkbox next to the clients you want to unblock.
**Step 3** Click the Unblock Client(s) link at the bottom of the page.
**Step 4** You will be asked to confirm unblocking these clients. Click Yes. The clients now display as unblocked on the Enforcement > Clients page.
Moving Clients

Moving clients allows you to move a client to a different client group. Moving clients is only supported for Host-based groups. To move clients, follow the steps listed:

**Step 1** Navigate to the **Enforcement > Clients** page.

**Step 2** Select the checkbox next to the clients you want to move.

**Step 3** Click the **Move Client(s)** link at the bottom of the page. A pop-up window displays asking you to select the destination client group. Select the radio button, then click **OK**.

![Move Client(s) window](image)
Troubleshooting the Policy & Reporting Admin

See the following sections for Content Filtering Client errors:
- Installation Errors on page 47
- Content Filtering Client Errors on page 47

Installation Errors

There are two specific errors that may occur during installation of the Content Filtering Client:
1. An invalid serial number is entered.
2. The serial number entered is not licensed for the Content Filtering Client.

In both of these install errors, the installation will fail and a notepad with log messages will display. You can save this log file for diagnostic reference. You may need to use this log if you contact Dell SonicWALL Support.

Content Filtering Client Errors

The following section allows you to view the various error messages that may display on the Content Filtering Client. The images in this section may be useful for diagnostics.

Figure 1  Content Filtering Client: Expired License

The following error message displays when the Content Filtering Client license has expired. Log in to your MySonicWALL account to renew your service subscription.
Figure 2  Content Filtering Client: Node Count Exceeded

The following error message displays when the Content Filtering Client node count has been exceeded. Navigate to the Security Services > Client CFS Enforcement page to configure the correct number of nodes.

Figure 3  Content Filtering Client: No Policy Specified

The following error message displays when the Content Filtering Client policy is not specified. Navigate to the Security Services > Client CFS Enforcement page to configure the correct number of nodes.
The following error message displays when the Content Filtering Client is blocked from use. Navigate to the Security Services > Client CFS Enforcement page to unblock the client.

The following error message displays when the Content Filtering Client is set to log only. The client is not blocking access to Websites. Navigate to the Security Services > Client CFS Enforcement page to change the client to block.

For more information and related documentation, see the Dell SonicWALL Support Site:
https://support.software.dell.com/
https://forum.sonicwall.com