Enforced Client Policy & Reporting Server (EPRS) 2.3
Administration Guide
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>5</td>
</tr>
<tr>
<td>About this guide</td>
<td>5</td>
</tr>
<tr>
<td>Document contents</td>
<td>5</td>
</tr>
<tr>
<td>Guide conventions</td>
<td>6</td>
</tr>
<tr>
<td>About EPRS</td>
<td>6</td>
</tr>
<tr>
<td>How EPRS Works</td>
<td>6</td>
</tr>
<tr>
<td>How to access CFC</td>
<td>7</td>
</tr>
<tr>
<td>Navigating the interface</td>
<td>7</td>
</tr>
<tr>
<td>Installing the client on user systems</td>
<td>8</td>
</tr>
<tr>
<td>System</td>
<td>9</td>
</tr>
<tr>
<td>Status</td>
<td>9</td>
</tr>
<tr>
<td>Schedules</td>
<td>9</td>
</tr>
<tr>
<td>Adding a Schedule Group</td>
<td>10</td>
</tr>
<tr>
<td>Editing a Schedule Group</td>
<td>11</td>
</tr>
<tr>
<td>Deleting a Schedule Group</td>
<td>12</td>
</tr>
<tr>
<td>Certificates</td>
<td>12</td>
</tr>
<tr>
<td>Searching for Certificates</td>
<td>12</td>
</tr>
<tr>
<td>Importing a Certificate</td>
<td>13</td>
</tr>
<tr>
<td>Deleting a Certificate</td>
<td>13</td>
</tr>
<tr>
<td>LDAP</td>
<td>14</td>
</tr>
<tr>
<td>Settings</td>
<td>14</td>
</tr>
<tr>
<td>Schema</td>
<td>15</td>
</tr>
<tr>
<td>Directory</td>
<td>17</td>
</tr>
<tr>
<td>Users &amp; Groups</td>
<td>18</td>
</tr>
<tr>
<td>Test</td>
<td>19</td>
</tr>
<tr>
<td>Google Directory</td>
<td>20</td>
</tr>
<tr>
<td>Settings</td>
<td>20</td>
</tr>
<tr>
<td>Users and Groups</td>
<td>21</td>
</tr>
<tr>
<td>Test</td>
<td>22</td>
</tr>
<tr>
<td>User Groups</td>
<td>23</td>
</tr>
<tr>
<td>About the User Groups list</td>
<td>23</td>
</tr>
<tr>
<td>Searching for a User Group</td>
<td>25</td>
</tr>
<tr>
<td>Synchronizing LDAP</td>
<td>26</td>
</tr>
<tr>
<td>Deleting User Groups</td>
<td>26</td>
</tr>
<tr>
<td>Importing User Groups</td>
<td>26</td>
</tr>
<tr>
<td>Importing User Groups from LDIF</td>
<td>28</td>
</tr>
<tr>
<td>Assigning Primary Groups</td>
<td>29</td>
</tr>
<tr>
<td>Users</td>
<td>31</td>
</tr>
<tr>
<td>About the users list</td>
<td>31</td>
</tr>
</tbody>
</table>
Overview

Dell SonicWALL offers comprehensive web content security that blocks selected web content and enforces protection and productivity policies. The main components are Content Filtering Service (CFS), Content Filtering Client (CFC), and Enforced Client Policy & Reporting Server (EPRS). CFS protects the devices behind the firewall; CFC protects devices regardless of where the device is located, even if it is connected outside the firewall, and EPRS provides administrators with the means to manage CFC from a central web interface.

This document describes how to use EPRS. Global policies can be created and assigned to all CFC client systems without having to log into each system separately. Additionally, policies can be defined for groups or individual users that can also be managed from the central web interface.

Topics:
- About this guide describes how this guide is organized and the conventions used to designate specialized text.
- About EPRS describes how to navigate EPRS and license a client. It also provides general administration guidelines.

About this guide

This document is intended for system administrators who define filtering policy for systems that will be accessing web content from the internet.

- Document contents describes how this document is organized.
- Guide conventions defines the text conventions used in this document.

Document contents

This document includes:

- This chapter, Overview, provides a general document overview and describes the conventions used within this guide.
- Chapter 2, System on page 9, describes the System option, which includes viewing status, managing Schedule Groups and managing certificates.
- Chapter 3, LDAP on page 14, describes how to access user and group data from the LDAP server.
- Chapter 4, Google Directory on page 20, describes how to access user and group data from Google Directory.
- Chapter 5, User Groups on page 23, describes how to utilize user groups that have already been established in LDAP and Google Directory. You can then apply the same policies to everyone in a group. All the groups can be viewed and managed from this option.
- Chapter 6, Users on page 31, describes how to view and manage users.
- Chapter 7, Content Filter on page 39, discusses how to set up and customize the content filtering for the Content Filtering Client (CFC).
• Chapter 8, Enforcement on page 46, reviews how to configure enforcement policies and describes settings for Client Groups and Clients.

• Chapter 9, Reports on page 54, shows the reports that are available from the Reports tab.

• Chapter 10, Troubleshooting on page 59, provides some troubleshooting tips for common issues.

Guide conventions

The following conventions used in this guide are as follows:

Table 1. Text conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Highlights dialog box, window, and screen names. Also highlights buttons. Also used for file names and text or values you are being instructed to type into the interface.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence. Sometimes indicates the first instance of a significant term or concept.</td>
</tr>
<tr>
<td><strong>Computer code</strong></td>
<td>Indicates sample code or text to be typed into data fields.</td>
</tr>
</tbody>
</table>

About EPRS

EPRS provides a single point from which to configure filtering policies and view reporting from users systems that are running CFC. EPRS is comprised of:

• **Web management interface and policy manager**—a Web-based interface that provides the system administrator the ability to configure, create, and apply global policies and generate activity reports for client systems.

• **Policy Server**—Supports policy functions including global management and user access credentials.

• **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.

Additional topics:

• How EPRS Works
• How to access CFC
• Navigating the interface
• Installing the client on user systems

How EPRS Works

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.

EPRS features include dynamic updates of licensing on the firewall registered to use the content filtering client an policy application based on client licensing.

**NOTE:** 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, EPRS 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 to access CFC

MySonicWALL provides links that the administrator can click to access the EPRS management interface in order to create or manage client policies. Two links are provided:

- Firewall (unit) level link to manage CFC policies licensed on this 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.

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 EPRS interface using Single Sign-On.

Logging in to EPRS from MySonicWALL allows you to configure and view policies and reporting for all the Dell SonicWALL appliances that are registered to that MySonicWALL account.

When you log in to EPRS from an individual firewall, the interface only displays configuration pages for the unit from which you logged in.

Navigating the interface

When you first open EPRS, the default display is a global view of System > Status.

The far left pane displays the devices being managed. You can select a specific device to view or manage or you can select the top node name, as in the figure above, to see information applicable to the global node.

**NOTE:** If you have only a single node or unit, the node pane is not displayed.

The Global View provides the Settings, Policies, and Client Groups pages, but does not provide the Clients pages since it pertains to a single Dell SonicWALL appliance.

You can hide the node pane by clicking on the green arrow in the top bar. Click on the arrow again to expand the view.

From the EPRS interface you can switch between Policies view and Reports view. Select the tab of the view that you want. Different options are listed depending on whether you selected the global node or a specific device.
Installing the client 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.
The System option on the Policies tab allows you to view status on the nodes, manage the schedules and manage the certificates. If you have an environment with more than one firewall in it, you can view and manage the system settings at two levels: globally and on the firewall. By selecting the global node (the top node in the left pane) you can configure and make changes across all the firewalls in your environment. By selecting an individual node, or firewall, you can configure and make changes that apply only to that particular node.

Topics:
- Status
- Schedules
- Certificates

**Status**

The global view (global node is selected) of the System > Status page is the default display when you first access EPRS. To see the status of particular node, select the node from the left pane.

The System > Status page displays the status information for the node selected. The status information includes:

- **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 CFC installed
  - Total number of nodes licensed to install the Content Filtering Client
• LDAP Settings—Displays LDAP Domain Alias
• LDAP Automatic Sync Status—Displays a message noting status and when LDAP was last synchronized.
• Google Directory Automatic Sync Status—Displays a message noting status and when LDAP was last synchronized.

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

Schedules

The System > Schedules page displays the default scheduled configured and available to use for policy configuration. You configure and manage additional schedules from this page. If you expand a specific schedule name, details of the schedule is displayed. If you expand the Name group, all the schedule names are expanded.

Topics:
• Adding a Schedule Group on page 10
• Editing a Schedule Group on page 11
• Deleting a Schedule Group on page 12

Adding a Schedule Group

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

1. Navigate to the System > Schedules page. Click the Add Schedule Group link.
2. Enter the Name of the Schedule Group.
3. Select the Day(s) for the schedule to be enforced.
4. Specify the Start Time for the schedule to begin. Time should be entered in using the 24-hour format.
5. Specify the Stop Time for the schedule to end. Time should be entered in using the 24-hour format.
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 time period in the list by selecting the period and clicking Delete, or clicking Delete All to delete all schedules listed.
7. Click OK to save a Schedule Group.

Editing a Schedule Group

To edit a schedule group that has already been created:

1. Navigate to the System > Schedules page.
2. Click the Edit icon of the Schedule Group you wish to edit. The Schedule Settings screen displays.
3. You can add a schedule by specifying the parameters and clicking Add. You can also delete a time period in the list by selecting the existing schedule and clicking Delete, or clicking Delete All to delete all schedules listed.
4. Click OK to save changes.
Deleting a Schedule Group

To delete a schedule group:

1. Navigate to the System > Schedules page.
2. Check the box next to the Schedule Group you wish to delete. To delete multiple Schedule Groups, select multiple groups.
3. 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.

Certificates

The System > Certificates page allows administrators to perform a search for certificates. This page also allows administrators to manage certificates and certificate requests.

Topics:

- Searching for Certificates on page 12
- Importing a Certificate on page 13
- Deleting a Certificate on page 13

Searching for Certificates

To search for a certificate:

1. 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.
2. In the blank field, type in the text that you want to search for.
3. Click Search.
4. Click Clear to return the search fields to their default values and clear the text field.
Importing a Certificate

EPRS 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 encoded file.

To import a certificate:

1. On the System > Certificates page, click the Import link. The Import Certificate page displays.

2. Browse to where the certificate is stored and select the file.
3. Select Import to import the certificate from your local system.

Deleting a Certificate

To delete a certificate:

1. Navigate to the System > Certificate page.
2. Check the box next to the certificate you wish to delete.
3. Click the Delete Certificate(s) link. You can also click the Delete icon under the Configure column of the group you wish to delete.
Lightweight Directory Access Protocol (LDAP) is one of the options under Directory Services that administrators can use to efficiently manage Users and Groups from the LDAP server. LDAP is used to sync Users/Groups into EPRS, so CFS Policies can be tied to the Client Groups where the Clients belong. If you have an environment with more than one firewall in it, you can manage LDAP at two levels: globally and on the firewall. By selecting the global node, you can configure and make changes across all the firewalls in your environment. By selecting an individual node, or firewall, you can configure and make changes that apply only to that particular unit.

Topics:
- Settings on page 14
- Schema on page 15
- Directory on page 17
- Users & Groups on page 18
- Test on page 19

**Settings**

To configure the settings on the LDAP page:

1. On the Policies tab, navigate to Directory Services > LDAP. The LDAP page defaults to the Settings tab.

2. Check the box to Configure LDAP.
3 Enter the name or IP address for the LDAP Server.

4 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. Be sure to open this port number in your firewall for inbound communication with the LDAP server.

5 Specify the Server timeout period in seconds. If no connection is made after this period elapses the client stops attempting to connect to the server.

6 Specify Overall operation timeout in minutes. This is the maximum time spent on any auto-operation.

   NOTE: Some operations, such as directory configuration or importing user groups, can take several minutes, especially if running across multiple LDAP servers.

7 Select one of the following authentication methods:

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Definition and process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous login</td>
<td>Select to login without the LDAP server authenticating information or “binding” to the server.</td>
</tr>
<tr>
<td>Give login name/location in tree</td>
<td>Select to authenticate through a login process. Also:</td>
</tr>
<tr>
<td></td>
<td>• Enter the Login username.</td>
</tr>
<tr>
<td></td>
<td>Note: You need to provide the user’s distinguished name.</td>
</tr>
<tr>
<td></td>
<td>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 Directory Services &gt; LDAP, Directory tab.</td>
</tr>
<tr>
<td></td>
<td>• Enter the Login password. If you leave the password field empty, the current password will remain unchanged.</td>
</tr>
<tr>
<td></td>
<td>• Select the Protocol version from the drop down list.</td>
</tr>
<tr>
<td>Give bind distinguished name</td>
<td>Select to bind to the LDAP server using the full distinguished name. Also:</td>
</tr>
<tr>
<td></td>
<td>• Enter the Bind distinguished name.</td>
</tr>
<tr>
<td></td>
<td>• Enter the Login password. If you leave the password field empty, the current password will remain unchanged.</td>
</tr>
<tr>
<td></td>
<td>• Select the Protocol version from the drop down list.</td>
</tr>
</tbody>
</table>

8 Check the Use TLS (SSL) box to enable the authentication of servers and clients and encryption of messages on LDAP.

9 Click Update to save these settings.

Schema

To set up the LDAP schema:

1 On the Policies tab, navigate to Directory Services > LDAP.

2 Select the Schema tab.

3 Select the LDAP Schema from the drop-down list.
   • Selecting any of the predefined schemas automatically populates 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 and go to the next procedure.
To configure a user-defined schema:

1. In the LDAP Schema field, select User defined from the drop down list.

2. In the User Objects section:
   a. Define the Object class. This defines which attribute represents the individual user account to which the login name attribute and the user group membership attribute apply.
   b. Define the Login name attribute. This is the LDAP attribute that corresponds to the User ID.
   c. Define the User group membership attribute. This is the LDAP attribute that lists the groups or mailing lists that the user is a member of.
   d. Define the Additional user group ID attribute. If set and Use is enabled (the boxed checked), 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. If a group is found with the Additional user group match attribute set to that value then the user is also made a member of that group.

3. In the User Group Objects section:
   a. Define the Object class for the group for the LDAP schema.
   b. Specify the Member attribute that corresponds to group members.
   c. Set the Additional user group match attribute. This is 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:** This attribute may be inefficient to the load performance of your LDAP server.

4. Select Read from Server to retrieve the LDAP schema from the LDAP server.

5. Choose to:
   - Automatically update the schema configuration
   - Export details of the schema
6 Click OK.
7 Click Update to save these settings.

Directory

Depending on the authentication method you specified on the Settings tab, you may have to enter additional information on the Directory tab.

To configure Directory settings:

1 On the Policies tab, navigate to Directory Services > LDAP.
2 Select the Directory tab.

3 Depending on your selection on the Settings tab, define the User Directory Information:
   - If you selected Anonymous Login or Give bind distinguished name, provide the Primary domain or check the box to Fetch domain alias automatically.
   - 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.
4 Click Update to save these settings
Users & Groups

To mirror LDAP users and user groups:

1. On the Policies tab, navigate to Directory Services > LDAP.

2. Select the Users & Groups tab.

3. Check the box to Mirror LDAP users and user groups automatically.

4. Specify the Refresh period in hours. This is the period between mirroring operations. A valid value can range from 8 to 168 hours.

5. Click Update to save these settings.
To test the LDAP settings:

1. On the Policies tab, navigate to Directory Services > LDAP.

2. Select the Test tab.

3. Enter a valid LDAP User name and Password.

4. Click the Test button. EPRS retrieves any messages from the LDAP server as well as returned user attributes in the appropriate fields.
Google Directory

Google Directory is one of the options under Directory Services that administrators can use to efficiently manage Users and Groups from the Google server. If you have an environment with more than one firewall in it, you can manage Google Directory at two levels: globally and on the firewall. By selecting the global node, you can configure and make changes across all the firewalls in your environment. By selecting an individual firewall you can configure and make changes that apply only to that particular unit.

**NOTE:** Both Google Directory and LDAP server can be configured on the same firewall.

Topics:
- Settings
- Users & Groups
- Test

### Settings

To configure the Google Directory:


2. **Check the box to enable Configure Google Directory.**
3 Enter the **Domain** name for Google Directory service.

4 Set up an authorized service account the server-to-server interactions between EPRS and Good Directory service can occur. This only needs to be done once.
   a Make a note of the Client ID of the service account for use later: `11316127257108595191`.
   b Login to [https://admin.google.com/](https://admin.google.com/) using your Google Super admin account (Service account email) for the domain.
   c Navigate to Security > Advanced settings > Authentication > Manage API client access.
   d In the **Client name** text box, enter the client ID.
   e In the **API Scopes** text box, copy/paste the string below:
     - [https://www.googleapis.com/auth/admin.directory.group.member.readonly](https://www.googleapis.com/auth/admin.directory.group.member.readonly)
     - [https://www.googleapis.com/auth/admin.directory.group.readonly](https://www.googleapis.com/auth/admin.directory.group.readonly)
     - [https://www.googleapis.com/auth/admin.directory.orgunit.readonly](https://www.googleapis.com/auth/admin.directory.orgunit.readonly)
     - [https://www.googleapis.com/auth/admin.directory.user.readonly](https://www.googleapis.com/auth/admin.directory.user.readonly)
   f Click on **Authorize**.

5 Enter the **Service Account Email**.

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

### Users and Groups

**To mirror Google Directory users and user groups:**

1 On the **Policies** tab, navigate to **Directory Services > Google Directory**.

2 Select the **Users & Groups** tab.

3 Check the box to **Mirror LDAP users and user groups automatically**.
4 Specify the **Refresh period** in hours. This is the period between mirroring operations. A valid value can range from 8 to 168 hours.

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

**Test**

*To test the Google Directory settings:*

1 On the **Policies** tab, navigate to **Directory Services > Google Directory**.

2 Select the **Test** tab.

3 Enter a valid user ID (primary email of the user).

4 Click the **Test** button. EPRS retrieves any messages from Google as well as returned user attributes in the appropriate fields.
User Groups

The User Groups function allows you to utilize user groups that have already been established in LDAP and Google Directory. You can then apply the same policies to everyone in a group. All the groups can be viewed and managed on the Policies tab at Directory Services > User Groups.

If you have an environment with more than one firewall in it, you can also manage User Groups at two levels: globally and on the firewall. By selecting the global node, you can configure and make changes across all the firewalls in your environment. By selecting an individual firewall you can configure and make changes that apply only to that particular unit.

Topics:
- Searching for a User Group on page 25
- Synchronizing LDAP on page 26
- Deleting User Groups on page 26
- Importing User Groups on page 26
- Importing User Groups from LDIF on page 28
- Assigning Primary Groups on page 29

About the User Groups list

The User Groups list has several tools that are useful for finding and managing user group information. At the top of the list is a search function. Refer to Searching for a User Group on page 25 for information on using the search.

The names in the body of the table represent what has been mirrored from either LDAP or Google Directory. The source of the information is listed in the column called Mirrored From. The Type column indicates what kind of group this is. Options include User Group or Organizational Unit. Members tells how many users are in the group. The Directory column indicates the source for the Users information. The options are LDAP or Google (for Google Directory).
In the Configuration column, several icons allow operations on the User Group listed on that line. The edit and delete icons allow you to manage user data.

- The view/edit icon allows you to view the settings for the group (Settings tab) and you can edit the group members on the Members tab.
The group icon allows you to set this group as the Primary Group to the users (or some of the user) in the group. Refer to Assigning Primary Groups on page 29, for more information.

The delete icon allows you to delete the group on this line. You are asked to confirm the deletion before continuing.

At the bottom of the list, a note states how many user groups were found and how many of them have no members.

### Searching for a User Group

The User Groups Search function is useful if you have a large number of user groups and need find a specific one. The function can search for text in the Name, Mirrored From, Type or Directory fields. To search for a specific user group, choose the node that you want to search. On the Policies tab, select Directory Services > User Groups.

To search for a user group:

1. Select the user group field to be searched. You can select either the Name, Mirrored From, Type, or Directory fields.
2. To specify the type of match, 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.

Synchronizing LDAP

The User Groups page allows you to synchronize your LDAP and Google Directory to easily authenticate users. Click the Synchronize link at the bottom of the page to efficiently synchronize the list of User Groups.

Synchronizing user groups:

- Replicates any membership changes for user groups listed in the User Groups Mirrored from LDAP and Google Directory.
- Removes any deleted user groups from the list of User Groups Mirrored from LDAP/Google Directory.
- Removes client groups for the deleted user groups.

You will be asked to confirm your action because of the changes that could be made to your groups.

Deleting User Groups

To delete user groups:

1 On the Policies tab, navigate to Directory Services > User Groups.
2 Check the box corresponding to the User Group you want to delete. Then, click the Delete User Group(s) link at the bottom of the page or click the Delete icon in the Configure column for that group.

   NOTE: You can delete multiple groups at a time. Check the boxes by the group names you want to delete and click the Delete User Group(s) link at the bottom of the page.

3 Click on OK after being asked to confirm that you want to delete the group.

   NOTE: If you delete a group that has clients that uses a policy defined for that group, you get a warning message showing the relationship between the user group to the client. Then you can take corrective action based on the comments provided.

Importing User Groups

User groups can be imported from either your LDAP server or the Google Directory or both.

To import User Groups:

1 On the Policies tab, navigate to Directory Services > User Groups.
2 Click the Import User Groups link at the bottom of the User Groups page. A list of available user groups displays. The following figure shows the view for LDAP.
3 Check the Directory Type and change it to the type you want by selecting from the drop down menu. The following figure shows the view for Google Directory.
You can then select the groups to import by checking the box and click the **Save Selected** button to add those user groups to EPRS.

**NOTE:** If you have a long list of User Group/OU Names, you can use the Search function at the top of the page to filter the list. Select the field to search on (name, type, location); choose the type of search (equals, starts with, ends with, contains); input the search string and select **Search**.

You can also perform other functions from the Import page:

- To remove user groups from EPRS, select one or more groups by checking the box, then click the **Remove from List** button.
- Click on Undo to undo any action.

## Importing User Groups from LDIF

EPRS also supports importing from Lightweight Directory 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

| NOTE: | Inclusion of other LDAP attributes in the file may result in large file volume. The server may take a considerable amount of time to process the large files |

| NOTE: | 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:**

2. Click the Import User Groups from LDIF link at the bottom of the User Groups page.
3. Click the Browse button to select the LDIF file.
4. Select Import.

### Assigning Primary Groups

The 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. An individual user may belong to multiple groups, each of which has a variety of policies to enforce. To ensure the correct policies are applied to this user, the administrator should assign the primary group to which the user should belong.

| NOTE: | If a user is not assigned to a Primary Group, EPRS assigns the user to the first Primary Group the user is a part of. |

**To assign primary groups to users:**

1. Click the Assign Primary Group icon.
   - A dialog window displays the list of groups and users.
2 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.

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.

3 Click the OK button to finish and save changes.

**NOTE:** For large groups, this may take several minutes to populate.

**NOTE:** When assigning a user to a user group, you can approach from one of two perspectives. When making the assignment from the User Group page, you can look at all the individuals that make up the user group. You can then easily validate that all the users needed for that group are included and remove any that should not be in there. When making the assignment from the Users page, you only see the group that individual belongs to, and you can choose a different group, if appropriate.
The **Users** function allows you to view and manage users on the **Policies** tab at **Directory Services > Users**. If you have an environment with more than one firewall in it, you can manage Users at two levels: globally and on the firewall. By selecting the global node, you can configure and make changes across all the firewalls in your environment. By selecting an individual firewall you can configure and make changes that apply only to that particular unit.

### Topics:

- About the users list on page 31
- Searching for Users on page 32
- Deleting Users on page 34
- Assigning a Primary Group on page 34
- Blocking/Unblocking Users on page 35
- Importing Users on page 35
- Importing Users from LDIF on page 38

### About the users list

The Users list has several tools that are useful for finding and managing user information. At the top of the list is a search function. Refer to **Searching for Users** on page 32 for information on using the search.

The names in the body of the table represent what has been mirrored from either LDAP or Google Directory. Both the **Name** and the **Display Name** are shown.

The information in the **Primary Group** column shows that a user is a member of multiple groups. The number indicates how many other groups that user is a member of. If you hover the mouse over the group icon, a message will show indicating if this user needs to be assigned to a Primary Group. Go to **Assigning a Primary Group** on page 34 for information on how to assign a user to a Primary Group.

A green check in the **Allowed** column indicates that the user is not blocked from using the filtering client. A red X indicates the user is blocked.

The **Directory** column indicates the source for the Users information. The options are LDAP or Google (for Google Directory).

In the **Configuration** column, the edit and delete icons allow you to manage the user data. Refer to **Editing Users** on page 33 for more information on using the edit icon. Refer to **Deleting Users** on page 34 for more information on using the delete icon.
Searching for Users

The Users Search function is useful if you have a large number of users and need to find a specific one. The function can search for text in the Name, Display Name, Allowed or Directory fields. To search for a specific users, choose the node that you want to search. On the Policies tab, select Directory Services > Users.

To search for a user:

1. Select the user group field to be searched. You can select either the Name, Display Name, Allowed, or Directory fields.
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.
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.
Editing Users

Selecting the edit icon for a user allows you to block or unblock a user and select a primary group.

To edit a user:

1. On the Policies tab, navigate to Directory Services > Users.
2. Click on the edit icon for the user you want to change.
3. Check the Block box to block this user from being filtered.
4. Select the Groups tab.
5. Select the Primary Group from the drop down list.
6. Click on OK to save settings.
Deleting Users

To delete users:

1. On the Policies tab, navigate to Directory Services > Users.
2. Check the box corresponding to the User you want to delete. Then, click the Delete User(s) link at the bottom of the page or click the Delete icon in the Configure column for that group.
3. When the confirmation message pops up, click on OK if you want to continue with deleting the user.

**NOTE:** You can delete multiple users at a time. Check the boxes by the user names you want to delete and click the Delete User(s) link at the bottom of the page.

Assigning a Primary Group

The Users 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. An individual user may belong to multiple groups, each of which has a variety of policies to enforce. To ensure the correct policies are applied to this user, the administrator should assign the primary group to which the user should belong.

To assign a user to a primary group:

1. On the Policies tab, navigate to Directory Services > Users.
2. Check the box for the user you want to assign. Multiple nodes can be selected and assigned at the same time.
3. Click on the Assign Primary Group link at the bottom of the list. A window displays.

4. Select the Primary Group from the drop-down list at the top of the window.
5. Click the OK button to finish and save changes.

**NOTE:** When assigning a user to a user group, you can approach from one of two perspectives. When making the assignment from the Users page, you only see the group that individual belongs to, and you can choose a different group, if appropriate. When making the assignment from the User Group page, you can look at all the individuals that make up the user group. You can then easily validate that all the users needed for that group are included and remove any that should not be in there.
Blocking/Unblocking Users

Blocking and unblocking provides a way of managing individual licenses. If, for example, someone changed assignments and no longer needs a filtering license, you can opt to block that user’s use of the license, making it available to someone else. A blocked license can be restored.

To block users:

1. On the Policies tab, navigate to Directory Services > Users.
2. Check the box for the user you want to block. You can select more than one user at a time.
3. Select the Block User(s) link. The system asks for verification that you want to block this user.
4. Click OK to confirm that you want to block this user.

To unblock users:

1. On the Policies tab, navigate to Directory Services > Users.
2. Check the box for the user you want to unblock. You can select more than one user at a time.
3. Select the Unblock User(s) link. The system asks for verification that you want to unblock this user.
4. Click OK to confirm that you want to unblock this user.

Importing Users

You can import users from your LDAP server or from the Google Directory.

To import users:

1. On the Policies tab, navigate to Directory Services > Users.
2. Click the Import Users link at the bottom of the page. A list of available users displays. The following figure shows the view for Google Directory, but LDAP would be very similar.
3 Check the Directory Type and change it to the type you want by selecting LDAP or Google Directory from the drop down list.

4 Select the users to import and click the **Save selected** button to add those users to your EPRS users.

You can perform other functions from this same window. You can search for users and remove users. The search function works the same as described in other areas. Choose the field to search on, select the search parameters, provide the search string and select Search.

Users can be removed in several ways:

- **All selected users**—Select the users from the list, then select the **All selected users** option. 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 and then the search string. 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]**—Select either **at** or **at or under** from the drop down list. From the next drop down list, select the location of the users. For example, 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 removes all users listed in the engineering@sonicwall.com group.

**NOTE:** If there are no user groups found on the LDAP server or Google Directory, a list of possible reasons displays. See the image below for an example.
### LDAP Users Search

**Search:**
- **User ID**
- **Equals**

**Directory Type**
- Select Directory Type: **LDAP**

Listed below are the users that were read from the LDAP server. Select the users to import, and then click Save selected to add those user names to the LDAP users.

Showing 0 of 0 users

No users were found on the LDAP server.

Possible reason(s) for failure:
- The users have already been added.
- The users are indeed not available on the LDAP server.
- Ensure schema settings match with the configured LDAP server.
- Synchronize LDAP is in progress.
- The server configured is not reachable. Check the server configuration.
- Server timeout may have occurred before completing the action.
- If Protocol Version is configured to Version 3, make sure the server configured supports proper authentication mechanism.
- If TLS is enabled, make sure the CA certificate has been imported and is valid.

---

- **Remove from list...**
  - **All selected users**
  - **Any user whose name**
  - **contains**
  - **All users**

[Save selected] [Cancel]
Importing Users from LDIF

Similar 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 currently configured for Users:

- **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:** Inclusion of other LDAP attributes in the file may result in large file volume. The server may take a considerable amount of time to process the large files.

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

**To import Users from an LDIF file:**

2. Click the Import Users from LDIF link at the bottom of the Users page.
3. Click the Browse button to select the LDIF file.
4. Select Import.
The Content Filter option is used to set up and customize the content filtering for CFC. If you have an environment with more than one firewall in it, you can manage the filtering at two levels: globally and on the firewall. By selecting the global node (the top node in the left pane) you can configure and make changes across all the firewalls in your environment. By selecting an individual node, or firewall, you can configure and make changes that apply only to that particular unit.

Topics:
- Settings
- Custom List
- Policies

Settings

To configure the Content Filter Settings, choose the global or firewall that you want to manage. (In this example a firewall has been selected.) On the Policies tab, select Content Filter > Settings.

Topics:
- Enforcement setting
- Blocked web page display
- CFS settings
Enforcement setting

When a client system running CFC is put on the network behind the firewall, you can opt to suspend CFC if Gateway CFS is active.

To configure Enforcement Settings:

1. Check the box if you want to Suspend CF Client when behind Firewall with active Gateway CFS.
2. Update the Firewall List/Client Distribution Group with the serial numbers of the firewalls traffic is being routed through.
   
   **NOTE:** The firewall listed can be edited in this section too. Enter serial Number in the text field and click on the Add icon. Click on the edit icon to update a serial number and save it. Click on the delete icon to delete a firewall from the list.

3. Select Update to save the Enforcement Settings or Reset to reload the prior settings.

Blocked web page display

To select the Web page to display when blocking:

Choose to display the default Web page or customize your own Web page.

- Leave the text field blank to use the default page.
- Use the Preview button to see what the web page will look like.
• Select Default Blocked Page to return back to using the default page.
• Select Update to save any changes to the web page display settings or Reset to reload the prior settings.

CFS settings

These settings are used when on the user system is protected by the firewall and CFC is suspended.

To select the CFS Settings:

1. Check the box to Enable HTTPS Content Filtering. HTTPS Content Filtering is based on IP and hostname. While HTTP Content Filtering can perform redirects to enforce authentication or provide a block page HTTPS filtered pages will be silently blocked.
2. Check the box to Show a notification when HTTPS is blocked. If left unchecked, no notification is given.
3. Check the box to automatically Block Access to URL that is marked as forbidden.
4. Check the box to automatically Log Access to URL that is marked as forbidden.
5. Select Update to save any changes to the CFS settings or Reset to reload the prior settings.

Custom List

To configure the Content Filter Custom List, choose the global or node that you want to manage. (In this example a node has been selected.) On the Policies tab, select Content Filter > Custom List.

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

• Allowed Domains—Allows user access to these domains with their Web browser.
  • Select Add New Allowed Domain to add a domain to the allowed list. You can add multiple domains at the same time; separate them with a semicolon (;).
  • Select Import... to select a text file of allowed domain names. Each domain name should appear on a separate line.
  • Click on the delete icon next to the domain name to delete it from the allowed list. You can also check the box next to one or more domain names and select Delete Allowed Domain(s).

• Forbidden Domains—Forbids user access to domains with their Web browser.
  • Select Add New Forbidden Domain to add a domain to the forbidden list. You can add multiple domains at the same time; separate them with a semicolon (;).
• Select Import... to select a text file of forbidden domain names. Each domain name should appear on a separate line.
• Click on the delete icon next to the domain name to delete it from the forbidden list. You can also check the box next to one or more domain names and select Delete Forbidden Domain(s).

• Keywords—Defines keywords used to offer protection against Web sites that have not explicitly been added to the Master Database or defined as allowed or forbidden site.
  • Select Add New Keyword to add a keyword to the list. You can add multiple keywords at the same time; separate them with a semicolon (;).
  • Select Import... to select a text file of keywords. Each keyword should appear on a separate line.
  • Click on the delete icon next to the keyword to delete it from the list. You can also check the box next to one or more keywords and select Delete Keyword(s).

### Policies

The Content Filter > Policies page allows you to search for, add, and delete policies that block objectionable Web sites. To configure the Content Filter > Policies, choose the global or node that you want to manage. (In this example a node has been selected.) On the Policies tab, select Content Filter > Policies.

| NOTE: | A default policy is provided called Default. This policy can be viewed and cloned, but cannot be deleted. |

**Topics:**
- Searching for policies
- Add/edit Policy

### Searching for policies

The Policies page displays the policies that have been configured for CFC. As with many pages, the Policies page has a search function on it so you can easily find the specific policy you want or filter a long list to something smaller. The search is made on the Name field.

**To search for a policy:**

1. 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.
2. In the blank field, type in the text that you want to search for.
3. Click Search.
4. Click Clear to return the search fields to their default values and clear the text field.
Add/edit Policy

Adding and editing a policy are very similar, using the same policy setup window. Select the Add New Policy option to define your own policies for CFC users. Select a policy and click on the edit icon edit a policy.

To add a policy:

1. On the Policies tab, navigate to Content Filter > Policies.
2. At the bottom of the Policies list, click the Add New Policy link at the bottom of the page. The policies set up page displays.
3. On the Policy tab, enter the policy name in the Name field.
4. On the Categories tab, select the forbidden categories from the list provided. You can opt to select all categories by checking the Select All Categories box at the top of the page.
5 On the Settings tab set the following options:

**Custom Global Settings**

| Source of Allowed Domains | Select None, Global or Per policy from the drop down list. |
| Source of Forbidden Domains | Select None, Global or Per policy from the drop down list. |
| Source of Keyword | Select None, Global or Per policy from the drop down list. |

**Safe Search Enforcement**

| Enable Safe Search Enforcement | Select to Enable Safe Search Enforcement. |

**YouTube for Schools**

| Enable YouTube for Schools | Select to Enable YouTube for Schools. |
| School ID | Enter your school ID. Note that the ID field is not active until YouTube for Schools is enabled. |

**Filter Forbidden URLs by time of day**

| Time of day drop down list | Select the time of day you want filtering enforced. Several options are provided to choose from. The default is Always on. |

6 The Custom List tab create a list of Allowed Domains, Forbidden Domains or Keyword.

In the Content field add the domain name you want to allow or forbid, or add the keyword and click Add. You can also highlight or an entry in the list and choose Update to make changes or Remove to delete the entry. Select Remove all to delete all entries in that section.
7 Configure the setting on the Advanced tab. The following table provides more information on each of the settings.

<table>
<thead>
<tr>
<th>Override Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow client to override forbidden websites</td>
</tr>
<tr>
<td>Override Password</td>
</tr>
<tr>
<td>Use blank password</td>
</tr>
<tr>
<td>Override Duration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorized Processes - Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Process Name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorized Processes - Certificate Subject Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Subject Cert Name</td>
</tr>
</tbody>
</table>

8 Click on OK to save the policy.
Navigate to the Enforcement menu on EPRS, located on the Policies tab. You can configure enforcement policies, as well as settings for Client Groups and Clients. If you have an environment with more than one firewall in it, you can manage the enforcement at two levels: globally and on the firewall. By selecting the global node, you can configure and make changes across all the firewalls in your environment. By selecting an individual firewall you can configure and make changes that apply only to that particular unit.

Topics:

- Policies on page 46
- Client Groups on page 48
- Clients on page 51

Policies

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 are suitable for use with most Content Filtering Clients. They cannot be edited or deleted.

You can create a new policy or clone one from an existing policy, such as the Default Desktop Policy. Cloning the Default Desktop Policy or an existing policy is recommended. Then edit specific fields within the cloned policy. This is an effective way to create a new policy that is similar to an 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.

Topics:

- Policies on page 46
- Client Groups on page 48
- Clients on page 51

To clone a policy or add a new policy:

1. Navigate to the Enforcement > Policies page and choose either the global node or a specific firewall for the policy.

2. 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.
3 On the General tab, input or change the name of the Policy in the **Name** field.

4 Add descriptive information about the policy in the **Comments** field.

5 Under the **Version Settings** section, select the desired **Version** (specific release) from the drop-down list. This allows the policy to be configured for a specific version. You can select **General Release**, **Early Release**, **Alpha** or **Beta**.

6 Select the **Content Filter** tab.

7 Select the **Default** local policy from the drop-down menu.
8 Select a Scheduled policy from the drop-down list. A scheduled policy is one that has a Schedule associated with it. If a Schedule is selected and the schedule matches the time, the policy is used for enforcement during the specified window of time. If a scheduled policy is not selected, the default would apply all the time. Note that only policies with a schedule set appear in this drop-down list.

9 Click OK.

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 acquire the policies as defined in the Default Desktop Policy. All mobile devices, such as a laptop, 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.
Topics:

- About the Client Groups list
- Searching Client Groups
- Adding or Editing Client Groups
- Deleting Client Groups

About the Client Groups list

The Client Groups list has several tools that are useful for finding and managing client group information. At the top of the list is a search function. Refer to Searching Client Groups on page 50 for information on using the search.

The following table describes the columns in the Client Groups list.

<table>
<thead>
<tr>
<th>Name</th>
<th>Represents the client groups that have been defined.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Indicates what kind of group this is. Options include User Group, Organizational Unit, or Host.</td>
</tr>
<tr>
<td>Desktop Policy</td>
<td>Indicates which desktop policy is being applied to the group.</td>
</tr>
</tbody>
</table>
Searching Client Groups

The Client Groups Search function is useful if you have a large number of client groups and need to find a specific one. The function can search for text in the Name, Type, Desktop Policy, Mobile Policy or Directory fields. To search for a specific user group, choose the node that you want to search. On the Policies tab, select Enforcement > Client Groups.

To search for a client group:

1. Select the client group field to be searched. You can select either the Name, Type, Desktop Policy, Mobile Policy, or Directory fields.
2. To specify the type of match, 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.

Adding or Editing Client Groups

To add or edit a client group:

1. On the Policies tab, navigate to the Enforcement > Client Groups page.
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. The Add Client Group window displays.
3 Type a descriptive name into the **Group Name** field
4 In the **Comment** field, enter a descriptive comment.
5 Select a policy for the group from the **Desktop Policy** drop-down list. All existing policies are available for selection.
6 Select a policy for the group from the **Mobile Policy** drop-down list. All existing polices are available for selection.
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:

1 On the **Policies** tab, navigate to the **Enforcement > Client Groups** page.
2 The delete options are:
   - To delete all client groups except the default, check the box next to the **Name** column heading, then click **Delete Client Group(s)** at the bottom of the page.
   - To delete multiple client groups, check the box next to each one you want to delete and click **Delete Client Group(s)**.
   - To delete a single client group, click the trash can icon in the same row, or check the box next to it and then click **Delete Client Group(s)**.

**NOTE:** The Default Client Group and User Group-based Client Groups cannot be deleted so they have a grayed-out icon Trash icon.

When Client Groups with clients are deleted:

- It does not allow you to delete, but prompts you to move the users to another client group.
- A tool tip get a message warning that the client groups cannot be deleted. The warning message shows the relationship between the client group to the clients. Then you can take corrective action based on the comments provided.

## 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.

Topics:

- [Searching for Clients](#) on page 52
- [Deleting Clients](#) on page 52
- [Blocking Clients](#) on page 53
- [Unblocking Clients](#) on page 53
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:
1. Navigate to the Enforcement > Clients.
2. Select the client field to be searched from the drop down list. You can select the Host Name, Client Group, Client Version, Allowed, or Client Users.
3. 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.
4. In the blank field, type in the text or value that you want to search for.
5. Click Search.
6. 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:
1. On the Policies tab, navigate to the Enforcement > Clients page.
2. The delete options are:
   - To delete all clients, check the box next to the Host Name column heading, then select Delete Client(s).
   - To delete multiple clients, check the box next to each one you want to delete, then click Delete Client(s).
   - To delete a single client, click the trash can icon in the same row, or check the box next to it and then click Delete Client(s).
3. Click OK in the confirmation dialog box.

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:
1. On the Policies tab, navigate to the Enforcement > Clients page.
2. Check the box next to the clients you want to move.
3 Click the Move Client(s) link at the bottom of the page.

![Move Client(s) dialog](image)

4 When the pop-up window displays asking you to select the destination client group, select the option you want.

5 Select OK.

### Blocking Clients

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

**To block one or multiple clients:**

1 On the Policies tab, navigate to the Enforcement > Clients page.
2 Check the box next to the clients you want to block.
3 Click the Block Client(s) link at the bottom of the page. You will be asked to confirm blocking these clients.
4 When the confirmation message appears, click OK.
   
   Under the Allowed column the green check box turns into a red X, indicating those clients have been blocked.

Blocking allows the client to recover the licenses back into the pool. After a blocked client gets a policy update from client, EPRS wipes all content filter policies from the client machine. From this point on, the client system has no content filter protection. 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 also allows access to the Internet if it is a client behind a firewall enforcing client content filtering.

**To unblock one or multiple clients:**

1 On the Policies tab, navigate to the Enforcement > Clients page.
2 Check the box next to the clients you want to unblock.
3 Click the Unblock Client(s) link at the bottom of the page.
4 When the confirmation message appears, click OK.
   
   Under the Allowed column the red X turns into a green check mark, indicating those clients have been unblocked.
Reports

The reporting server provides a summary of raw data used in reports, and supports the various types of reports along with search and filtering functions.

Topics:
- Categories on page 54
- Sites on page 55
- Initiators on page 56
- Details on page 58

Categories

The categories report provides information the Categories, Match and Attempts.

![Categories Report Example]

Each report has several options for sharing or viewing the data. These options apply to all reports.

- In the upper right corner of the report, you can chose to export the report to a PDF or CVS file.
- The icons in the upper right corner of the shaded area allow you to change the view to chart only, data only or combined chart and data.
- The icon with two curved arrows refreshes the data.
- To view a percentage amount, move the cursor over a category item listed on the right or a section of the pie chart.
- Click on the category or chart item to view the detail report. The categories Match name is shown on the top right side of the screen as shown in the figure below. Click on the Categories option to return to the pie chart view.
Sites

The sites report provides the Site Name, Match and Attempts. To view a percentage amount, move the cursor over a category item listed on the right or a section of the pie chart.
Click on the category or chart item to view the detail report. The Site Name is shown on the top right side of the screen as shown in the figure below.

Initiators

The initiators report provides information on the Initiator Host, User and Attempts. To view a percentage amount, move the cursor over a category item listed on the right or a section of the pie chart.
Click on the category or chart item to view the details report. The **Initiator Host** name is shown on the top right side of the screen as shown in the figure below.
Details

The details report provides information for Timeline, Categories, Sites and Initiators. To view a specific report, click on an item under the report type.

| NOTE: To add a filter click on the + sign to view the drop down menu as shown in the figure below. |
Troubleshooting

 Topics:

- Installation Errors on page 59
- Content Filtering Client Errors on page 59

Installation Errors

Two specific errors 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 fails and a notepad opens with log messages displays. 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

This section describes how to view the various error messages that may display on the Content Filtering Client. The images in this section may be useful for diagnostics.

The following error message displays when the Content Filtering Client license has expired. Log in to your MySonicWALL account to renew your service subscription.
The following message displays when the Content Filtering Client policy is not specified. Navigate to the Policies > Enforcement > Policies page to configure the Policy Settings.

The following 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 message displays when the Content Filtering Client is set to log only. The client is not blocking access to Websites. Navigate to the Policies > Enforcement > Clients 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://support.software.dell.com/)
- [https://forum.sonicwall.com](https://forum.sonicwall.com)
Dell listens to customers and delivers worldwide innovative technology, business solutions, and services they trust and value. For more information, visit http://www.software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases).
- View Knowledge Base articles.
- Obtain product notifications.
- Download software. For trial software, go to http://software.dell.com/trials.
- View how-to videos.
- Engage in community discussions.
- Chat with a support engineer.