

# SonicWall<sup>®</sup> Management CONSOLE

Administration

SONICWALL<sup>®</sup>

# Contents

<b>Zero Touch Pre-Provisioning</b> .....	<b>4</b>
Configuring Zero Touch Pre-Provisioning .....	4
<b>Workflow</b> .....	<b>8</b>
Settings .....	8
Workflow Setting .....	8
Change Order Default Schedule Settings .....	9
Delete Capture Security Center Change Order Data .....	9
Approval Groups .....	9
Approval Groups Search .....	10
Adding an Approval Group .....	10
Editing and Approval Group .....	11
Setting the Default Approval Group for Each Module .....	11
Change Orders .....	12
Change Orders View Style .....	12
Searching Change Orders .....	12
Adding a New Change Order .....	12
Editing Change Orders .....	13
Deleting Change Orders .....	13
Comparing Change Orders .....	13
Managing the Change Orders .....	14
<b>Tasks</b> .....	<b>15</b>
Scheduled Tasks .....	15
Tasks View Style .....	15
Search Criteria .....	15
Search Results .....	16
<b>Log</b> .....	<b>17</b>
View Log .....	17
<b>Management</b> .....	<b>19</b>
General .....	19
Configuring the Miscellaneous Settings .....	19
Users .....	20
User Types .....	20
Configuring a User .....	20
Configuring Screen Access .....	21
Configuring Unit Access .....	22
Configuring Action Permissions .....	22
Custom Groups .....	23
Creating Custom Fields .....	23
Sessions .....	23
Schedules .....	24

Searching for Schedules . . . . .	24
Managing Schedule Groups . . . . .	24
Inheritance Filters . . . . .	26
Message of the Day . . . . .	27
<b>Reports . . . . .</b>	<b>28</b>
Scheduled Reports . . . . .	28
Searching for Scheduled Reports . . . . .	28
Creating Scheduled Reports . . . . .	28
Customizing Scheduled Reports . . . . .	29
Archive . . . . .	29
Downloading Archived Reports . . . . .	29
<b>Events . . . . .</b>	<b>31</b>
Settings . . . . .	31
Severity . . . . .	32
Threshold . . . . .	32
Searching Thresholds . . . . .	33
Adding a Custom Threshold . . . . .	33
Adding a Threshold Element . . . . .	33
Editing a Threshold . . . . .	34
Editing a Threshold Element . . . . .	34
Enabling/Disabling Thresholds and Threshold Elements . . . . .	34
Deleting Thresholds and Threshold Elements . . . . .	35
Alert Settings . . . . .	35
Searching Alert Settings . . . . .	35
Adding an Alert . . . . .	36
Enabling/Disabling an Alert . . . . .	36
Deleting Alerts . . . . .	37
Editing Alerts . . . . .	37
Current Alerts . . . . .	37
<b>Help . . . . .</b>	<b>38</b>
About Management Services . . . . .	38
Tips and Tutorials . . . . .	38
<b>SonicWall Support . . . . .</b>	<b>39</b>
About This Document . . . . .	40

# Zero Touch Pre-Provisioning

Zero Touch pre-provisioning configuration allows an administrator to create templates containing specific operations that can be performed on a zero-touch managed device, when it connects for the first time to Capture Security Center. Historically, in order to perform automatic operations on newly added devices, an administrator has to either add the unit manually and then create tasks to assign to the unit, or log in to the user interface to perform the same after the unit is added. This feature allows an administrator to assign such tasks on units even before they become available in Capture Security Center.

## Configuring Zero Touch Pre-Provisioning

Zero Touch pre-provisioning allows administrators to define and create templates containing specific operations that can be performed on a Zero Touch managed device, when it connects first time to CSC-MA. With pre-provisioning, it is easier to add multiple devices that do not require any additional configuration settings to be loaded later on for their operation.

 **NOTE:** All firewalls under a group must be of identical models to avoid conflicts on Golden Pref Push.

### *To configure Zero Touch:*

- 1 Navigate to **CONSOLE | Zero Touch**.
- 2 Click **Add**.
- 3 Enter a name and description for the template.

**CONFIGURATION SETTINGS**

**Name**

**Description**

---

**CONFIGURATION OPERATION SETTINGS**

☰ Secure Password Enforcement

The default password is not secured, users must configure new password and apply to units as soon as it comes online.

Enable Password Enforcement

**Note:**

1. Leave the passwords fields below empty to let GMS generate new random passwords for your SonicWall(s). The generated password for the unit can later be viewed from the System > Administrator screen.
2. Change password action requires the current password of the Firewall. Ensure the password stored for this unit is current. ZeroTouch units are added automatically with their default password. To update the password, go to Tree Control, Right click on the unit and choose Modify Unit.

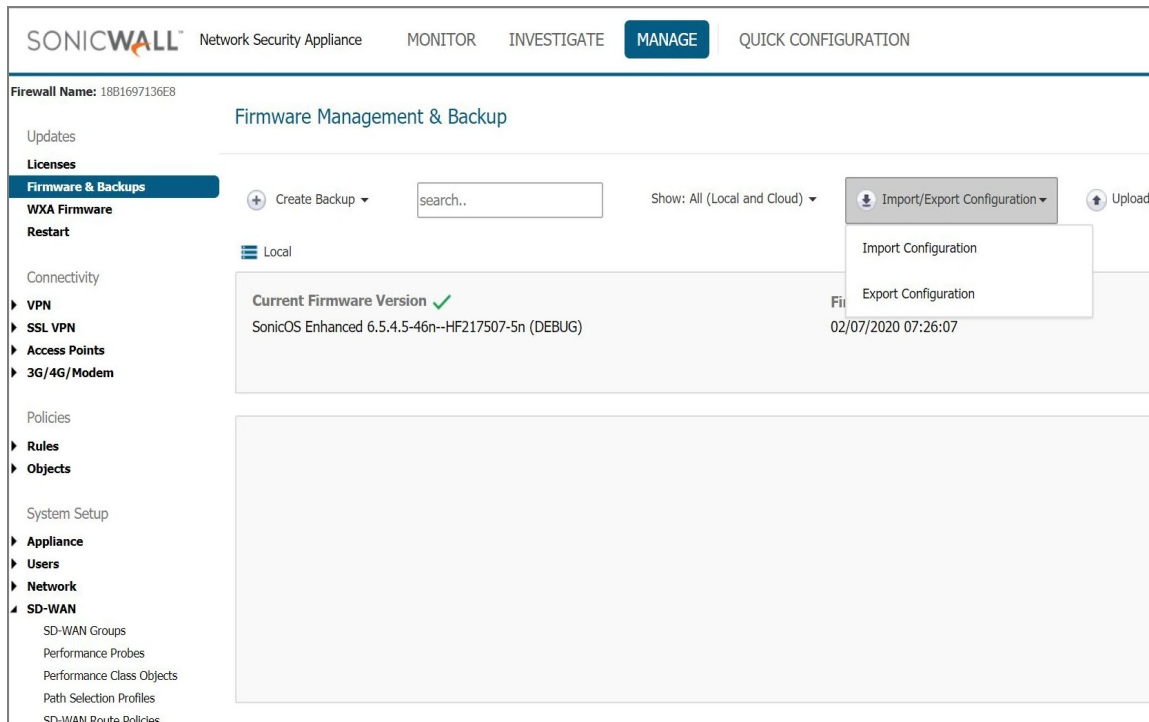
**New Password**   Show

**Confirm Password**

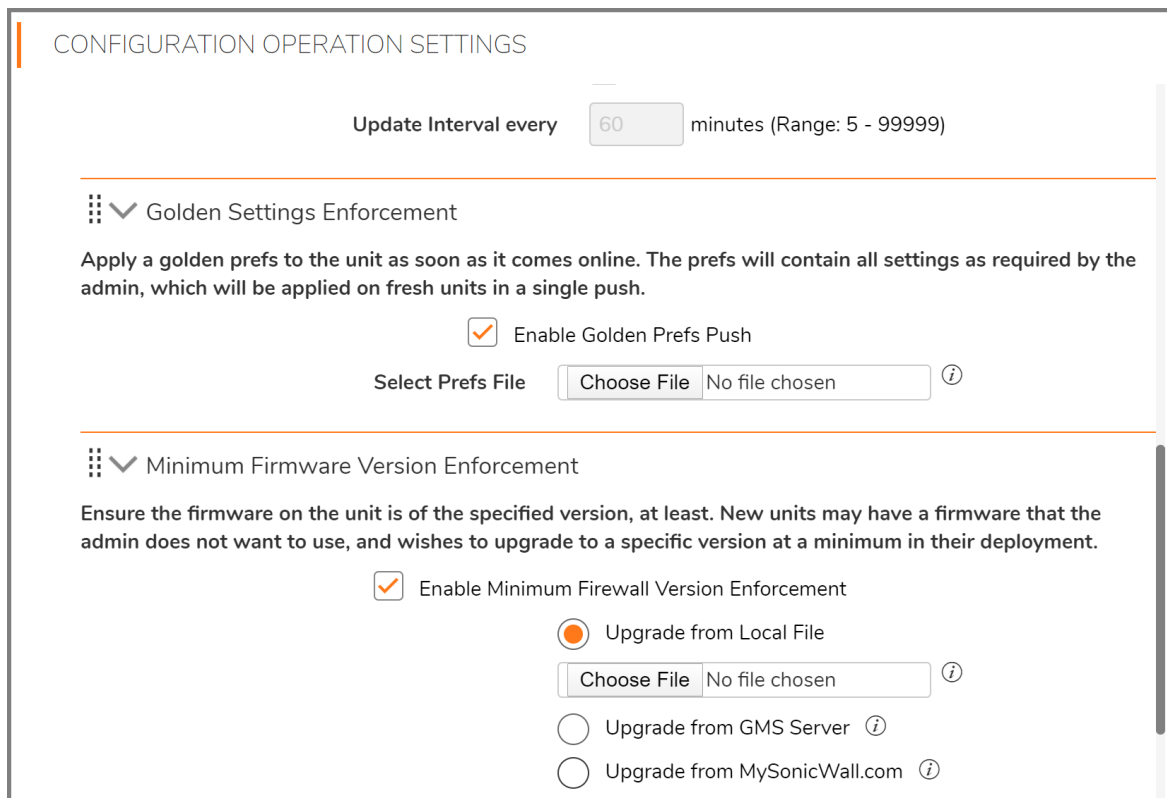
---

☰ > Firewall Settings Enforcement

- 4 Under **Secure Password Enforcement**, check **Enable Password Enforcement** and enter a new password.
- 5 Under Firewall Settings Enforcement, check **Enable Firewall Settings Enforcement** and then configure DNS settings and time zone settings.
- 6 Under Golden Settings Enforcement, check **Enable Golden Prefs Push**. The preferences file must be downloaded from the firewall.
- 7 To download configuration file from firewall:
  - Log in to the firewall
  - Click **Manage**.
  - Click **Firmware & Backups**.
  - Click **Import/Export Configuration** drop-down menu and select **Export Configuration**.
  - Download the file to the local machine.



8 Click **Choose File** and upload the configuration file downloaded from firewall.

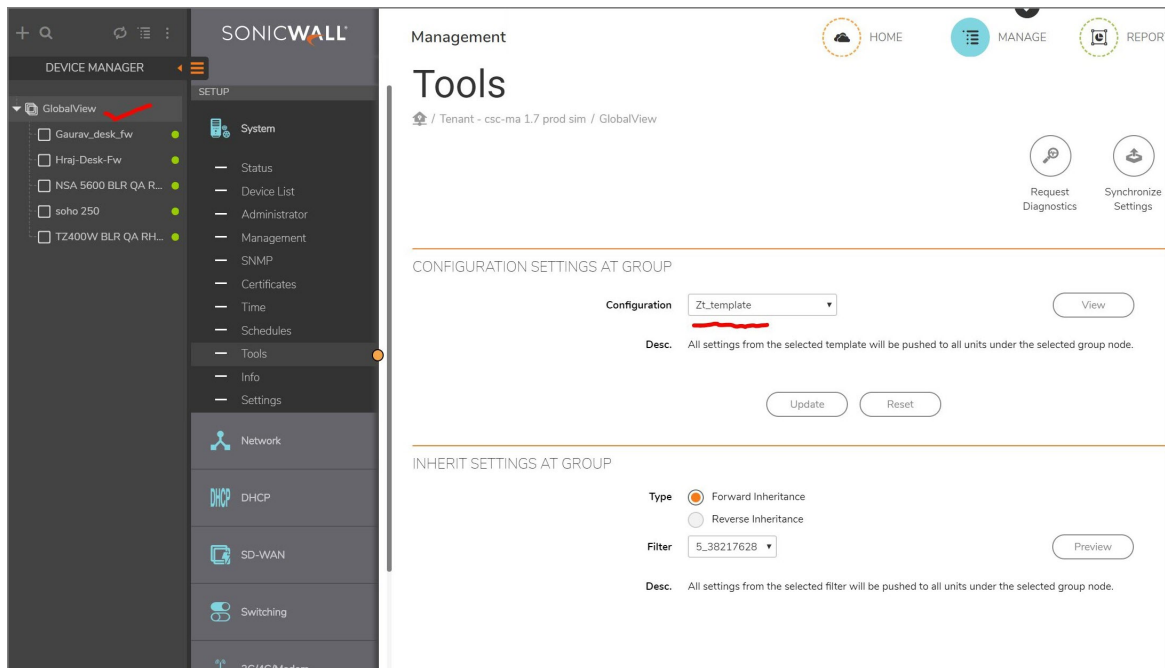


9 Expand **Minimum Firmware Version Enforcement**. When you set minimum firmware version enforcement, if a new unit has an older unsupported firmware, it is upgraded to the specified firmware.

10 Select one of the options. Your options are:

- Upgrade from Local File.

- Upgrade from GMS server.
  - Upgrade from MySonicWall.com.
- 11 If you select Upgrade from Local File, you have to upload the firmware from your computer manually.
  - 12 Expand Reporting, Analytics and Visualization Enforcement and check **Enable Reporting, Analytics, and Visualization Enforcement**.
    - Select Cloud Infrastructure if you want to receive logs in your cloud infrastructure.
    - Select SonicWall Analytics OnPrem if you want to receive logs in your SonicWall Analytics appliance.
  - 13 Click **Update**.
  - 14 To enforce the Zero Touch configuration file, navigate to **System | Tools** menu in **GlobalView**. In the **Configuration** drop-down menu, select the template file and click **Update**.



# Workflow

This chapter describes how to configure **Workflow** in the **CONSOLE | Workflow** page. With **Workflow** enabled, any configuration or policy changes made to Management **CONSOLE** screens must go through an approval process before being considered *live*. Only after the changes have been approved, are they pushed out to the appliances. **Workflow** also allows changes to be processed or executed to be scheduled. You can create approval groups - the members of which are to approve the changes.

The **Workflow** feature (Enable or Disable) can be enabled or disabled on a per-domain basis.

## Topics:

- [Settings](#)
- [Approval Groups](#)
- [Change Orders](#)

## Settings

Workflow is a system to oversee configuration changes made to one or more appliances. You can perform reviews and provide feedback on the changes proposed, assign ownership and provide accountability for all actions. All these steps include complete logging for auditing.

**NOTE:** Even when enabled, Workflow only applies on appliances that are actively licensed for the following services: CSC Management or CSC Management and Reporting.

On the **CONSOLE | Workflow > Settings** page, enable Workflow, configure default schedule settings, and delete change order data.

This section contains the following Settings topics:

- [Workflow Setting](#)
- [Change Order Default Schedule Settings](#)
- [Delete Capture Security Center Change Order Data](#)

## Workflow Setting

### *To configure the Workflow settings:*

- 1 Navigate to **CONSOLE | Workflow > Settings**.
- 2 Select the appropriate **Domain** from the drop-down menu to view corresponding settings.
- 3 Select the check-box for **Enable Change Order Management** and/or **Enable Approval Management** to activate the Workflow functionality.
- 4 Click **Update** to accept the changes you have made.



# Change Order Default Schedule Settings

Change orders can be scheduled to be executed on submission, based on the settings you define. Specifying a default automatically uses the selected setting when a new change order is created.

## *To configure a regular schedule to manage change orders:*

- 1 Select one of the following options for when you want change orders to go into effect:
  - **Execute Manually**
  - **At** and select an option from the drop-down list
- 2 Click **Update** to save the changes you made.

# Delete Capture Security Center Change Order Data

You can typically delete change orders that are more than two years old and no longer necessary. This is a one-time action that is executed based on the date selected for deletion. The delete action in this screen only purges data, tasks, and logs related to Change Orders.

## *To delete change order data:*

- 1 Navigate to **CONSOLE | Workflow > Settings**.
- 2 At the top, select the **Domain** from which to delete the change orders.
- 3 In the **Delete Capture Security Center Change Order Data** section, choose a date that is older than two years. Any change orders older than this data is deleted.
- 4 Click **Update** to save the changes you have made.

# Approval Groups

When using the change order process, you should start by defining the members of the various policy Approval Groups. These members have the final word on whether a proposed change order is approved or denied. You can create Approval Groups for each unit, and those groups can exist with one or more notification users.

The process by which change orders are approved, fully approved, partially approved, or denied begins at the submission level and progresses through the various levels defined by the change approval group.

A Default Approval Group is created for every new domain that has the domain 'admin' user listed as the default approver. The Default Approval Group is the default approval group applicable to the different modules. The Default Approval Group cannot be deleted; it can only be edited with new users being added or existing users being deleted.

After your Approval Groups have been established for each module, you can manage change orders for approving, scheduling, and processing the proposed changes through **Workflow**.

This section contains the following Approval Groups topics:

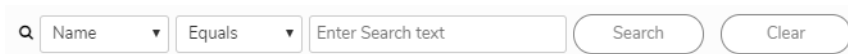
- [Approval Groups Search](#)
- [Adding an Approval Group](#)
- [Setting the Default Approval Group for Each Module](#)

## Approval Groups Search

On the **CONSOLE | Workflow > Approval Groups** page, you can search for specific approval groups.

**To search for specific approval groups:**

- 1 Navigate to **CONSOLE | Workflow > Approval Groups**.



- 2 In the first field, select **Name** or **Destination**.
- 3 In the second field, choose from **Equals**, **Starts with**, **Ends with**, or **Contains**.
- 4 In the third field, enter the text string to search on.
- 5 Click on **Search**.
- 6 To clear the Search filter, click on **Clear**.

## Adding an Approval Group

The **Add New Approval Group** option allows you to select users as approvers. The approval groups are listed in the table when done.

**To add an Approval Group:**

- 1 Navigate to **CONSOLE | Workflow > Approval Groups**.
- 2 Click **Add New Approval Group**.
- 3 Enter an approval group name in the **Name** field.
- 4 Select a domain from the **Domain** drop-down menu. Your selection should be the domain that is being managed by that Approval Group.

**NOTE:** Each domain admin user can view the Approval Groups only for that domain. Only the super administrator (admin@LocalDomain) can view all the Approval Groups for all domains. The super administrator can see an additional column that reveals the domain names.

- 5 Enter a short description in the **Description** field.
- 6 Click **Add New User** and select a user from the drop-down lists.

- 7 If you want people other than the approvers to receive notification about the approvals, click **Add Additional User**.
  - a Select **Email - User** or **Email - Ad hoc** from the first drop-down list.
  - b Choose the user from the second drop-down list.
  - c Click the **Delete** icon if you want to remove that user.
- 8 Click **OK**.

## Editing and Approval Group

### *To edit an Approval Group:*

- 1 Navigate to **CONSOLE | Workflow > Approval Groups**.
- 2 Click the **Edit** icon next to the Group Name that you would like to edit.
- 3 Enter a name in the **Name** field.
- 4 Select a domain from the **Domain** drop-down menu. Select the domain under the jurisdiction of this Approval Group.

**NOTE:** The Name and Domain fields are not editable for the Default Approval Group.

- 5 Update the description, if needed.
- 6 Click **Add New User** to add additional approvers to the Approval Group.
- 7 Click **Add Additional User** to include more users to receive notifications on approvals and other actions.
- 8 Click **OK**.

## Setting the Default Approval Group for Each Module

### *To set the default approval group for each module:*

- 1 Navigate to **CONSOLE | Workflow > Approval Groups**.
- 2 In the **Default Approval Group for Each Module** section, select the domain from the drop-down menu to view the corresponding Default Approval Group.
- 3 In the All Policies Panel Screens field, choose an option from the drop-down list.
- 4 Click **Update**.

# Change Orders

Change Order management is a component of Workflow that allows you to view changes made to appliance, preview changes inline (on the screen in the context of the appliance), and compares multiple change orders. The change orders are managed on the **CONSOLE | Workflow > Change Orders** page; you can add, edit, and delete change orders, although you can create items for the change order on any screen.

## Change Orders View Style

At the top of the **Change Orders** page, you can select which change orders are displayed in the **Change Orders** table. The options are:

- Active Changes Orders
- Processed Changes Orders
- All Change Orders, which includes both active and processed change orders

## Searching Change Orders

Use the search options at the top of the **Change Order** table to search for a specific change order.

- 1 In the **Name** field, select **Name** or **Destination**.
- 2 In the second field, choose **Equals**, **Starts with**, **Ends with**, or **Contains** based on your search string.
- 3 In the third field, enter the text string to search.
- 4 Click **Search**.
- 5 To clear the Search filter, click **Clear**.

## Adding a New Change Order

*To add a new change order:*

- 1 Select the **Add New Change Order** button.
- 2 Enter the change order **Name**.
- 3 Add a **Description** to the field provided.
- 4 Select the **Domain** from the drop-down list.
- 5 Select one of the following schedules:
  - **Execute Immediately**
  - **At** and select an option from the drop-down list

**i** | **NOTE:** You can also create a new schedule by clicking on **Add Schedule**. Define the data and time for the new schedule. Then select the new schedule from the **At** drop-down list.

- 6 Of the changes listed, identify which ones you want to include in this new change order.
- 7 Click **OK** to save the change order.

# Editing Change Orders

The options for editing a change order are similar to adding a change order.

## *To edit a change order:*

- 1 Click the **Edit** icon next to the change order you want to update.
- 2 Make changes to the fields needed under **Change Order Settings**, if needed.
- 3 In the **Changes** section, add or remove changes to the change order.
- 4 Click **OK** when done or **Cancel** to exit without saving the changes.

# Deleting Change Orders

You can delete one or more change orders from the change order table.

## *To delete multiple change orders:*

- 1 Check the box by the name of the change orders you want to delete.
- 2 Click the **Delete Change Order(s)** button.

## *To delete a single change order*

- 1 Click the **Delete** icon (garbage can) in the **Configure** column of the change order you want to delete.

# Comparing Change Orders






You can select change orders and compare them to each other.

## *To compare change orders:*

- 1 Select the change orders you want to compare by checking the box next to them.
- 2 Click **Compare Change Orders**.
- 3 In the window that appears, select the option you want to view:
  - Settings
  - Multi-RADIUS
  - Local Users
- 4 Close the window when done and clear the selected change orders.

# Managing the Change Orders

You can take several actions during the course of managing your change orders. Choose the appropriate icon in the ACTIONS column.

Action	Definition
	Validate this change order.
	Submit this change order for task creation.
	View contents of this change order.
	Preview contents of this change order against actual contents of a selected unit.
	View logs of this change order.

# Tasks

This section describes how to configure scheduled tasks in the **CONSOLE | Tasks** page.

## Topics:

- [Scheduled Tasks](#)

## Scheduled Tasks

As you complete multiple tasks through the Management **CONSOLE**, the Management service creates, queues, and applies them to the appliances. As the tasks are processed, some appliances might be down or offline. When this occurs, the tasks are re-queued and attempted again.

## Topics:

- [Tasks View Style](#)
- [Search Criteria](#)
- [Search Results](#)

## Tasks View Style

To filter only the type of tasks you want to see, navigate to **CONSOLE | Tasks > Scheduled Tasks** and select one of the check boxes under **TASKS VIEW STYLE**:

- **Pending Tasks**
- **Executed Tasks**
- **All Tasks**

Select **Change Order Tasks Only** if you want to see only Change Order Tasks.

## Search Criteria

You can search for tasks that meet a specific set of criteria by using **SEARCH CRITERIA**. Navigate to that section of the **Scheduled Tasks** page, set the search criteria and click **Start Search**. The updated results are displayed in the **Search Results** section.

Click **Clear Search** to clear the search parameters and update the search results.

# Search Results

Once you select a Task View or perform a search, the results are displayed under **SEARCH RESULTS**. By default Search Results shows 10 tasks per page. You can change the number of tasks shown per page by entering a number between 10 - 100.

If you know the task number, you can go to the task directly by entering the task number in **Go To Task Number**.

The search result has the following information:

- **Checkbox**—selects the task in which you want to perform an action. Your options are:
  - **Execute the tasks selected now**
  - **Re-schedule the tasks selected**
  - **Delete the tasks selected**
- **STATUS**—displays the status of the unit. Mouse over the icon to see the definition.
- **SONICWALL**—specifies the name of the SonicWall unit to which the task applies.
- **DESCRIPTION**—contains a description of the task.
- **CREATION TIME (LOCAL)**—specifies the date and time the task was generated.
- **SCHEDULED TIME (LOCAL)**—notes the time the task was scheduled in the local time zone of the appliance.
- **SCHEDULED TIME (AGENT)**—specifies the time the task was scheduled in the time zone of the agent.
- **LAST ATTEMPT (LOCAL)**—specifies the time the task was last attempted in the local time zone of the appliance.
- **NO. OF ATTEMPTS**—specifies the number of times the Management service has attempted to execute the task.
- **LAST ERROR**—specifies the error if the task was not successfully executed.
- **SGMS USER**—shows the name of the user who created the task.
- **Agent (IP)**—specifies the IP address of the agent. This column displays IPv6 and IPv4 addresses.



# Log

Logs help track activities in the system. These activities are associated, either directly or indirectly, with user-initiated actions or based on system-initiated actions. These logs are important support for audit trails and compliance purposes, as well as for troubleshooting system operation.

## Topics:

- [View Log](#)

## View Log

The log tracks changes made from the user interface, logins, failed logins, logouts, password changes, scheduled tasks, failed tasks, completed tasks, raw syslog database size, syslog message uploads, and time spent summarizing syslog data.

### To view the log:

- 1 Navigate to **CONSOLE | Log > View Log**.
- 2 Scroll down to the **SEARCH RESULTS** section.

Each log entry contains the following fields:

- **DATE**—specifies the date of the log entry.
- **MESSAGE**—contains a description of the event.
- **SEVERITY**—displays the severity of the event (Alert, Warning, or Info).
- **SONICWALL**—specifies the name of the SonicWall appliance that generated the event (if applicable).
- **GMS USER**—identifies the user role.
- **USER IP**—specifies the user name and IP address.

You can also sort the **SEARCH RESULTS**. Click on any one of the column headings to sort the table descending or ascending based on the column heading.

- 3 Enter any number between 10 and 100 in the **Messages Per Screen** field to set number results shown per page.

### To search the results:

 **TIP:** You can press **Enter** to navigate from one element to the next in this section.

- 1 Navigate to **CONSOLE | Log > View Log**.
- 2 In the **SEARCH CRITERIA** section, use the following fields, as needed, to refine your search:
  - **Select Time of logs (From and To)**—Select from and to date to find the log entries created during the time.

- **SonicWall Node**—displays all log entries associated with the specified SonicWall appliance that you list.
  - **Message contains**—enter any text find the events relevant to the text.
  - **Severity**—select the severity level of the log. Your options are:
    - **All (Alert, Warning, and Info)**
    - **Alert and Warning**
    - **Alert**
  - Select **Match case** to make the **SonicWall Node** and **Message contains** search fields case sensitive.
  - Select one of **Exact Phrase**, **All Words**, or **Any Word** to customize your search.
- 3 Click **Start Search**.
  - 4 To clear all values from the input fields and start over, click **Clear Search**.
  - 5 To download the results as an HTML file on your system, click **Export Logs** and download the file to your computer.

# Management

This chapter describes the settings available in the **CONSOLE | Management** section.

## Topics:

- [General](#)
- [Users](#)
- [Custom Groups](#)
- [Sessions](#)
- [Schedules](#)
- [Inheritance Filters](#)
- [Message of the Day](#)

## General

On the **CONSOLE | SYSTEM SETUP > Management > General** page, you can configure Capture Security Center miscellaneous settings.

## Configuring the Miscellaneous Settings

### *To configure the miscellaneous settings:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Management > General**.
- 2 The **MISCELLANEOUS SETTINGS** section appears.
- 3 Set the **Capture Security Center Inactivity Timeout** in the field provided. The time should be state in minutes. An entry of **-1** means the system never times out.
- 4 Set the number of rows that appear in non-reporting related screens in **Max Rows Per Screen**. The value can range from 10 to 100.
- 5 Define the **Auto Save Dashboard Settings**. The value can range from 1 to 60. An entry of **-1** means the auto save is not enabled.
- 6 To configure what you want to see on the Appliance Selection Panel, enable or disable the following:
  - Select Icons, Text, or Icons and Text (default)
  - Check Enable Audio alarm when a Managed Unit goes Up/Down or both.

- 7 To configure the **Message of the Day**:
  - a Click on **View Message of the Day**.
  - b Disable the **Message of the Day** by checking the box **Don't display message when logging in**.
  - c Click **Close**.
- 8 Click **Update** to save the new settings.

## Users

To operate in complex environments, Capture Security Center Management is designed to support multiple users, each with his or her own set of permissions and access rights. This section contains the following subsections:

- [User Types](#)
- [Configuring a User](#)
- [Configuring Screen Access](#)
- [Configuring Unit Access](#)
- [Configuring Action Permissions](#)

**i** **NOTE:** If you do not want to restrict access to SonicWall appliances or functions, but want to divide SonicWall Capture Security Center responsibility among multiple users, use views to provide specific criteria to display groups of SonicWall appliances. Depending on the type of task they are trying to perform, users can switch between these views as often as necessary. For more information, refer to [Configuring Action Permissions](#).

**i** **NOTE:** All of the user configuration options are available through the command-line interface. For more information, refer to the [Capture Security Center Command-Line Interface Guide](#).

## User Types

A user type is a group of users who complete similar tasks and have similar permissions.

Capture Security Center provides four pre-configured groups:

- **Administrators**—Full view and update privileges.
- **End Users**—No privileges.
- **Guest Users**—No privileges.
- **Operators**—View privileges only.

## Configuring a User

You can use the Users page to configure different settings of a user type or a user.

**To configure a SonicWall user or user type:**

- 1 Navigate to **CONSOLE | Management > Users**. The Users page appears.
- 2 Select a user or user type under **All Users**.

- 3 Under **General** tab, you can change default view, specify date until when the user should be active, and select one of the preset schedules for the user.
- 4 Click **OK**.

## Configuring Screen Access

The Screen Permissions page contains a hierarchical list of all screens that appear within Capture Security Center. From this screen, you can control access to individual screens or all screens within a section. This includes permissions for users or groups to view, or view and update reports

**i** | **NOTE:** By default, a new user group has no privileges.

### *To configure screen access settings for a user or user group:*

- 1 Navigate to **CONSOLE | Management > Users**. The Users page appears.
- 2 Select a user or user type under **All Users**.
- 3 Click the **Screen Permissions** tab.
- 4 Under **All Screens**, select a panel, section, or screen. For example, for Reports panel screens, you can select the whole panel, the unit type section such as Firewall, SMAs, or Email Security (ESs), the group of reports for that type of unit, or the individual report or screen for which you want to set permissions.

On the right side of the pane, select from the following:

- To prevent any access to the object, select **None**.
  - To allow view only access, select **View Only**.
  - To allow the user or group to make updates only for unit-level screens and not for group-level screens, select **Update At Unit Level Only**. This option is only available for objects in the Policies and Reports panels.
  - To allow the user or group to make updates at the unit level screens as well as one level up, select **Update At Unit and One Level Up**.
  - To update all levels, click **Update At All Levels**.
- 5 Click **Update** to apply the permission changes.
  - 6 You might see a warning screen if you are applying permission changes to a group, verify that you wish to apply these changes to the group and all users within that group and click **OK**.

**i** | **NOTE:** The more specific settings override the more general settings. For example, if you select View Only for the Status group of reports and select None for the Up-Time over Time report, then the selected user only sees the Up-Time Summary report in the Status reports and have View Only permission for that report.

- 7 To clear all screen settings and start over, click **Reset**.
- 8 When finished, click **Update**.

# Configuring Unit Access

The Unit Permissions page contains a hierarchical list of all SonicWall appliances that appear within Capture Security Center. From this screen, you can control access to SonicWall groups or individual SonicWall appliances.

## *To configure appliance access settings for a user:*

- 1 Navigate to **CONSOLE | Management > Users**. The Users configuration page appears.
- 2 Select a user.
- 3 Click the **Unit Permissions** tab.
- 4 Select a View from the **Views** pull-down menu.
- 5 To provide the user with access to a SonicWall group or appliance, check the box next to the appliance name, then click **Update**.
- 6 Repeat **Step 5** for each group or appliance to add.
- 7 To prevent the user from accessing a SonicWall group or appliance, uncheck the box next to the group or appliance name, then click **Update**.
- 8 Repeat **Step 7** for each group or appliance to remove.

# Configuring Action Permissions

The Action Permissions tab contains a list of actions and view options that can be enabled/disabled for a user type or user.

## *To configure the action permissions:*

- 1 Navigate to **CONSOLE | Management > Users**. The Users page appears.
- 2 Select the user or group.
- 3 Click the **Action Permissions** tab.
- 4 Select the unit actions you wish to be available for the group or user in the **Units** section.

### Available Units Actions

Name	Description
Add Unit, Modify Unit, Delete Unit	Add, delete, or modify the management specifications of managed units.
Rename Unit	Renames the unit.
Login to Unit	Gains access to the managed unit's interface through Capture Security Center.
Modify Properties	Modifies the properties of the managed units.

- 5 Select the view options you wish to be available for the group or user in the **Views** section.

### Available Views Options

Name	Description
Manage View	Alters the properties of views.
Change View	Change between views.

- 6 Click **Update**.

# Custom Groups

The Capture Security Center uses an innovative method for organizing SonicWall appliances.

SonicWall appliances are not forced into specific, limited, rigid hierarchies. Simply create a set of fields that define criteria (for example, country, city, state) that separate SonicWall appliances. Then, create and use views to display and sort appliances on the fly.

## Creating Custom Fields

When first configuring Capture Security Center, you must create custom fields that are entered for each SonicWall appliance. Capture Security Center supports up to ten custom fields.

**NOTE:** Although SonicWall supports up to ten custom fields, only seven fields can be used to sort SonicWall appliances in any view.

Capture Security Center is pre-configured with four custom fields: Country, Company, Department, and State. These fields can be modified or deleted.

### *To add custom fields:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Management > Custom Groups**.
- 2 Right-click **Custom Groupings** in the right pane.
- 3 Click **Add Category** from the pop-up menu.
- 4 Enter the category name of the first field such as Department.
- 5 Enter a Default Value, such as Engineering.
- 6 Click **OK**.
- 7 Select the newly created field and select **Add Category** from the pop-up menu.
- 8 Enter the name of the new field.
- 9 Repeat Steps 6 through 8 for each field that you want to create. You can create up to ten fields.

**NOTE:** Although the fields appear to be in a hierarchical form, this has no effect on how the fields will appear within a view. To define views, see [Configuring Action Permissions](#).

To delete fields, right-click any of the existing fields and select **Delete Category** from the pop-up menu.

# Sessions

The Sessions page of the Management section allows you to view session statistics for currently logged in users and to end selected sessions.

### *To end a session:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Management > Sessions**.
- 2 Select any active session to end it.
- 3 Click **End selected sessions**.

# Schedules

The Schedules page allows you to create and manage schedules and schedule groups for enforcing schedule times.

- [Searching for Schedules](#)
- [Managing Schedule Groups](#)
- [Managing Schedules](#)

## Searching for Schedules

Use the search options at the top of the **SCHEDULE GROUPS** and **SCHEDULES** tables to search for a specific schedule.

- 1 In the first field, select **Name**, **Description** or **Enabled?**.
- 2 In the second field, select a logical condition based on what information you want to search.
- 3 In the third field, enter the text string to search on.
- 4 Click on **Search**.
- 5 To clear the Search filter, click on **Clear**.

## Managing Schedule Groups

The Schedule Groups table displays all your predefined and custom schedules. In the Group Schedules table, there are four default group schedules from which to choose: **Daily 24x7**, **Weekdays 24x7**, **8x5 Work Hours**, and **Weekend Hours**.

A group schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a right-arrow button appears next to the schedule name. Clicking the **Expand** icon expands the schedule to display all the day and time entries for the schedule.

You can modify these group schedules by clicking the **Edit** icons in the Configure column to display the **Edit Schedule Group** window.

## Adding Schedule Groups

*To add a schedule group:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Management > Schedules**.
- 2 Click **Add Schedule Group**.
- 3 Enter a descriptive name for the group schedule in the **Name** field.
- 4 Enter a group schedule description in the **Description** field.
- 5 Click **Visible to Non-Administrators** if you would like to make the schedule viewable by the public.
- 6 By clicking once on the desired Schedule time descriptions, use the arrow keys to move them into the right field. These are the parameter that will be used in your schedule group range.
- 7 Click **Update** to group the entries into one named schedule.



## Editing Schedule Groups

To edit an existing schedule group, navigate to **CONSOLE | Management > Schedules** and click the **Edit** icon on the right side of the screen. The screen and procedure for editing are the same as those for adding an event schedule group. See [Schedules](#).

## Deleting Schedule Groups

You can delete schedule groups. You cannot delete predefined static schedules or schedule groups. Only Administrators and Owners can delete schedules or schedule groups.

**i** | **NOTE:** Deleting a Schedule or Schedule Group that is in use is not permitted. A warning message displays when this action is performed.

### *To delete a schedule group:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Management > Schedules** and select the check box next to the name of the group you would like to delete.  
  
All subordinate check boxes are selected when you click the Schedule Name. Expand the group arrow if you would like to delete individual entries from the group.
- 2 Click **Delete Schedule Group(s)/Remove Schedule(s) from Group**.
- 3 Confirm the deletion by clicking **OK** on the window that appears.

## Managing Schedules

The Schedules table displays all your predefined and custom schedules. In the Schedules table, there are several default schedules you can use or modify.

You can modify these schedules by clicking the **Edit** icons in the Configure column to display the **Edit Schedule** window.

## Adding Schedules

### *To create a schedule:*

- 1 Navigate to **CONSOLE | Management > Schedules** and click **Add Schedule**. The **Add Schedule** page is displayed.
- 2 Enter a descriptive name for the schedule in the **Name** field.
- 3 Select a domain name from **Domain** drop-down menu.
- 4 Enter a schedule description in the **Description** field.
- 5 Click **Visible to Non-Administrators** if you would like to make the schedule viewable by the public.
- 6 Click **Disable** to take the schedule offline but still available for use later when activated.
- 7 Click **Invert** to reverse the schedule order.
- 8 Select one of the following radio buttons for **Schedule**:
  - **One-time occurrence** – For a one-time schedule at the configured **Date and Time**.
  - **Recurrence** – For schedules that occur repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under **Recurring** become active, and the fields under **One-time occurrence** become inactive.

- 9 For a One-time Occurrence, configure the starting date and time by entering the **Month, Day, and Year** (mm/dd/yyyy) and the **Hour, and Minute** in the fields. The time is represented in 24-hour format.
- 10 In the fields under **Recurrence**, select the check boxes for the days of the week to apply to the schedule or select **All**.
- 11 Under **Recurrence**, type in the time of day for the schedule to begin in the **Start Time** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
- 12 Under **Recurrence**, type in the time of day for the schedule to stop in the **End Time** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
- 13 Click **Add**.
- 14 Click **Update** to add the schedule to the **Schedule List**.

## Editing Schedules

Navigate to **CONSOLE | Management > Schedules** and click the **Edit** icon on the right side of the screen. The screen and procedure for editing are the same as those for adding a schedule. See [Managing Schedules](#).

## Deleting Schedules

You can delete custom schedules, but you cannot delete the default **Work Hours, After Hours, or Weekend Hours** schedules.

### *To delete individual schedule objects that you created:*

- 1 To delete existing days and times from the **Schedule List**, select the row and click **Delete Schedule(s)**. Or, to delete all existing schedules, click the check box next to **Name** and then click **Delete Schedule(s)**.

## Inheritance Filters

The Inheritance Filters page specifies which settings are inherited from the group when adding a new SonicWall appliance.

### *To configure the SNMP Inheritance Filter page:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Management > Inheritance Filters**.
- 2 To edit an existing filter, select the filter from the **Select Filter** list box. To specify a new filter, select **New Filter** from the **Select Filter** pull-down menu and type a name in the **Filter name** field.
- 3 Select which page settings are inherited in the **Inheritance Filter Detail** section.
- 4 Select the type of access that is available to each user group from the **Access for each User Type** section.
- 5 When you are finished, click **Add** for a new filter or click **Update** for an existing filter. The settings are changed. To clear the settings and start over, click **Reset**.

# Message of the Day

The Message of the Day page displays a message when administrators log on to Capture Security Center.

## *To configure the Message of the Day page:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Management > Message of the Day**.
- 2 Check the box to enable the option if not already done.
- 3 Select all users, a user group, or an individual user.
- 4 Enter message text in the **Message** field.
- 5 Select whether the message text is displayed in plain text or HTML.
- 6 Select the start and end date of the message (default: current day).
- 7 When you are finished, click **Update**.
- 8 Repeat this procedure for each group or user for which this message is displayed.

# Reports

The **Reports** section lets you search through Scheduled Reports. You can also create, delete, or archive Scheduled Reports. **Reports** has the following sections:

- [Scheduled Reports](#)
- [Archive](#)

## Scheduled Reports

The **Scheduled Reports** page shows you the number of schedules in the system, the date on which weekly schedules were last attempted, the date on which monthly schedules were last attempted, next scheduled email/archive time, next weekly reports time, and the next monthly reports time.

## Searching for Scheduled Reports

You can sort the **Scheduled Reports** table based on schedule name, report ID, schedule type, email subject, schedule owner, last run time, and status. You can also use the search field to search and find a particular scheduled report.

### *To search for a Scheduled Report:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Reports > Scheduled Reports**.
- 2 At the top left of the table, in the search field, type the schedule name or ID.
- 3 Click Enter.

## Creating Scheduled Reports

The **Scheduled Reports** page shows you the details about the scheduled reports in a table format. You have the options to search, schedule, archive, edit, or delete reports in the **Scheduled Reports** table.

### *To create a Scheduled Report:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Reports > Scheduled Reports**.
- 2 At the top-right of the table, click **Create a Schedule Report**.
- 3 In the **CREATE SCHEDULE** page, select the device and click **Next**.
- 4 Under **REPORT LIST**, select the reports to which you want to create a schedule.
- 5 Click **Next** and follow the on-screen instructions.

# Customizing Scheduled Reports

The **Scheduled Reports** page lets you customize scheduled PDF reports. You can customize logo, cover title, header, and footer in a scheduled report.

## To customize a Scheduled Report:

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Reports > Scheduled Reports**.
- 2 At the top-right of the table, click **Create a Schedule Report**.
- 3 In the **CREATE SCHEDULE** page, enter the schedule name and schedule interval and then click **Next**.
- 4 Click **Select Reports to Archive** icon next to the device and click **Next**.
- 5 Select the components and click **Next**.
- 6 Under **COVER PAGE SETTINGS**, you can upload a logo and specify a cover title.
- 7 Click **Next** and click **Create**.

## Archive

Archive page shows you the list of archived **Scheduled Reports**. You can sort the archived reports table based on schedule name, format, source, trigger, generation time, start time, or end time.

You can download archived reports or delete reports, if you no longer need them.

## Downloading Archived Reports

### To download multiple archived reports:

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Reports > Archive**.
- 2 Select the check boxes in front of each of the report that you want to download.

3 At the top-right of the table, click **Select Multiple Rows to Download**.

# Events

The Management Console provides a customized and controlled way in which events are managed and alerts are created. In the **CONSOLE** view, you can systematically configure each sub-component of your alert in order for the alert to best accommodate your needs.

To get the most benefit, you must configure alerts for important events. In the **CONSOLE | SYSTEM SETUP > Events** options, you can configure the frequency of subscription expiration and task failure notifications, as well as severities, thresholds, schedules, and alerts for handling events.

## Topics:

- [Settings](#)
- [Severity](#)
- [Threshold](#)
- [Alert Settings](#)
- [Current Alerts](#)

## Settings

In the **CONSOLE | SYSTEM SETUP > Events > Settings** page, you can specify the following:

- Email Alert Format Preference, such as HTML (default), email, or SMS.
- Email Alert Thresholds.

### *To configure the Settings:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Events > Settings**.
- 2 Under **Email Alert Format Preferences**, select whether the email alert is sent as **HTML**, **Plain Text**, or **Plain Text (Simple)**. The Simple setting sends a very short email to ensure that the email is not cut off by character limits.
- 3 Under E-Mail Alert Thresholds, input the number of times to send an email when a task fails. The count can range from 0 to 50. Enter 0 if you don't want email alert.
- 4 Set threshold limit for transaction log size to receive alerts when transaction logs reach the threshold.
- 5 Click **Update**.

# Severity

In the **CONSOLE | SYSTEM SETUP > Events > Severity** page, you can create your own severity levels or use predefined severity levels. You can delete severity levels in this screen as well. Defining the severity priority can also be performed in this screen. Users with permissions to the Severity screen can create and edit these severities.

The Management service supplies the following three predefined severity levels:

- **Information:** This is the lowest severity level
- **Warning:** This is a mid-range severity level
- **Critical:** This is the highest severity level

## *To configure Event Severities:*

- 1 Navigate to **CONSOLE | Events > Severity**.
- 2 Do one of the following:
  - To re-order existing severities with the new sequence numbers that you entered, entering a new severity sequence number in the **Sequence** field of each item and click **Update**.
  - To add a new severity level, scroll to the bottom of the list and click **Add Severity**.
- 3 In the **Add Severity** dialog box, type a name for the new severity level in the **Name** field.
- 4 Choose a color that you want to assign for this severity level by clicking on the color icon. You can see a preview of the color you selected in the **Preview** field.
- 5 Click **Update**.
- 6 In the **Severity** table, assign the level for the new severity you created by changing the numbering in the **Sequence** column.
- 7 Click **Update**.

## *To edit or delete a Severity:*

- 1 To edit a Severity, click the **Edit** icon.
- 2 Configure the Severity Settings, then click **Update**.
- 3 To delete a Severity, select the check box for the severity you wish to delete, then click **Update**. You can also click **Delete** in the Edit column, to delete a single report.

**i** | **NOTE:** Deleting a Severity that is in use is not permitted. A warning message displays when this action is performed.

# Threshold

In the **CONSOLE | Events > Threshold** screen, you can view existing event thresholds, enable or disable them, and configure their elements. A threshold defines the condition for which an event is triggered. Predefined thresholds have names similar to predefined Alert Types. Each threshold can contain one or more threshold elements. An element consists of an Operator, a Value, a Description, and a Severity.

## **Topics:**

- [Searching Thresholds](#)
- [Adding a Custom Threshold](#)



- [Adding a Threshold Element](#)
- [Editing a Threshold](#)
- [Editing a Threshold Element](#)
- [Enabling/Disabling Thresholds and Threshold Elements](#)
- [Deleting Thresholds and Threshold Elements](#)

## Searching Thresholds

Use the search options at the top of the **Thresholds** table to search for a specific threshold.

- 1 In the first field, select **Name**.
- 2 In the second field, select **Equals**, **Starts with**, **Ends with**, or **Contains** based on your search string.
- 3 In the third field, enter the text string to search.
- 4 Click **Search**.
- 5 To clear the Search filter, click **Clear**.

## Adding a Custom Threshold

*To add a custom threshold:*

- 1 Navigate to **CONSOLE | Events > Threshold**.
- 2 Scroll to the bottom of the list and click **Add Threshold**.
- 3 In the **Add Threshold** window, type a name for the threshold value in the **Name** field.
- 4 Select **Visible to Non-Administrators** if you want the threshold to be visible to non-administrators. If enabled, anyone can view the threshold elements and use the threshold in customized reports.

**i** **NOTE:** If **Visible to Non-Administrators** is unchecked, only users from the Administrator group or the threshold creator is able to view, use, edit, and delete the threshold. Whether this is selected or not, only the users from the Administrator group and the threshold creator is able to edit or delete this object.

- 5 Click **Update**.

## Adding a Threshold Element

Elements are components of a threshold. You must define a threshold by defining its elements.

*To add a threshold element to the threshold:*

- 1 Click the **+** icon in the **Configure** column of the **CONSOLE | Events > Threshold** page.
- 2 In the **Operator** drop-down list, select the logical operator from the list of operators.
- 3 In the **Value** field, enter a value.
- 4 In the **Description** field, enter a description to override the auto-generated description.
- 5 In the **Severity** field, select a severity category.

- 6 Select **Disable** if you want to disable the threshold. This allows you to temporarily disable the threshold without deleting it.
- 7 Click **Update**.


## Editing a Threshold

### *To edit your custom or existing threshold:*

- 1 Navigate to **CONSOLE | Events > Threshold** and click the **Edit** icon in the **Configure** column.
- 2 Make the changes needed for the Threshold.
- 3 Click **Update**.

## Editing a Threshold Element

### *To edit an existing element of a Threshold:*

- 1 Navigate to **CONSOLE | Events > Threshold** and click the **Edit** icon located in the **Configure** column in the element row.  
  
 **NOTE:** Some alerts created by certain Alert Types contain predefined Thresholds that you may not be able to edit.
- 2 In the **Operator** field, from the drop-down list select the logical operator to apply to your threshold element.
- 3 In the **Value** field, enter the value for your threshold element.
- 4 In the **Description** field, enter the description for your threshold element.
- 5 In the **Severity** field, select the severity priority from the drop-down menu. These are color coded for your easy reference on the **CONSOLE | Events > Threshold** page.
- 6 To disable the threshold element, check the **Disable** box. That allows you to temporarily disable the threshold without deleting it.
- 7 Click **Update**.

## Enabling/Disabling Thresholds and Threshold Elements

The **Events** feature provides a **Disable** check box that allows you to disable or enable thresholds or individual elements within that threshold. Disabling an element or threshold rather than deleting it allows you to keep it in your list. If it is needed again, you can simply enable it.

You can disable a threshold by disabling all its elements. You can also disable individual elements within a threshold.

### *To enable or disable Thresholds and/or their elements:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Events > Threshold**. You have the following two options for the enabling/disabling feature:
  - You can enable or disable a Threshold by disabling/enabling all the elements that exist within it.


- You can enable/disable the individual elements within a Threshold.
- 2 Click the **Edit** icon that is on the same line as the element you want to enable or disable.
  - 3 Check the box next to **Disable** to disable the element or clear the box to enable the element.
  - 4 Click **Update**.

## Deleting Thresholds and Threshold Elements

On the **CONSOLE | Events > Threshold** screen, you can delete Thresholds and Threshold Elements. This can be done by using **Delete Threshold(s)/Element(s)**. To view the elements within a threshold, expand the threshold. You can select which threshold or elements within that threshold to delete. If you delete a threshold, the elements within that threshold are automatically deleted as well.

### *To delete thresholds and threshold elements:*

- 1 On the **CONSOLE | SYSTEM SETUP > Events > Threshold** screen, expand the threshold to view the individual elements, if needed.
- 2 To delete the Threshold, check the box to the left of the threshold name. Its elements are automatically selected as well.
- 3 To delete an element, select only the element check box.

 **NOTE:** Deleting a Threshold that is in use is not permitted. A warning message displays when this action is performed.

- 4 When you have finished with your selections, click **Delete Threshold(s)/Element(s)** at the bottom of the table.

## Alert Settings

The **CONSOLE | SYSTEM SETUP > Events > Alert Settings** window provides predefined alerts that apply to all of Management services. These are status type alerts and do not use thresholds. Hover your mouse over the **Information** icon to display information about them. You can configure the predefined alerts to use different destinations and schedules.

### Topics:

- [Searching Alert Settings](#)
- [Adding an Alert](#)
- [Enabling/Disabling an Alert](#)
- [Deleting Alerts](#)
- [Deleting Alerts](#)

## Searching Alert Settings

Use the search options at the top of the **Alerts** table to search for a specific alert.


- 1 In the first field, select **Name** or **Alert Type**.
- 2 In the second field, select a logical condition based on what alerts you want to search.

- 3 In the third field, enter the text string to search.
- 4 Click **Search**.
- 5 To clear the Search filter, click on **Clear**.

## Adding an Alert

### *To add an alert:*

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Events > Alert Settings**.
- 2 Click **Add Alert** at the bottom of the table.
- 3 Enter a **Name**.
- 4 Add a **Description** for your alert.
- 5 Enable **Visible to Non-Administrators** if you want your alert to be visible to non-administrators.
- 6 Check **Disable** if you want to disable this alert.
- 7 Enter a **Polling Interval** value.
- 8 To configure an Alert Type:
  - a Select the **Alert Type** from the drop-down list.

 **NOTE:** When an alert type is selected, a description for that alert is displayed in the Alert Type panel.
  - b Click **Update**. To reset the settings, click **Reset**.
- 9 Click the **Add Destination** link under the Destination/Schedule section. You can designate up to five destinations where you want alerts to be sent.
- 10 Click the **DESTINATION** drop-down list, then select the type of destination.
- 11 Select one of the schedules from the **SCHEDULE** drop-down list to set the frequency of alerts to be sent to the destination(s).
- 12 Click **Update** to finish adding an alert.


## Enabling/Disabling an Alert

- 1 Navigate to **CONSOLE | SYSTEM SETUP > Events > Alert Settings**.
- 2 Check or uncheck the **ENABLED** box next to the alert(s) you wish to enable.
- 3 Click the **Enable/Disable Alert(s)** button.
- 4 Click **OK**.

# Deleting Alerts

## *To delete an alert:*

- 1 Check the boxes next to the alerts you wish to delete.
- 2 Click **Delete Alert(s)**.
- 3 Click **OK**.

 **NOTE:** You can also delete an alert by clicking the Delete icon under the Configure section of the alert you wish to delete.

# Editing Alerts

After an alert is created, you can go back and edit it at any time. Click the **Configure** icon next to the alert you wish to edit and follow the same process described in [Adding an Alert](#) to edit your existing alert.

# Current Alerts

You can view the list of current alerts on the **CONSOLE | SYSTEM SETUP > Events > Current Alerts** page. The list shows you the severity level and a shorty description about the current alerts.

# Help

To access the online help, click the **Help** button in the top-right corner of the user interface. The online help provides context-sensitive conceptual overviews, configuration examples, and troubleshooting tips.

## Topics:

- [About Management Services](#)
- [Tips and Tutorials](#)

## About Management Services

The **CONSOLE | HELP > Help > About** page displays the version of Management services being run, who the service is licensed to, database information, and the End User License Agreement (EULA).

To access the online help, click the **Help** icon in the top-right corner of the user interface.

## Tips and Tutorials

The Tips and Tutorials resource is not available for this release.

# SonicWall Support

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

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

# About This Document

## Legend



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



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



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

Capture Security Center Administration  
Updated - February 2020  
Software Version - 1.7  
232-004724-01 Rev A

## Copyright © 2020 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>.

## Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
SonicWall Inc. Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035