SonicWall® Global Management System 8.7 Console

Administration

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. Select the language based on your geographic location to see the EUPA that applies to your region.

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

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.

SonicWall GMS Console Administration
Updated — January 2019
Software Version — 8.7
232-004603-00 Rev A

Contents

Part 1. CONSOLE

Part 2. Console

Section

CONSOLE

- Console

Part 1

Console

1

Configuring Workflow and Change Management

This chapter describes how to configure Workflow in the **CONSOLE | Workflow** page. With Workflow enabled, any configuration or policy changes made to GMS 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 provides for scheduling changes to be processed or executed and allows for creating approval groups - the members of which being authorized to approve the changes.

The Workflow feature (Enable or Disable) is available at the granular level for each individual domain. The feature can be enabled or disabled on a per domain basis.

Topics:

- Introduction to Workflow and Change Management on page 8
- Settings on page 8
- Approval Groups on page 9
- The Compare Change Orders option shows the difference between two change orders. on page 14

Introduction to Workflow and Change Management

To begin, navigate to **CONSOLE | Workflow > Settings > Approval Groups** and start by defining the members of the various policy Approval Groups (see Approval Groups in the sections that follow). These members have the final word on whether a proposed change order is approved or denied. You can create Approval Groups for each module, 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. By default, until defined, the approval group.

After your Approval Groups have been established for each module, you can manage change orders for approving, scheduling, and executing (or processing) proposed changes through Change Order Management (see Change order management in the sections that follow).

Settings

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

Topics:

Enabling Workflow

To configure the Workflow settings, complete the following steps:

1. Navigate to **CONSOLE | Workflow > Settings**. The Settings page displays.
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.

Configuring Change Order Default Schedule Settings

To configure a regular schedule to manage change orders, complete the following steps:

1. Click the radio button next to the desired instance you would like change orders to go into effect. Choose between **Execute Manually**, **Immediate on Approval**, or **At** to change at a time you select from the pull-down menu.
2. Click **Update** to accept the changes you have made.

Deleting GMS Change Order Data

You can manually 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 GMS Change Order Data, complete the following steps:

1. Navigate to **CONSOLE | Workflow > Settings**. The Settings page displays.
2. In the **Delete GMS Change Order Data** section, choose a date older than two years at which point to delete the outdated Change Orders.
3. Select the Domain from which to delete the Change Orders.
4. Click **Update** to accept the changes you have made.

Approval Groups

The following sections detail the requirements of GMS transitioning to one of the states mentioned previously:

On the **CONSOLE |Workflow > Approval Groups** page, you can search for specific approval groups, add, modify, or delete approval groups, or select a default approval group.

Features of the Approval Groups section include:

You can delete all the group users from a Custom Approval group but not from the “Default Approval Group.” The “Default Approval Group” should have at least one who can provide approvals.

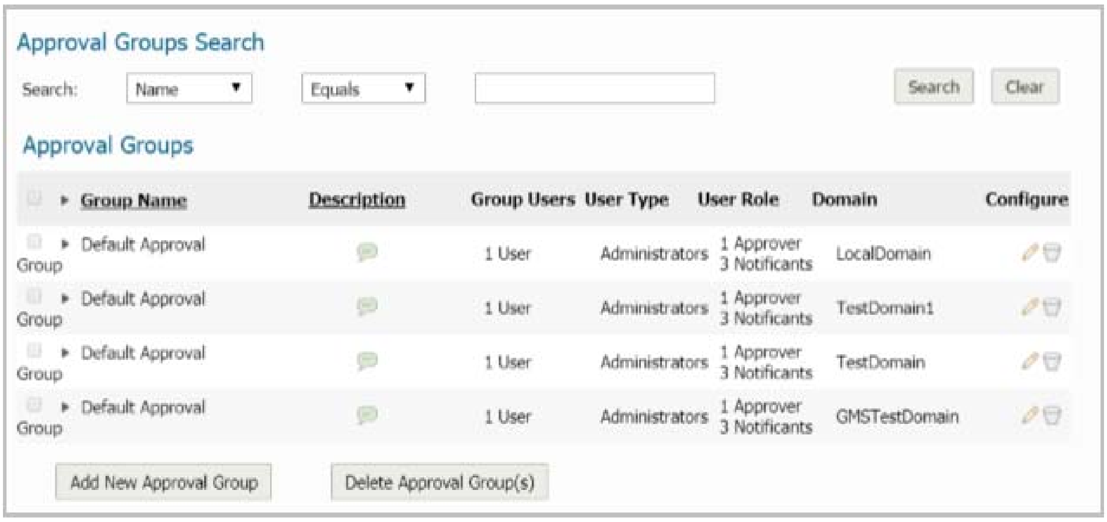
Topics:

- Approval Groups Search on page 10
- Configuring Approval Groups on page 10
- Default Approval Group for Each Module on page 12

Approval Groups Search

To search for specific approval groups, complete the following steps:

1 Navigate to **CONSOLE | Workflow > Approval Groups.** The Approval Groups page appears.



Approval Groups Search

Search: Name ▼ Equals ▼ Search Clear

Approval Groups

□	Group Name	Description	Group Users	User Type	User Role	Domain	Configure
□	Default Approval Group		1 User	Administrators	1 Approver 3 Notificants	LocalDomain	
□	Default Approval Group		1 User	Administrators	1 Approver 3 Notificants	TestDomain1	
□	Default Approval Group		1 User	Administrators	1 Approver 3 Notificants	TestDomain	
□	Default Approval Group		1 User	Administrators	1 Approver 3 Notificants	GMSTestDomain	

2 Use the Search drop-down menu to search for a specific Approval Group Name or Description.

3 Select **Equals**, **Starts with**, **Ends with**, or **Contains** from the drop-down menu.

4 Enter the Search terms in the box and click **Search**.

Configuring Approval Groups

The **Add New/Edit Approval Group** screen allows you to select users as Approvers. You can remove added approvers from the approval group. The GMS users are listed from the users table.

To Add an Approval Group, complete the following steps:

1 Navigate to **CONSOLE | Workflow > Approval Groups**. The Approval Groups page appears.

2 Click **Add New Approval Group**. The Add New Approval page appears.

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. Options include the LocalDomain or a TestDomain.

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 (DAG)” is the default approval group applicable to the different modules. The DAG cannot be deleted, it can only be edited and new users can be added as approvers or Notification users and existing users can be deleted.

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

5. Enter a short description in the **Description** field.
6. Click **Add New User**. This adds additional approvers and their roles to the Approval Group. Options include: Administrators and End-Users.
7. Click **Add Additional User** to include more users that you would like to receive notifications on approvals and other actions performed by the approvers and any changes in the state of a Change Order that would be associated with this group.
   - If a user-created approval group that is already associated with a change order pending approval is deleted from the system, the default approval group applicable for that screen to which the change order belongs applies. The Delete confirmation screen clearly explains that the Approval Group being deleted is currently associated with one or more unapproved change orders and that on deletion of the approval group, the system associates the Default Approval Group for that module with those change orders to which the change orders belong.
   - The Approval Groups page has a section where the default approval group for each module can be selected. By default, the ‘Default Approval Group (DAG)’ is the default approval group for each module. You can also set a Custom Approval Group as the default for any module.
   - You can also create a custom approval group with no approvers in it. There could be none or more ‘Notification’ users. However, a warning/confirmation message is shown to confirm the creation of an approval group that has no approvers or users in it.
8. Click **OK**.

To Edit an Approval Group, complete the following steps:

1. Navigate to **CONSOLE | Workflow > Approval Groups**.
2. Click the **Edit** icon next to the Group Name that you would like to edit. The Edit Approval Group page appears.
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. Options include the LocalDomain or a TestDomain.

   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 (DAG)” is the default approval group applicable to the different modules. The DAG cannot be deleted, it can only be edited and new users can be added as approvers or Notification users and existing users can be deleted.

   Each domain admin user is able to view the Approval Groups only for that domain. Only the super admin (admin@LocalDomain) can view all the Approval Groups for all domains. The super admin can see an additional column that reveals the domain names.
5. Enter a short description in the **Description** field.
6. Click **Add New User**. This adds additional approvers and their roles to the Approval Group. Options include: Administrators and End-Users.
7. Click **Add Additional User** to include more users that you would like to receive notifications on approvals and other actions performed by the approvers and any changes in the state of a Change Order that would be associated with this group.
   - If a user-created approval group that is already associated with a change order pending approval is deleted from the system, the default approval group applicable for that screen to which the

change order belongs applies. The Delete confirmation screen clearly explains that the Approval Group being deleted is currently associated with one or more unapproved change orders and that on deletion of the approval group, the system associates the Default Approval Group for that module with those change orders to which the change orders belong.

- The Approval Groups page has a section where the default approval group for each module can be selected. By default, the 'Default Approval Group (DAG)' is the default approval group for each module. You can also set a Custom Approval Group as the default for any module.
- You can also create a custom approval group with no approvers in it. There could be none or more 'Notification' users. However, a warning/confirmation message is shown to confirm the creation of an approval group that has no approvers or users in it.

8 Click **OK**.

Default Approval Group for Each Module

To set the default approval group for each module, complete the following steps:

1 Navigate to **CONSOLE | Workflow > Approval Groups**. The Approval Groups page appears.

2 In the Default Approval Group for Each Module section, select the domain under the jurisdiction of this Approval Group from the drop-down menu to view the corresponding Default Approval Group. Options include the LocalDomain or a TestDomain.

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 (DAG)" is the default approval group applicable to the different modules. The DAG cannot be deleted, it can only be edited and new users can be added as approvers or Notification users and existing users can be deleted.

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

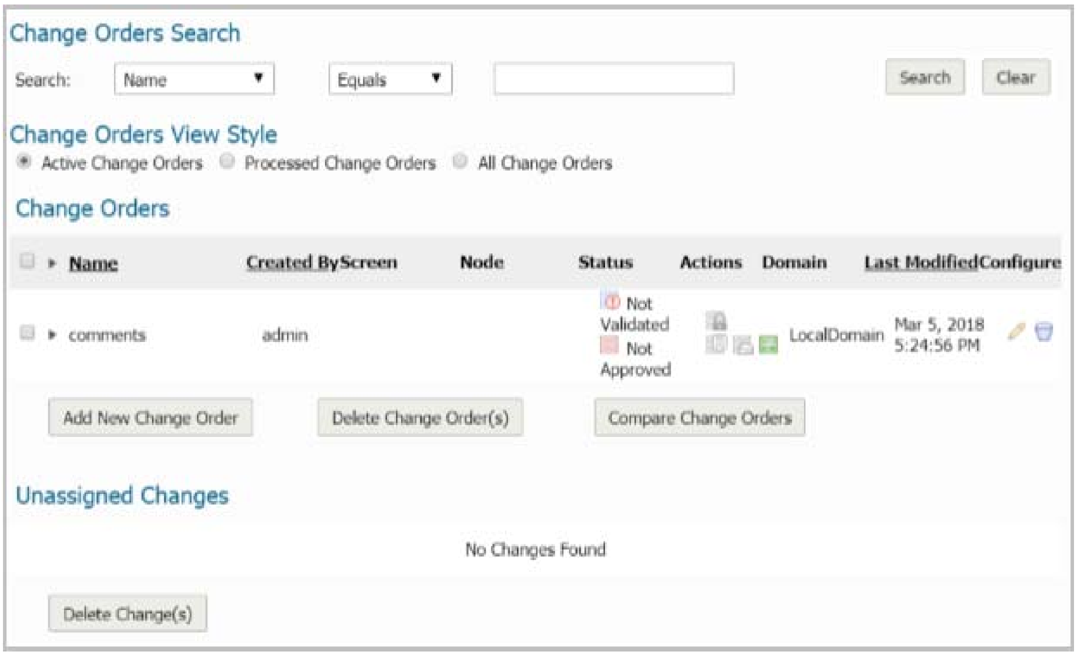
3 Click **Update**.

Change Orders

Topics:

- Change Audit Report
- Change Compliance Report

You can add changes on any screen to create a change order. The changes can be added to existing change orders or you can create new change orders on the fly. On the **CONSOLE | Workflow > Change Orders** page, you can add, edit, and delete change orders.



Change Orders Search

Search: Name ▾ Equals ▾ Search Clear

Change Orders View Style

● Active Change Orders ○ Processed Change Orders ○ All Change Orders

Change Orders

□	Name	Created By	Screen	Node	Status	Actions	Domain	Last Modified	Configure
□	comments	admin			Not Validated Not Approved		LocalDomain	Mar 5, 2018 5:24:56 PM	

Add New Change Order | Delete Change Order(s) | Compare Change Orders

Unassigned Changes

No Changes Found

Delete Change(s)

A change order should have at least one Approval Group associated with it. The approvers in that approval group would approve the change order.

You can configure a schedule for processing or executing change orders after their approval and then create tasks for the target appliances.

Change orders can also be scheduled at the Default, or with one of three options: a) Execute Manually b) Immediate on Approval c) On a given schedule. “At.” When change orders are executed manually, click **Execute Manually** under Schedule for the change order. The Execute option is enabled only after the change order has been fully approved. The change order reaches the fully approved state after it is accepted by all the members of the approval group associated with the change order.

When a change order is scheduled to execute **Immediate on Approval**, the change order is directly picked up for processing, task creation, or execution after the change order has reached the fully approved state.

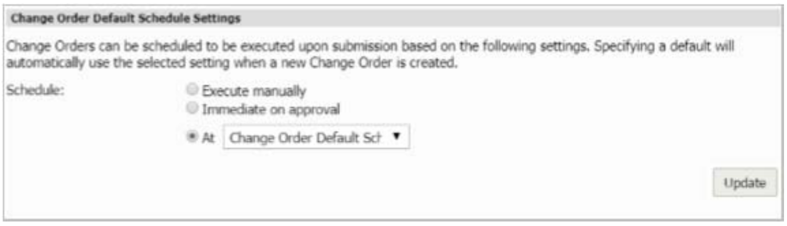
When a change order is scheduled on a particular schedule, it is picked up for processing, task creation, or execution as soon as the schedule is met, provided the change order has reached the fully approved state at that point. If a change order has not been fully approved before the schedule is met or it has lapsed, the change order cannot be implemented. The change order has to be reopened and then resubmitted with a new schedule. However, if the change order has been scheduled on a recurring schedule, it will get picked up for processing at the next scheduled occurrence only after the change order has reached the fully approved state.

Select any one of the three scheduling options as a default selection on the **CONSOLE | Workflow > Settings** screen.

You can view changes made to any change order. The view functionality shows the change objects on a per screen basis.

To schedule approvals at a specific time, complete the following steps:

1 Navigate to **CONSOLE | Workflow > Settings**. In the Change Order Default Schedule Settings section, click the radio button for **At** and select a schedule from the pull-down.



Change Order Default Schedule Settings

Change Orders can be scheduled to be executed upon submission based on the following settings. Specifying a default will automatically use the selected setting when a new Change Order is created.

Schedule: ○ Execute manually
○ Immediate on approval
● At Change Order Default Sch ▼

2 Click **Update**.

You can also preview a change order. The preview functionality shows a preview of the changes to be applied to the Running Configuration after a change order is selected on the screen.

The Compare Change Orders option shows the difference between two change orders.

Change Audit Report

Information about changes has been consolidated so that you can more easily verify that change orders were successfully implemented. Rather than having to analyze data on the Change Orders screen, Scheduled Tasks, and Logs, a single report now tracks the changes submitted and can report on the status for a specified time period. This also meets the requirements of an audit report.

This new Audit Report can be generated on an on-demand basis, or it can be scheduled and delivered to the administrator in a PDF format. The report contains the details of the changes pushed to the unit during a time period, whether the changes took effect on the units, whether there were errors or warnings, and if the task would be re-attempted.

To run a Change Audit Report:

1 Navigate to **CONSOLE > Workflow > Change Orders**.

2 Go to the bottom of the page to specify the **Date Range**.

3 Select **Generate Audit Report**.

A pdf is generated and sent to the administrator of the domain.

Change Compliance Report

The Change Compliance Report contains the details about changes pushed to the units. It tells whether the changes took affect, whether errors or warnings occurred, and if they did, whether the task would be re-attempted. This report can be scheduled or requested on-demand and is delivered in PDF form.

To run a Compliance Report:

1 Navigate to **CONSOLE | Workflow > Change Orders**.

2 Select the change orders that you want status for (at a single or multiple change order level).

3 Go to the bottom of the page to specify the **Date Range**.

4 Select **Generate Change Compliance Report**.

A pdf is generated and sent to the administrator of the domain.

2

Managing Scheduled Tasks

This chapter describes how to configure scheduled tasks and default tasks in the **CONSOLE | Tasks** page.

Topics:

- Default Tasks on page 15
- Scheduled Tasks on page 18

Default Tasks

The Defaults Tasks page allows the Super Administrator to configure the default tasks that are executed when adding new units or on existing units in the GMS deployment. These tasks can also be manually executed on existing units on-demand.

Deployment Considerations

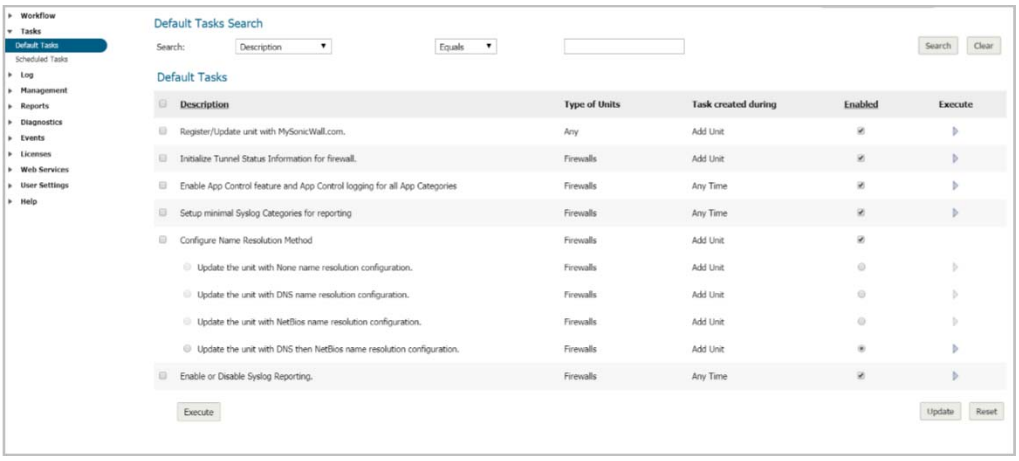
Consider the following before managing the default tasks:

- Upgrading from older versions of GMS to GMS 8.0 migrates all the existing units according to the selected default tasks.
- Enable the desired Name Resolution Method to match your current GMS setup.

Managing the Default Tasks

To view and manage default tasks, complete the following steps:

1 Navigate to **CONSOLE | Tasks > Default Tasks**. The Default Tasks page displays.



Default Tasks Search

Search: Description ▾ Equals ▾

Default Tasks

□	Description	Type of Units	Task created during	Enabled	Execute
□	Register/Update unit with MySonicWall.com.	Any	Add Unit	☑	▷
□	Initialize Tunnel Status Information for firewall.	Firewalls	Add Unit	☑	▷
□	Enable App Control feature and App Control logging for all App Categories	Firewalls	Any Time	☑	▷
□	Setup minimal Syslog Categories for reporting	Firewalls	Any Time	☑	▷
□	Configure Name Resolution Method	Firewalls	Add Unit	☑	
	○ Update the unit with None name resolution configuration.	Firewalls	Add Unit	○	▷
	○ Update the unit with DNS name resolution configuration.	Firewalls	Add Unit	○	▷
	○ Update the unit with NetBios name resolution configuration.	Firewalls	Add Unit	○	▷
	○ Update the unit with DNS then NetBios name resolution configuration.	Firewalls	Add Unit	●	▷
□	Enable or Disable Syslog Reporting.	Firewalls	Any Time	☑	▷

2 Search for tasks by using the **Default Tasks Search** section. Select search criteria from the following:

- Description
    - Equals
    - Starts with
    - Ends with
    - Contains
- Type of Units
    - Firewalls
    - SMAs
    - Aventail SMAs
    - ESs
- Task created during
    - Any Time
    - Add Unit
- Enabled
    - Yes
    - No

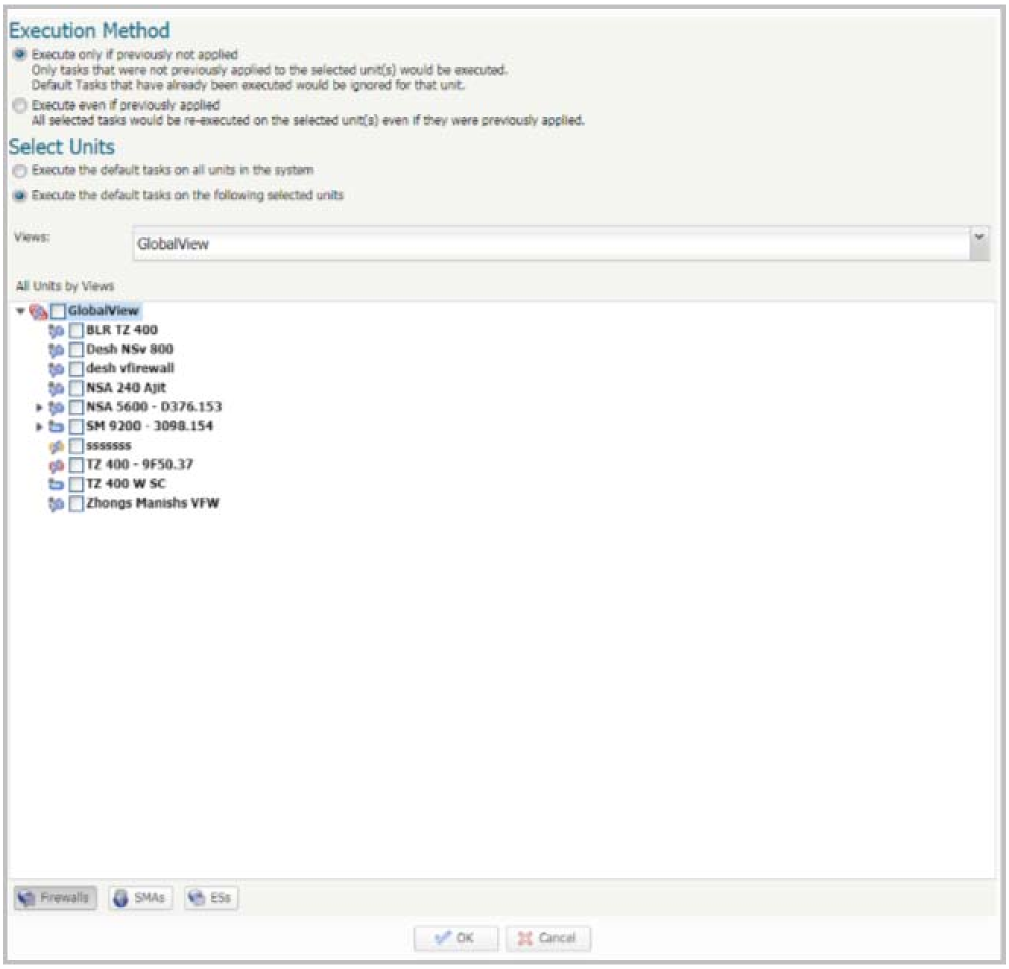
3 Select the desired default tasks from the **Default Tasks** list, or click the **check box** at the top of the list to select all the tasks.

> ⓘ **NOTE:** Certain tasks are grouped under one task, and only one of the sub-tasks can be selected from within this category. If the category is disabled, sub-tasks are all disabled as well.

4 Enable or disable configured tasks by selecting/deselecting the check boxes in the **Enable** column. Click **Update** after your changes are made.

5 To execute the selected tasks for the chosen units, click the **Arrow** icon in the **Execute** column. Or click the **Execute** link at the bottom of the page to configure multiple selected tasks.

The Select Units pop-up window displays.



Execution Method

● Execute only if previously not applied
Only tasks that were not previously applied to the selected unit(s) would be executed.
Default Tasks that have already been executed would be ignored for that unit.

○ Execute even if previously applied
All selected tasks would be re-executed on the selected unit(s) even if they were previously applied.

Select Units

○ Execute the default tasks on all units in the system

● Execute the default tasks on the following selected units

Views: GlobalView

All Units by Views

- □ GlobalView
  - □ BLR TZ 400
  - □ Desh NSv 800
  - □ desh vfirewall
  - □ NSA 240 Ajit
  - □ NSA 5600 - D376.153
  - □ SM 9200 - 3098.154
  - □ sssssss
  - □ TZ 400 - 9F50.37
  - □ TZ 400 W SC
  - □ Zhongs Manishs VFW

6 Click **Execute only if previously not applied** or **Execute even if previously applied**.

The Execute method selects how you want to execute the tasks for the selected units. This is used to handle situations where a combination of tasks might or might not have run because of the state of the tasks selected after the units were added to the system. When a unit is added to the system, the default tasks are executed against the unit. Depending on the type of unit, firmware version, and the selected defaults at that point of time, some or all of tasks are executed. If a task did not run when a unit (considering the version, type, and so on) was added or at a later time after adding, the pending tasks are automatically applied when the unit properties change. It is also possible to complete a “force execute” on all units, regardless of whether or not they have been previously executed to ensure that the task changes the settings exactly as requested.

7 Click **Execute the default tasks on all units in the system** or **Execute the default tasks on the following selected units**.

Unit selection allows the user to pick either all units in the system or selective units from each of the appliance types supported.

Either way, the tasks selected are applied only on units that match the default tasks’ properties which are related to Model, Firmware Version, Appliance Type, and so on.

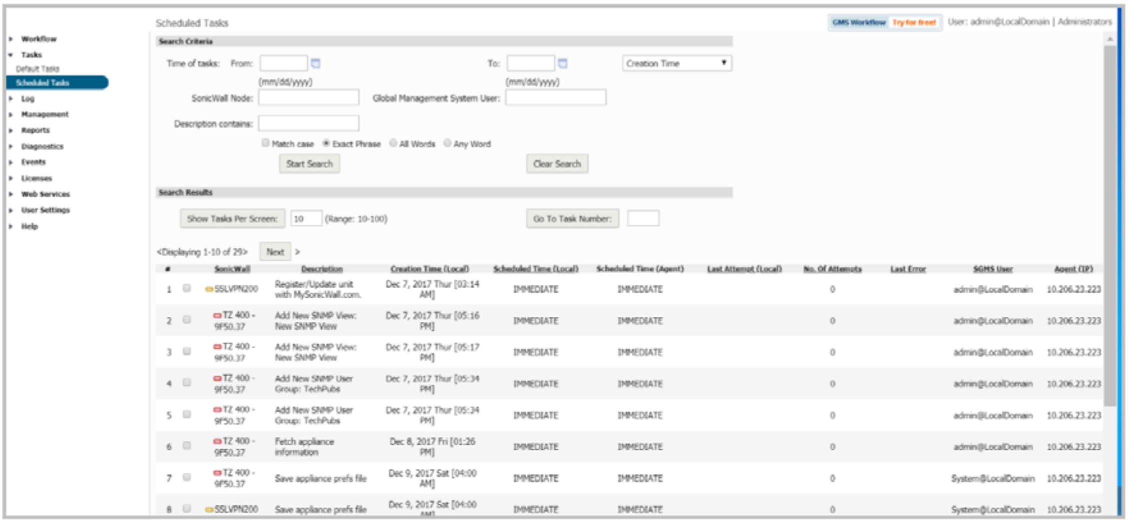
Tasks CANNOT be Edited or Deleted. The management interface only allows execution of selected tasks against the specified units.

Scheduled Tasks

As you complete multiple tasks through the GMS UI, GMS creates, queues, and applies them to the SonicWall appliances. As GMS processes tasks, some SonicWall appliances might be down or offline. When this occurs, GMS requeues the tasks and reattempts the changes.

To view and manage pending tasks, complete the following steps:

1 Navigate to **CONSOLE | Tasks > Scheduled Tasks**. The Scheduled Tasks page displays.



Scheduled Tasks

User: admin@LocalDomain | Administrators

Search Criteria

Time of tasks: From: (mm/dd/yyyy) To: (mm/dd/yyyy) Creation Time

SonicWall Node: Global Management System User:

Description contains:

□ Match case ● Exact Phrase ○ All Words ○ Any Word

Search Results

10 (Range: 10-100)

<Displaying 1-10 of 29>

#		SonicWall	Description	Creation Time (Local)	Scheduled Time (Local)	Scheduled Time (Agent)	Last Attempt (Local)	No. Of Attempts	Last Error	SGMS User	Agent (IP)
1	□	SSLVPN200	Register/Update unit with MySonicWall.com.	Dec 7, 2017 Thur [03:14 AM]	IMMEDIATE	IMMEDIATE		0		admin@LocalDomain	10.206.23.223
2	□	TZ 400 - 9F50.37	Add New SNMP View: New SNMP View	Dec 7, 2017 Thur [05:16 PM]	IMMEDIATE	IMMEDIATE		0		admin@LocalDomain	10.206.23.223
3	□	TZ 400 - 9F50.37	Add New SNMP View: New SNMP View	Dec 7, 2017 Thur [05:17 PM]	IMMEDIATE	IMMEDIATE		0		admin@LocalDomain	10.206.23.223
4	□	TZ 400 - 9F50.37	Add New SNMP User Group: TechPubs	Dec 7, 2017 Thur [05:34 PM]	IMMEDIATE	IMMEDIATE		0		admin@LocalDomain	10.206.23.223
5	□	TZ 400 - 9F50.37	Add New SNMP User Group: TechPubs	Dec 7, 2017 Thur [05:34 PM]	IMMEDIATE	IMMEDIATE		0		admin@LocalDomain	10.206.23.223
6	□	TZ 400 - 9F50.37	Fetch appliance information	Dec 8, 2017 Fri [01:26 PM]	IMMEDIATE	IMMEDIATE		0		admin@LocalDomain	10.206.23.223
7	□	TZ 400 - 9F50.37	Save appliance prefs file	Dec 9, 2017 Sat [04:00 AM]	IMMEDIATE	IMMEDIATE		0		System@LocalDomain	10.206.23.223
8	□	SSLVPN200	Save appliance prefs file	Dec 9, 2017 Sat [04:00 AM]	IMMEDIATE	IMMEDIATE		0		System@LocalDomain	10.206.23.223

2 Each task entry contains the following fields:

- **Number (#)**—specifies the number of the task entry.
- **SonicWall**—specifies the name of the SonicWall appliance to which the task applies.
- **Description**—contains a description of the task.
- **Creation Time**—specifies the date and time the task was generated.
- **Scheduled Time (Local)**—time the task was scheduled in the local time zone of the appliance.
- **Scheduled Time (Agent)—**time the task was scheduled in the time zone of the agent.
- **Last Attempt (Local)**—time the task was last attempted in the local time zone of the appliance.
- **No. of Attempts**—specifies the number of times GMS has attempted to execute the task.
- **Last Error**—if the task was not successfully executed, specifies the error.
- **SGMS User**—specifies the user who created the task.
- **Agent (IP)**—specifies the IP address of the agent. This column can accept/display IPv6 and IPv4 addresses.

3 To narrow the search, enter one or more of the following search criteria and click **Start Search**:

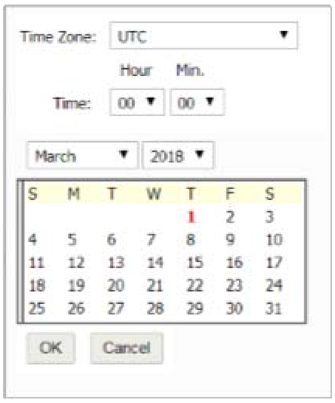
ⓘ | **TIP:** You can press Enter to navigate from one form element to the next in this section.

- **Calendar**—select the period of time for which GMS displays tasks. The pull down menu to the right enables you to specify that the date range applies to the task creation time, the local scheduled time, and the agent scheduled time.
- **SonicWall Node**—displays all tasks associated with the specified SonicWall appliance.
- **Description contains**—displays all tasks that contain the specified text.

- **Owner**—displays all tasks with the specified owner.
- **Task ID**—displays the task with the specified task ID.

4 To execute one or more scheduled tasks immediately, select their check boxes and click **Execute the tasks selected now**. You can also select all of the tasks on the page by checking **Select Only the 10 Tasks Displayed Above**, or select all tasks by checking **Select All Pending Tasks**.

5 To reschedule one or more pending tasks for another time, select their check boxes and click **Re-schedule the tasks selected**. The GMS Date Selector dialog box displays.



Time Zone: UTC

Time: Hour 00 Min. 00

March 2018

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

6 Select a new date when the task executes and click **OK**. The dialog box closes and the task executes at the selected time.

> **NOTE:** The task(s) executes based on the time setting of the SonicWall GMS agent server, UTC, or local browser's time.

7 To delete one or more tasks from the list of pending tasks, select their check boxes and click **Delete the tasks selected**. To delete all pending tasks, select **Select all Pending Tasks** and click **Delete the tasks selected**.

3

Configuring Log Settings

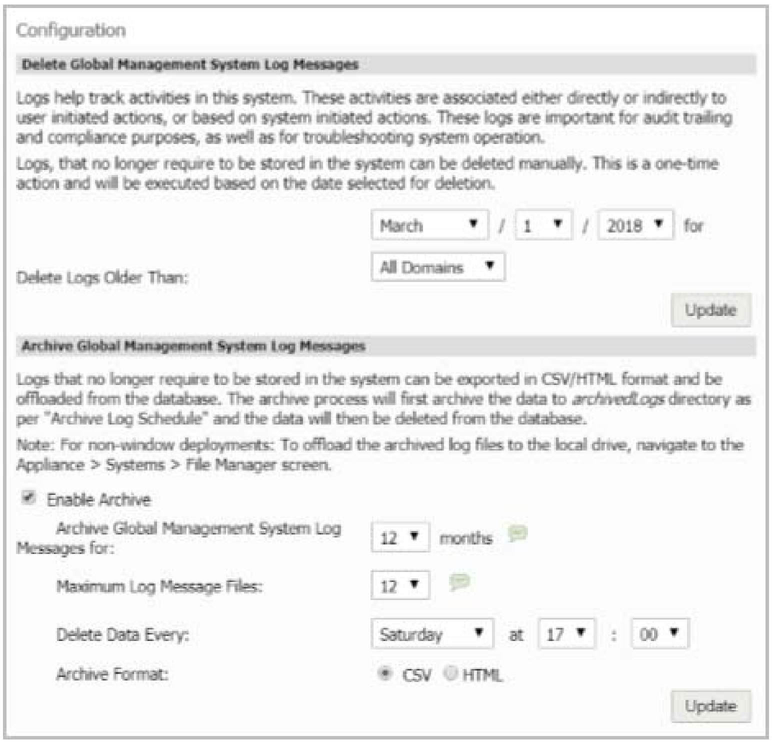
This chapter describes how to configure Log Settings. This includes adjusting settings on deleting log messages after a certain period of time, and setting criteria for viewing logs.

Topics:

Configuring Log Settings

In the **CONSOLE | Log > Configuration** screen, you can delete or archive GMS log messages. The Archive process archives the data to the “archivedLogs” directory as per the Archive Log Schedule, before the data is deleted from the database.

ⓘ **NOTE:** For UMH deployments, to offload the archived log files to a local drive, login to the /appliance management interface, then navigate to the **System > File Manager** page.



Configuration

Delete Global Management System Log Messages

Logs help track activities in this system. These activities are associated either directly or indirectly to user initiated actions, or based on system initiated actions. These logs are important for audit trailing and compliance purposes, as well as for troubleshooting system operation.

Logs, that no longer require to be stored in the system can be deleted manually. This is a one-time action and will be executed based on the date selected for deletion.

Delete Logs Older Than: March ▼ / 1 ▼ / 2018 ▼ for All Domains ▼

Update

Archive Global Management System Log Messages

Logs that no longer require to be stored in the system can be exported in CSV/HTML format and be offloaded from the database. The archive process will first archive the data to *archivedLogs* directory as per "Archive Log Schedule" and the data will then be deleted from the database.

Note: For non-window deployments: To offload the archived log files to the local drive, navigate to the Appliance > Systems > File Manager screen.

☑ Enable Archive

Archive Global Management System Log Messages for: 12 ▼ months

Maximum Log Message Files: 12 ▼

Delete Data Every: Saturday ▼ at 17 ▼ : 00 ▼

Archive Format: ● CSV ○ HTML

Update

To configure Log settings, select between the following options:

- **Delete Log Messages Older Than** — Select the month, day, year, and domain, and then click the **Update** link.

- **Enable Archive** — Select this check box to enable GMS log message archiving.
- **Archive GMS Log Messages for** — Select the number of months to archive log messages.
- **Maximum Log Message Files** — Select the maximum number of monthly archive files kept in the archivedLogs folder.
- **Delete Data Every** — Select a reoccurring day and time to delete data.
- **Archive Format** — Select the type of format to archive the GMS log messages. Choose between CSV or HTML.
- **Update** — Click **Update** after your settings are selected.

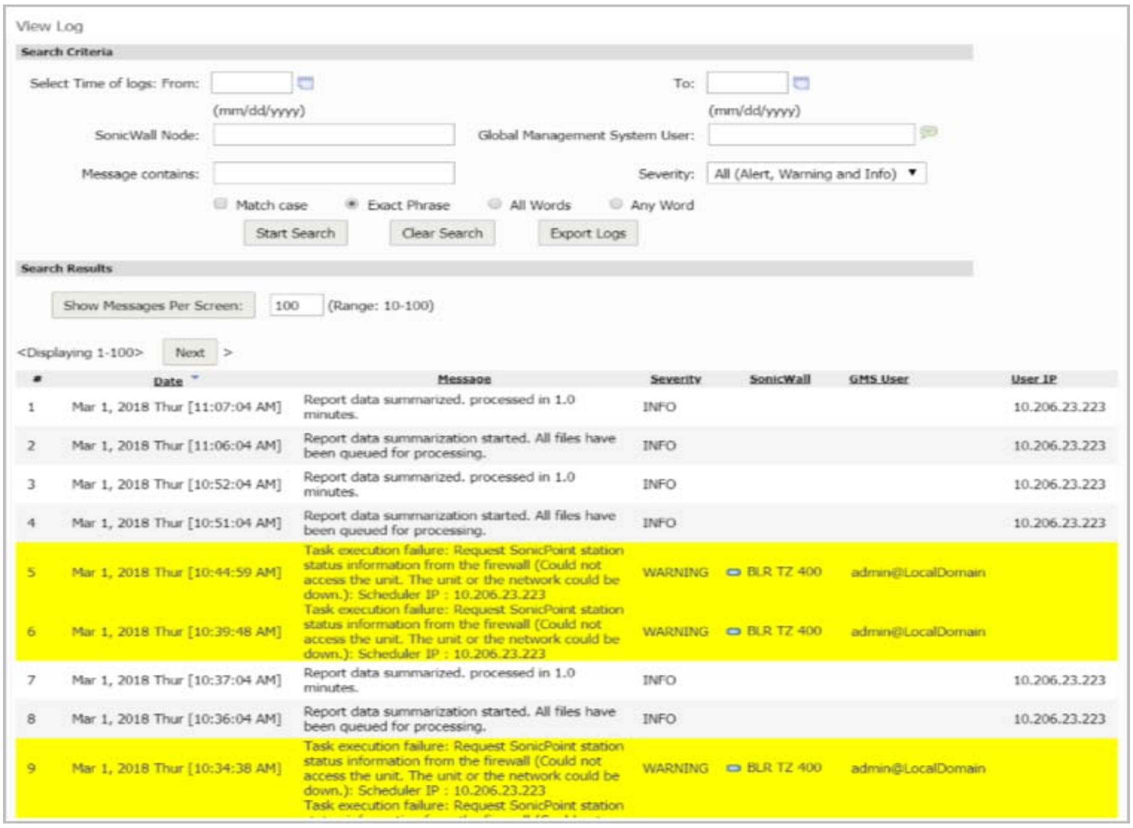
  ⓘ **NOTE:** The archive process first archives the data to the archivedLogs directory as per “Archive Log Schedule” and then the data is deleted from the database.

Configuring View Log Search Criteria

The GMS log keeps track of changes made within the GMS UI, 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 GMS log, complete the following steps:

1 Navigate to **CONSOLE | Log** > **View Log**. The View Log page displays.



View Log

Search Criteria

Select Time of logs: From: (mm/dd/yyyy) To: (mm/dd/yyyy)

SonicWall Node:

Global Management System User:

Message contains:

Severity: All (Alert, Warning and Info) ▼

☐ Match case ● Exact Phrase ○ All Words ○ Any Word

Start Search Clear Search Export Logs

Search Results

Show Messages Per Screen: 100 (Range: 10-100)

<Displaying 1-100> Next >

#	Date	Message	Severity	SonicWall	GMS User	User IP
1	Mar 1, 2018 Thur [11:07:04 AM]	Report data summarized. processed in 1.0 minutes.	INFO			10.206.23.223
2	Mar 1, 2018 Thur [11:06:04 AM]	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.223
3	Mar 1, 2018 Thur [10:52:04 AM]	Report data summarized. processed in 1.0 minutes.	INFO			10.206.23.223
4	Mar 1, 2018 Thur [10:51:04 AM]	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.223
5	Mar 1, 2018 Thur [10:44:59 AM]	Task execution failure: Request SonicPoint station status information from the firewall (Could not access the unit. The unit or the network could be down.): Scheduler IP : 10.206.23.223	WARNING	BLR TZ 400	admin@LocalDomain	
6	Mar 1, 2018 Thur [10:39:48 AM]	Task execution failure: Request SonicPoint station status information from the firewall (Could not access the unit. The unit or the network could be down.): Scheduler IP : 10.206.23.223	WARNING	BLR TZ 400	admin@LocalDomain	
7	Mar 1, 2018 Thur [10:37:04 AM]	Report data summarized. processed in 1.0 minutes.	INFO			10.206.23.223
8	Mar 1, 2018 Thur [10:36:04 AM]	Report data summarization started. All files have been queued for processing.	INFO			10.206.23.223
9	Mar 1, 2018 Thur [10:34:38 AM]	Task execution failure: Request SonicPoint station status information from the firewall (Could not access the unit. The unit or the network could be down.): Scheduler IP : 10.206.23.223	WARNING	BLR TZ 400	admin@LocalDomain	
		Task execution failure: Request SonicPoint station				

2 Each log entry contains the following fields:

- **#**—specifies the number of the log entry.
- **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).
- **User IP**—specifies the user name and IP address.

3 To narrow the search, configure some of the following criteria:

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

- **Select Time of logs**—displays all log entries for a specified range of dates.
- **SonicWall Node**—displays all log entries associated with the specified SonicWall appliance.
- **GMS User**—displays all log entries with the specified user.
- **Message contains**—displays all log entries that contain the specified text. This input field provides an auto-suggest functionality that uses existing log message text to predict what you want to type. It fills in the field with the suggested text and you can either press **Tab** to accept it or keep typing. Different suggestions appear as you continue to type if log messages match your input.
- **Severity**—displays log entries with the matching severity level:
  - **All (Alert, Warning, and Info)**
  - **Alert and Warning**
  - **Alert**
- Select **Match case** to make the **SonicWall Node**, **GMS User**, and **Message contains** search fields case sensitive.
- Select one of **Exact Phrase**, **All Words**, or **Any Word**.
  - **Exact Phrase** matches a log entry that contains exactly what you typed in the **Message contains** field
  - **All Words** matches a log entry that contains all the words you typed in the **Message contains** field, but the words can be non-consecutive or in any order
  - **Any Word** matches a log entry that contains any of the words you typed in the **Message contains** field

4 To view the results of your search criteria, click **Start Search.** To clear all values from the input fields and start over, click **Clear Search.** To save the results as an HTML file on your system, click **Export Logs** and follow the on-screen instructions.

5 To configure how many messages are shown per screen, enter a new value between 10 and 100 in the **Show Messages Per Screen** field. (default: 10). Click **Next** to display the next page, or click **Previous** to display the preceding page.

4

Configuring Zero Touch

This chapter shows how GMS integrates with the Zero Touch. GMS has automated the process of acquiring and configuring your firewalls with the Zero Touch feature as well as providing the mechanism to manage your firewalls with “zero” touch when you are setting it up for management. Simply put, the unit need only be plugged in for power and connected to the Internet for this feature to operate. Beyond that, the firewall, GMS, and other entities within the eco-system, function together to bring the unit under management.

Topics:

- Provisioning and Configuration
- DHCP/Auto IP Assignment
- Configuring Zero Touch with GMS

Provisioning and Configuration

You are also able to optionally choose to pre-configure your unit before it is even delivered. This feature requires the following changes in GMS:

- After GMS discovers the new unit and automatically adds it using data from MySonicWall, you are able to make group level configuration changes in GMS. The group already has the default configuration present depending on the firmware version of the unit.
- After the unit is online and acquired by GMS, you are able to push all configuration changes that were made using the Inheritance feature of GMS.

The unit can then be ready for use (with all the required configuration) within a few minutes of being plugged in.

DHCP/Auto IP Assignment

Configure a WAN IP for your device before connecting it to the Internet or any SonicWall services including MySonicWall, License Manager, and GMS.

As part of Zero Touch Management, automatic assignment of the WAN IP using DHCP is also possible. You need only to plug in the device to both a LAN and WAN and the IP assignment automatically takes place.

Configuring Zero Touch with GMS

Depending on the type of setup you intend to establish with Zero Touch, whether an All-In-One (AIO) or Distributed deployment, your work environment must meet particular requirements.

To install and configure GMS with Zero Touch, complete the following steps.

1 Download GMS from MySonicWall and complete the installation for a virtual environment. Refer to the following matrix for deployment requirements:

Features	Deployment Mode
ConnectWise Integration	AIO or Distributed
Zero Touch	AIO or Distributed

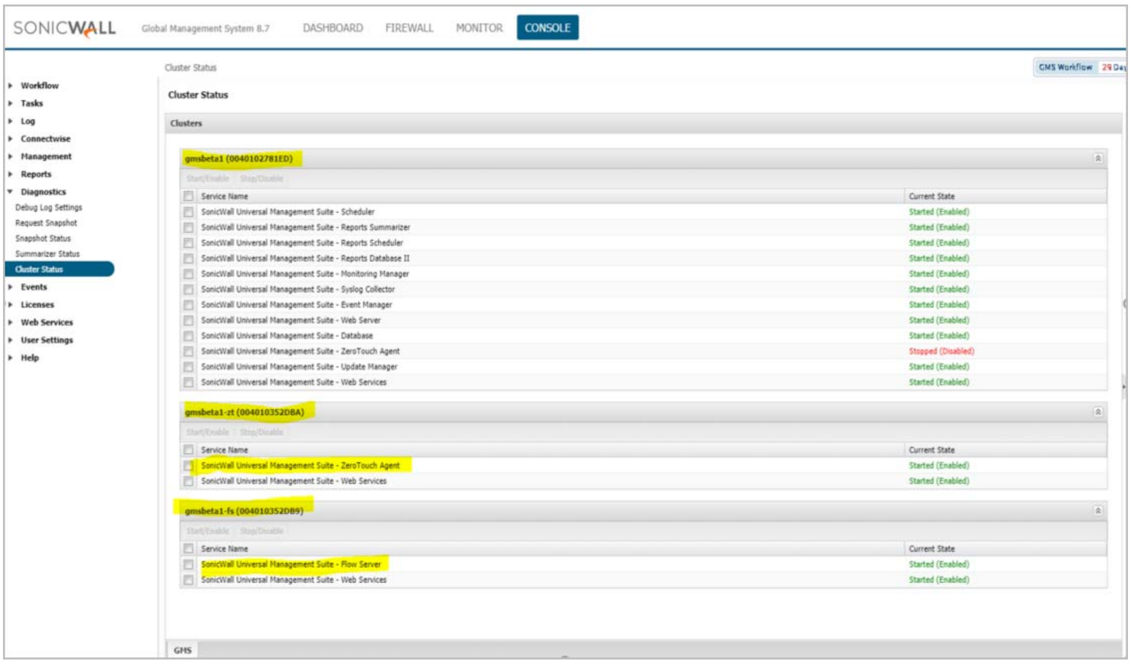
Firewall Sandwich Reporting	Distributed (AIO + one agent with role: Flow server)
ConnectWise Integration, Zero Touch, and Firewall Sandwich Reporting	Distributed (AIO + flow server agent) Distributed (Database + Console + flow server agent)

Enabling Zero Touch

For the Zero Touch feature to function correctly, you must have SonicOS 6.5.3.*x-xx*n or above running on your firewall. New firewall shipments already have that version and Zero Touch enabled in the firmware.

NOTE: Zero Touch was available in SonicOS 6.5.1.1-42n, but for best results, use the recommendation.

1 After you have installed the correct version of GMS and before enabling Zero Touch, you can optionally check **CONSOLE | Diagnostics > Cluster Status** to verify the Zero Touch services are running.



Cluster Status

Cluster Status

Clusters

gmsbeta1 (0040102781ED)

Service Name	Current State
SonicWall Universal Management Suite - Scheduler	Started (Enabled)
SonicWall Universal Management Suite - Reports Summarizer	Started (Enabled)
SonicWall Universal Management Suite - Reports Scheduler	Started (Enabled)
SonicWall Universal Management Suite - Reports Database II	Started (Enabled)
SonicWall Universal Management Suite - Monitoring Manager	Started (Enabled)
SonicWall Universal Management Suite - Syslog Collector	Started (Enabled)
SonicWall Universal Management Suite - Event Manager	Started (Enabled)
SonicWall Universal Management Suite - Web Server	Started (Enabled)
SonicWall Universal Management Suite - Database	Started (Enabled)
SonicWall Universal Management Suite - ZeroTouch Agent	Stopped (Disabled)
SonicWall Universal Management Suite - Update Manager	Started (Enabled)
SonicWall Universal Management Suite - Web Services	Started (Enabled)

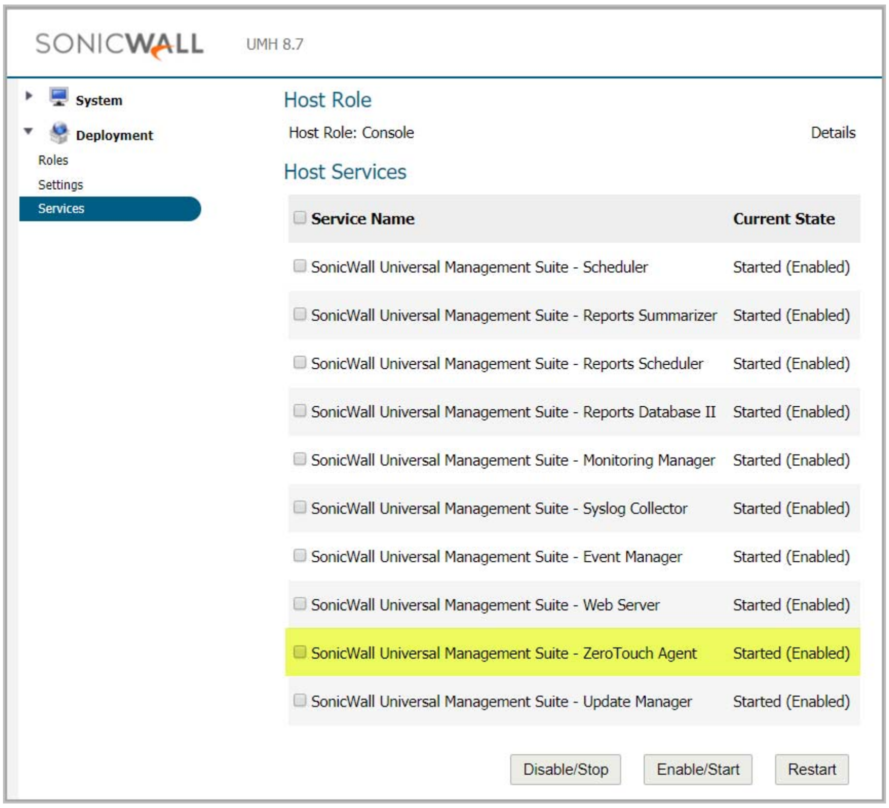
gmsbeta1-zt (004010352DBA)

Service Name	Current State
SonicWall Universal Management Suite - ZeroTouch Agent	Started (Enabled)
SonicWall Universal Management Suite - Web Services	Started (Enabled)

gmsbeta1-fs (004010352DB9)

Service Name	Current State
SonicWall Universal Management Suite - Flow Server	Started (Enabled)
SonicWall Universal Management Suite - Web Services	Started (Enabled)

2 You can also optionally check the agent console at **Deployment | Services** to determine whether the Zero Touch services are running in that environment.



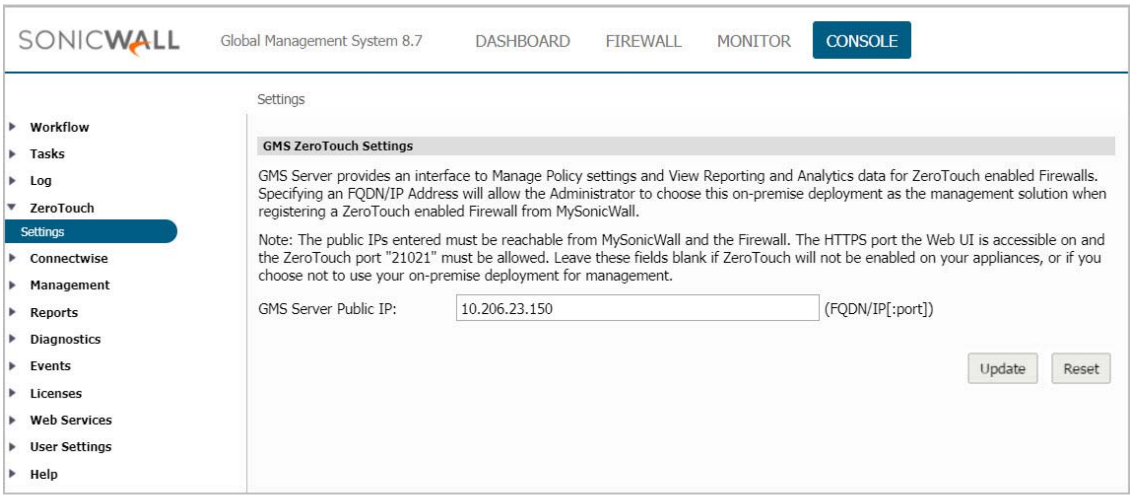
Host Role

Host Role: Console — Details

Host Services

☐ Service Name	Current State
☐ SonicWall Universal Management Suite - Scheduler	Started (Enabled)
☐ SonicWall Universal Management Suite - Reports Summarizer	Started (Enabled)
☐ SonicWall Universal Management Suite - Reports Scheduler	Started (Enabled)
☐ SonicWall Universal Management Suite - Reports Database II	Started (Enabled)
☐ SonicWall Universal Management Suite - Monitoring Manager	Started (Enabled)
☐ SonicWall Universal Management Suite - Syslog Collector	Started (Enabled)
☐ SonicWall Universal Management Suite - Event Manager	Started (Enabled)
☐ SonicWall Universal Management Suite - Web Server	Started (Enabled)
☐ SonicWall Universal Management Suite - ZeroTouch Agent	Started (Enabled)
☐ SonicWall Universal Management Suite - Update Manager	Started (Enabled)

3 Navigate to **CONSOLE | Zero Touch > Settings**.



GMS ZeroTouch Settings

GMS Server provides an interface to Manage Policy settings and View Reporting and Analytics data for ZeroTouch enabled Firewalls. Specifying an FQDN/IP Address will allow the Administrator to choose this on-premise deployment as the management solution when registering a ZeroTouch enabled Firewall from MySonicWall.

Note: The public IPs entered must be reachable from MySonicWall and the Firewall. The HTTPS port the Web UI is accessible on and the ZeroTouch port "21021" must be allowed. Leave these fields blank if ZeroTouch will not be enabled on your appliances, or if you choose not to use your on-premise deployment for management.

GMS Server Public IP: 10.206.23.150 (FQDN/IP[:port])

4 Before providing the FQDN/IP address for your GMS server, consider the following:

- The GMS server IP must be a reachable IP (publicly) for the AIOP or Console on ports 443 (or custom) and 21021 for the firewall.

5 After you have entered a valid FQDN/IP address, click **Update**. Click **OK** to confirm changes or **Cancel** to start over.

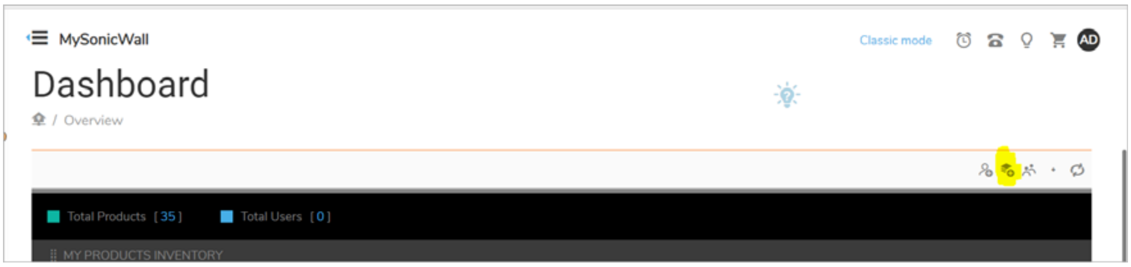
6 If you are running earlier versions of SonicWall firewalls, complete the following steps. If you are running a brand new firewall, skip to the second bullet.

- Delete the firewall from your MySonicWall account and then make sure it is updated to and running SonicOS version 6.5.3.1 -*xxn*. Reboot the firewall using the factory default settings.
- While registering the firewall on MySonicWall, be sure to enable the Zero Touch checkbox.
- Choose the GMS On-Prem policy server from the drop-down menu.

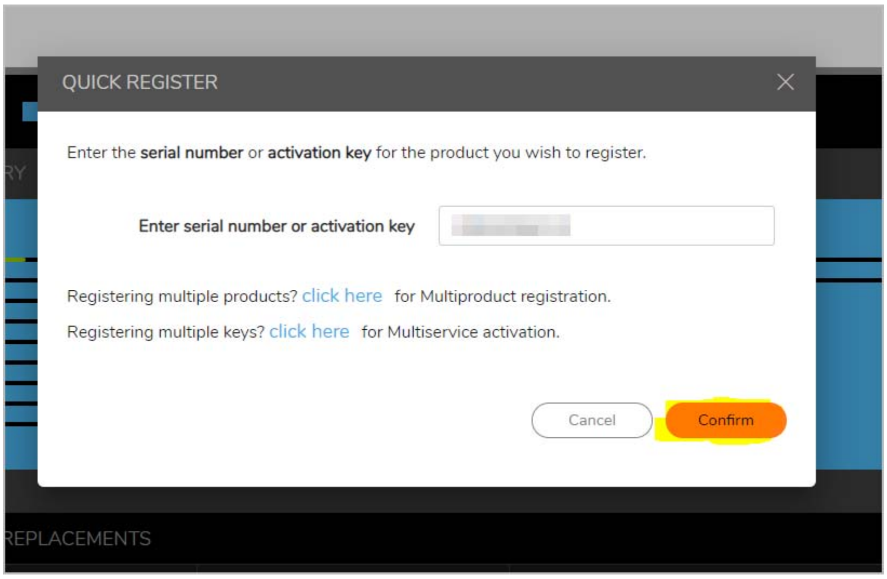
ⓘ | **NOTE:** Bulk deployment for Zero Touch is not supported in the this version of the software.

- You can specify values different from those already present. Edit the fields to specify the new IP addresses.

7 From the MySonicWall Dashboard, click the **Register** icon in the top right button bar.



8 In the Quick Register form that appears, enter the **serial number** or **activation key** (usually located on the bottom of your firewall) for the product you wish to register.



QUICK REGISTER

Enter the **serial number** or **activation key** for the product you wish to register.

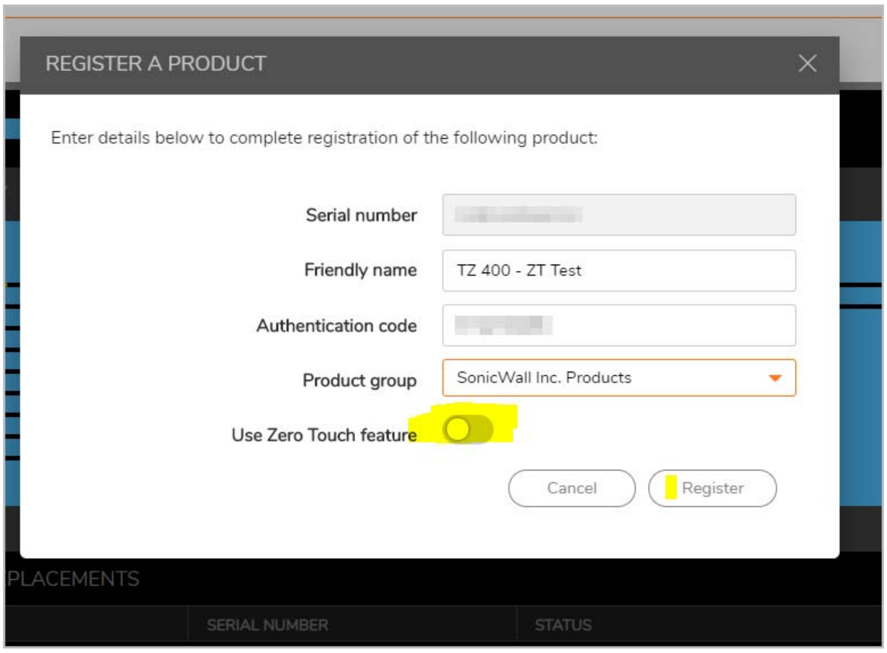
Enter serial number or activation key [redacted]

Registering multiple products? click here for Multiproduct registration.

Registering multiple keys? click here for Multiservice activation.

9 Click **Confirm**.

10 To complete the registration, enter a **Friendly name** for the specific firewall, an **Authentication code** (received from your vendor at the time of purchase), and a **Product group** for this particular firewall in the remaining fields.



REGISTER A PRODUCT

Enter details below to complete registration of the following product:

Serial number	[redacted]
Friendly name	TZ 400 - ZT Test
Authentication code	[redacted]
Product group	SonicWall Inc. Products
Use Zero Touch feature	

11 To use the **Zero Touch** feature, be sure to enable the slider button.

12 Click **Register**.

13 A drop-down box appears where you can choose GMS. Select GMS and provide the required details in the available fields.

After you have completed registration, the firewall appears on the GMS console (one to two minutes).

5

Configuring ConnectWise

This chapter shows how GMS integrates with the ConnectWise Manage platform to provide you with the ability to synchronize basic firewall details into the ConnectWise platform. This integration includes the capability of managing security events and SonicWall assets and provides the ability to create automated service tickets for alerts in the ConnectWise Manage platform. Features also include:

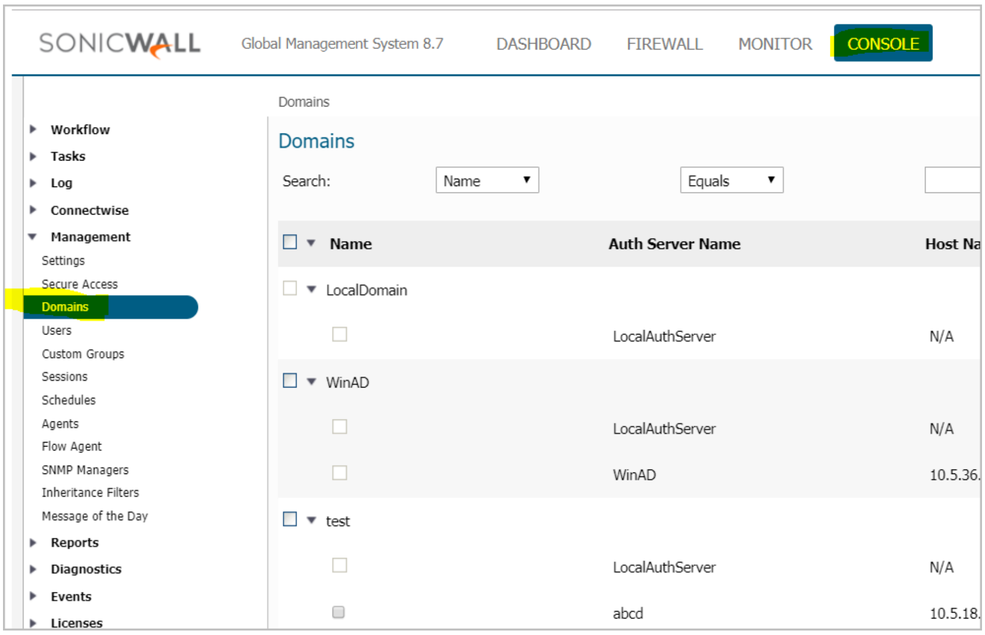
- **Asset Synchronization** - Assets managed by GMS (firewalls, Email Security, Secure Mobile Access) can synchronize with ConnectWise Manage.
- **Automated TIcketing** - GMS automatically creates and deletes tickets in ConnectWise Manage when alerts have been generated in GMS.

Topics:

Configuring ConnectWise Settings

To setup integration between GMS and ConnectWise:

1 Navigate to **CONSOLE | Management > Domains** and create a domain for managed companies. (Domains in GMS map to managed companies in ConnectWise Manage). See Domains for additional information.

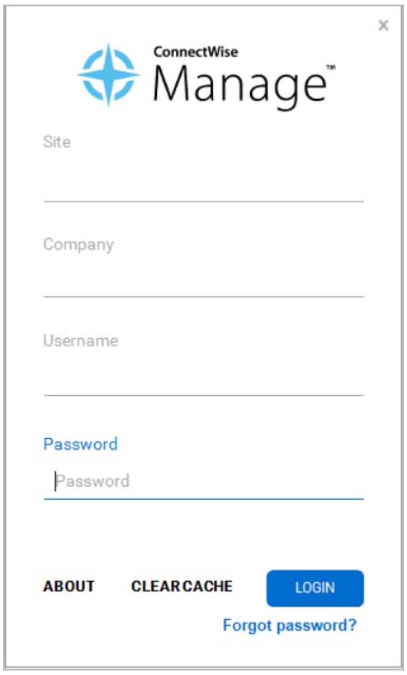


Domains

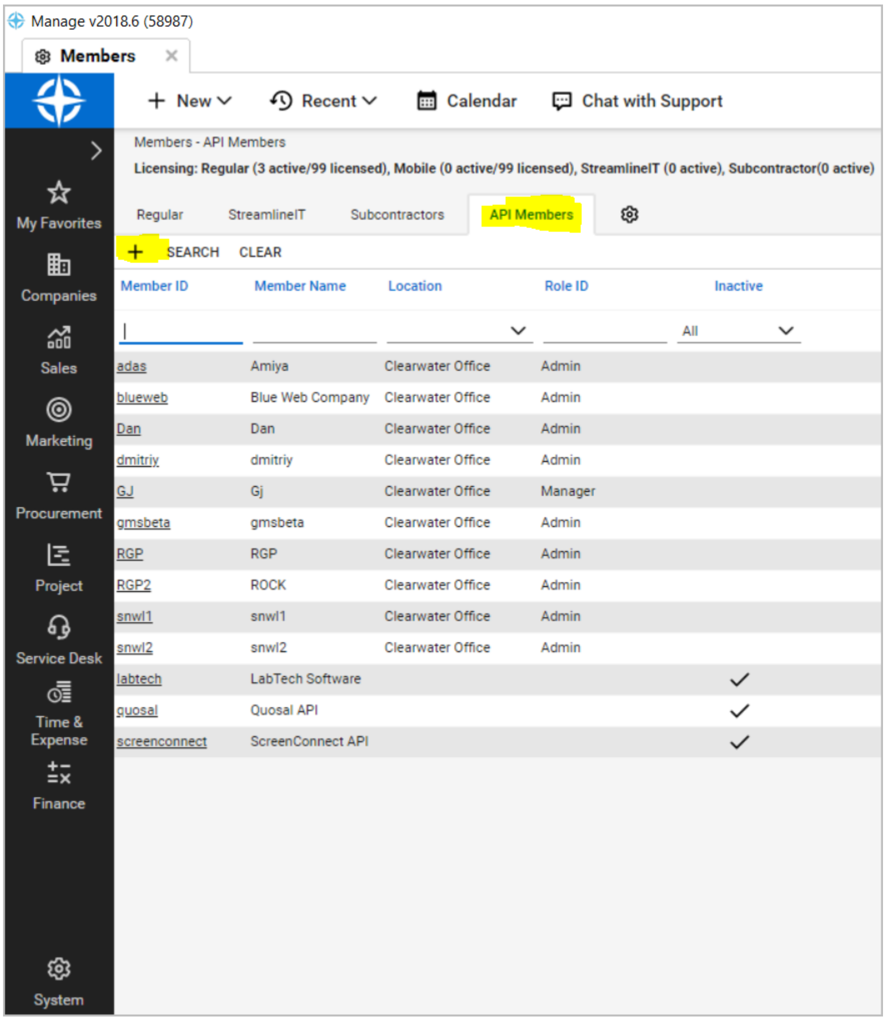
Search: Name ▾ Equals ▾

□ ▾ Name	Auth Server Name	Host Na
□ ▾ LocalDomain		
□	LocalAuthServer	N/A
□ ▾ WinAD		
□	LocalAuthServer	N/A
□	WinAD	10.5.36.
□ ▾ test		
□	LocalAuthServer	N/A
□	abcd	10.5.18.

2 Log in to **ConnectWise Manage**.



3 In ConnectWise, navigate to **System > Manage > API Members**.



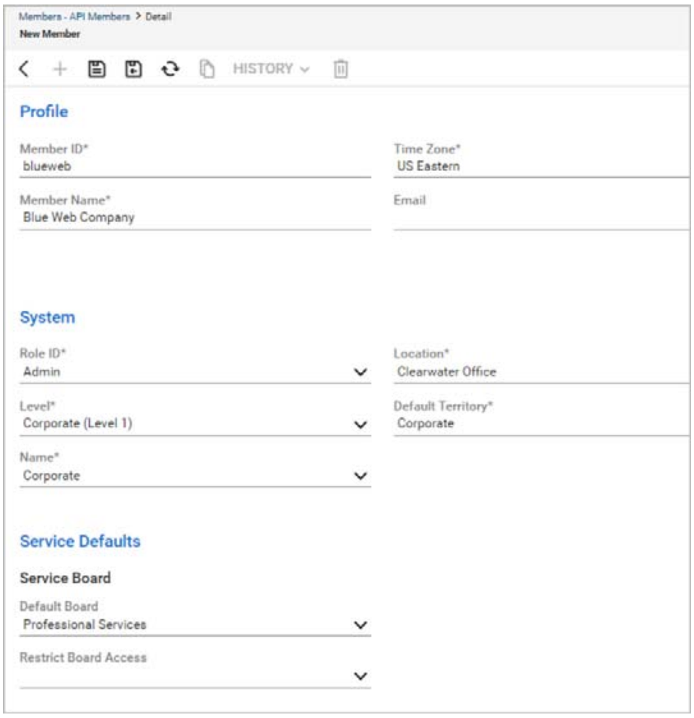
Members - API Members

Licensing: Regular (3 active/99 licensed), Mobile (0 active/99 licensed), StreamlineIT (0 active), Subcontractor(0 active)

Member ID	Member Name	Location	Role ID	Inactive
adas	Amiya	Clearwater Office	Admin	
blueweb	Blue Web Company	Clearwater Office	Admin	
Dan	Dan	Clearwater Office	Admin	
dmitriy	dmitriy	Clearwater Office	Admin	
GJ	Gj	Clearwater Office	Manager	
gmsbeta	gmsbeta	Clearwater Office	Admin	
RGP	RGP	Clearwater Office	Admin	
RGP2	ROCK	Clearwater Office	Admin	
snwl1	snwl1	Clearwater Office	Admin	
snwl2	snwl2	Clearwater Office	Admin	
labtech	LabTech Software			✓
quosal	Quosal API			✓
screenconnect	ScreenConnect API			✓

4 On the API Members tab, click the **+** sign to create a new API member for the managed company administrator.

5 In the System section, add an Admin profile for the managed company.



Members - API Members > Detail

New Member

HISTORY

Profile

Member ID*
blueweb

Time Zone*
US Eastern

Member Name*
Blue Web Company

Email

System

Role ID*
Admin

Location*
Clearwater Office

Level*
Corporate (Level 1)

Default Territory*
Corporate

Name*
Corporate

Service Defaults

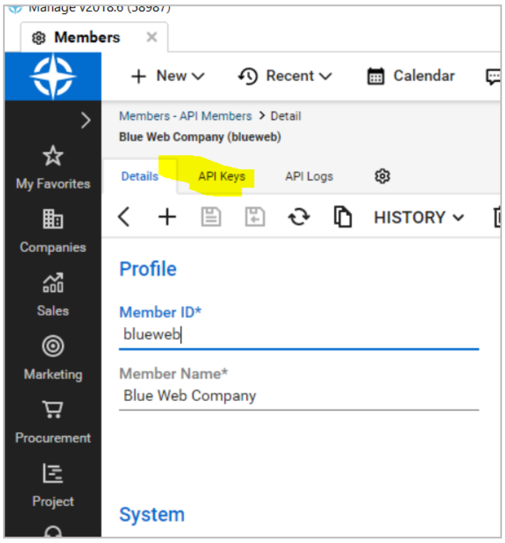
Service Board

Default Board
Professional Services

Restrict Board Access

6 Click **Save**.

7 Click the **API Keys** tab.



Members - API Members > Detail

Blue Web Company (blueweb)

Details API Keys API Logs

HISTORY

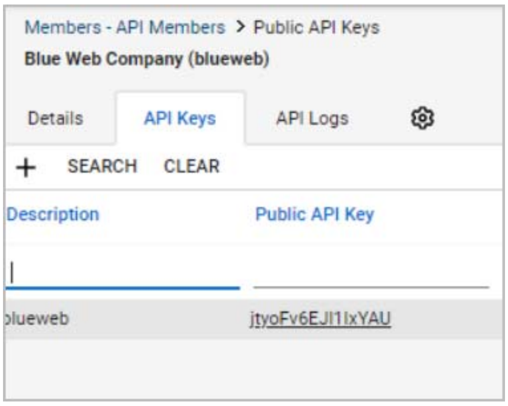
Profile

Member ID*
blueweb

Member Name*
Blue Web Company

System

8 Generate a **Public API Key** and a **Private API Key** for the Administrator.

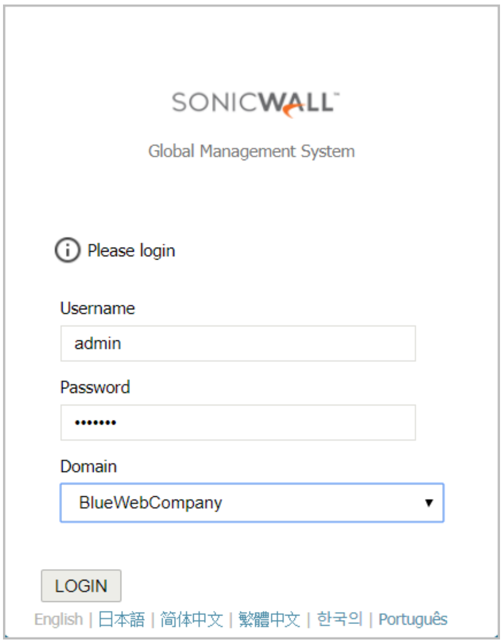


Members - API Members > Public API Keys

Blue Web Company (blueweb)

Description	Public API Key
blueweb	jtyoFv6EJI1IxYAU

9 Log back in to GMS using your newly created Domain (for the managed company).

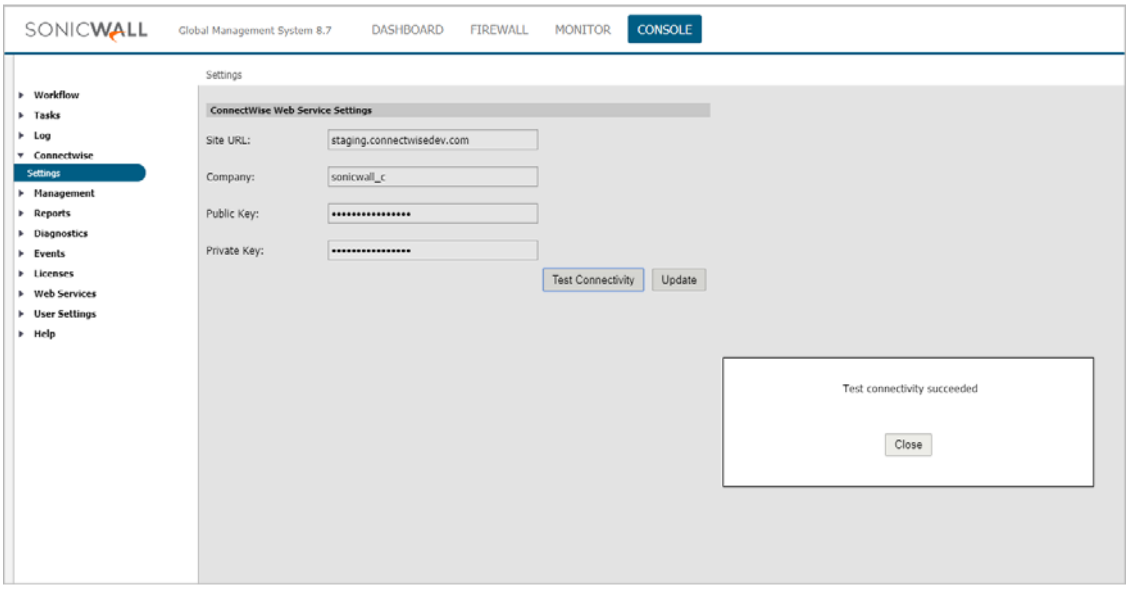


Username: admin

Password: •••••••

Domain: BlueWebCompany

10 Navigate to **CONSOLE | ConnectWise > Settings**.



Settings

ConnectWise Web Service Settings

Site URL: staging.connectwisedev.com

Company: sonicwall_c

Public Key: ••••••••••••••••

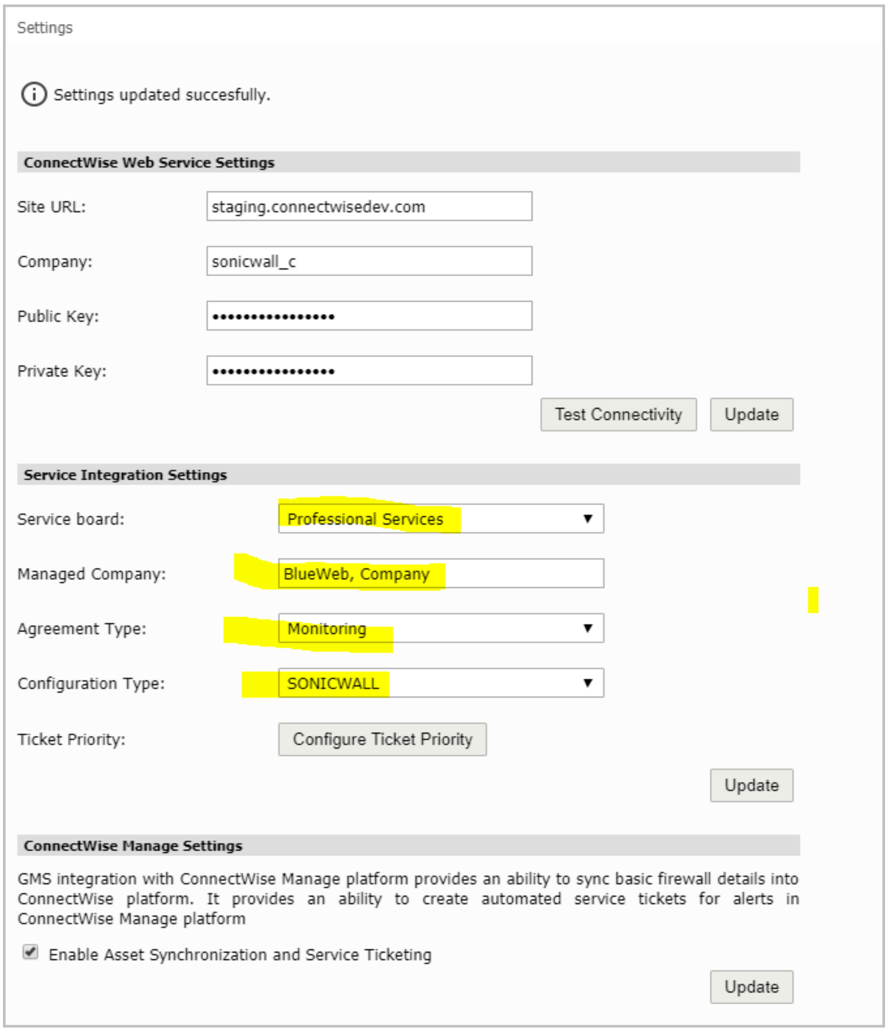
Private Key: ••••••••••••••••

Test connectivity succeeded

11 Complete the screen by entering the **Site URL**, your **Company Name**, the **Public Key** and the **Private key** you created for ConnectWise.

12 Click **Test Connectivity**.

13 If the connection is successful, click **Update** to move forward. Additional Service Integration Settings appear.



Settings

ⓘ Settings updated succesfully.

ConnectWise Web Service Settings

Site URL: staging.connectwisedev.com

Company: sonicwall_c

Public Key: ••••••••••••••••

Private Key: ••••••••••••••••

Service Integration Settings

Service board: Professional Services ▼

Managed Company: BlueWeb, Company

Agreement Type: Monitoring ▼

Configuration Type: SONICWALL ▼

Ticket Priority:

ConnectWise Manage Settings

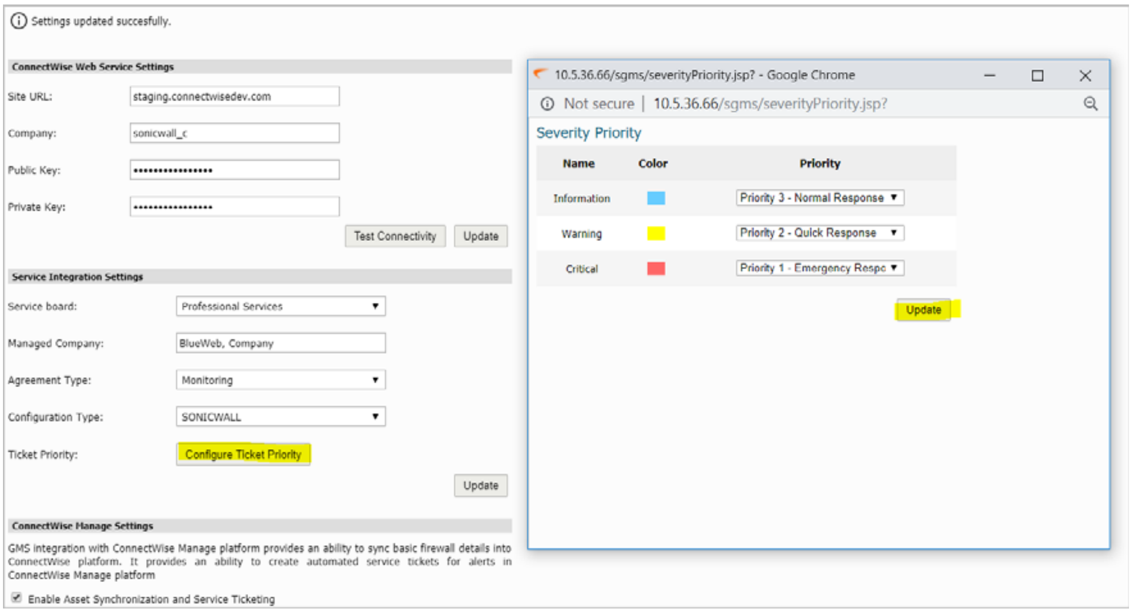
GMS integration with ConnectWise Manage platform provides an ability to sync basic firewall details into ConnectWise platform. It provides an ability to create automated service tickets for alerts in ConnectWise Manage platform

☑ Enable Asset Synchronization and Service Ticketing

14 Complete the additional settings as follows:

- **Service Board** - From the drop-down menu, choose the service board you are managing.
- **Managed Company** - Enter the name of the company you want to map to the GMS domain you logged in to.
- **Agreement Type** - Select an Agreement Type from the drop-down menu.
- **Configuration Type** - By selecting SONICWALL from the drop-down menu, SonicWall assets can be filtered on the ConnectWise Manage configuration dashboard.

15 Click **Configure Ticket Priority** to assign severity priorities.



Settings updated succesfully.

ConnectWise Web Service Settings

Site URL: staging.connectwisedev.com

Company: sonicwall_c

Public Key: ••••••••••••••••

Private Key: ••••••••••••••••

Test Connectivity | Update

Service Integration Settings

Service board: Professional Services

Managed Company: BlueWeb, Company

Agreement Type: Monitoring

Configuration Type: SONICWALL

Ticket Priority: Configure Ticket Priority

Update

ConnectWise Manage Settings

GMS integration with ConnectWise Manage platform provides an ability to sync basic firewall details into ConnectWise platform. It provides an ability to create automated service tickets for alerts in ConnectWise Manage platform

☑ Enable Asset Synchronization and Service Ticketing

10.5.36.66/sgms/severityPriority.jsp? - Google Chrome

Not secure | 10.5.36.66/sgms/severityPriority.jsp?

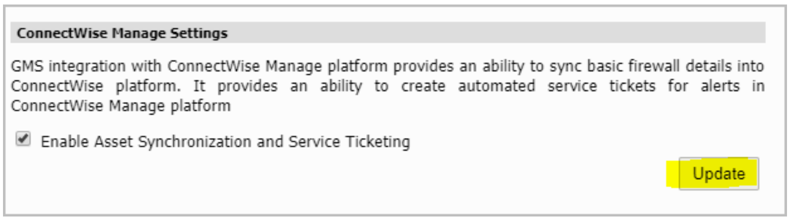
Severity Priority

Name	Color	Priority
Information	🟦	Priority 3 - Normal Response
Warning	🟨	Priority 2 - Quick Response
Critical	🟥	Priority 1 - Emergency Respo

Update

16 Click **Update**.

17 Ensure that the ConnectWise Manage Settings checkbox for **Enable Asset Synchronization and Service Ticketing** is selected.



ConnectWise Manage Settings

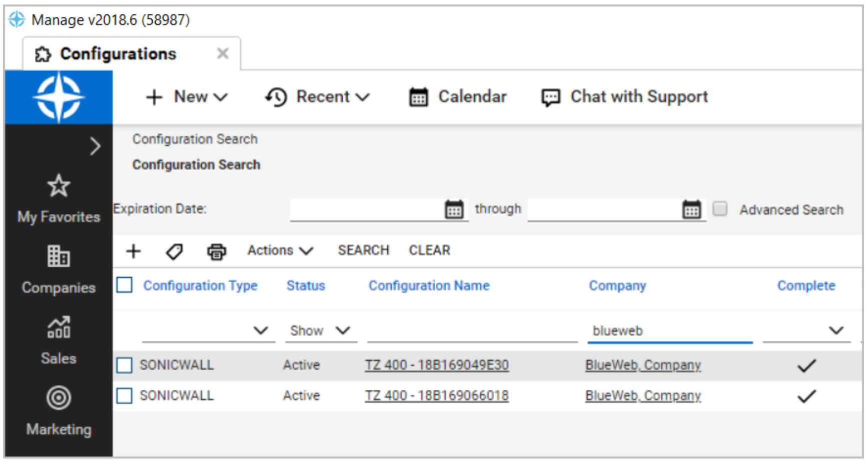
GMS integration with ConnectWise Manage platform provides an ability to sync basic firewall details into ConnectWise platform. It provides an ability to create automated service tickets for alerts in ConnectWise Manage platform

☑ Enable Asset Synchronization and Service Ticketing

Update

18 Click **Update**. The integration setup is complete.

You can log back in to ConnectWise to see that your assets (firewalls and so on) are synchronized with ConnectWise Manage.



Configuration Search

Configuration Search

Expiration Date: through □ Advanced Search

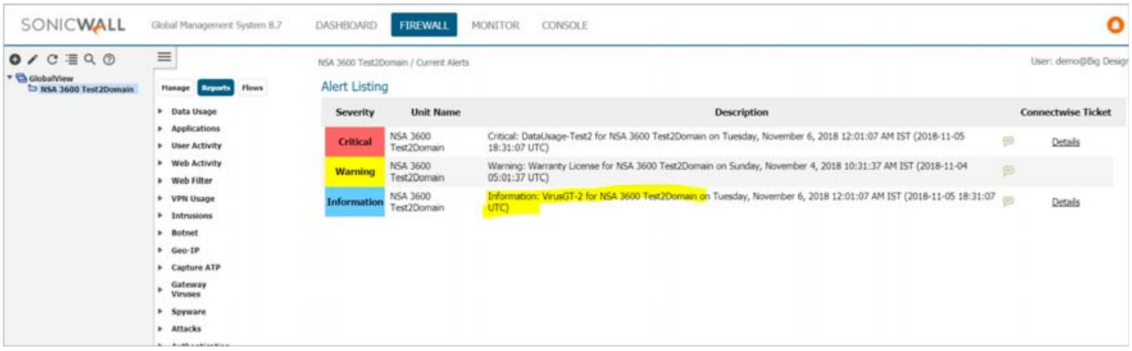
□	Configuration Type	Status	Configuration Name	Company	Complete
		Show		blueweb	
□	SONICWALL	Active	TZ 400 - 18B169049E30	BlueWeb, Company	✓
□	SONICWALL	Active	TZ 400 - 18B169066018	BlueWeb, Company	✓

Configuring Alerts

You can configure alerts in GMS, so that when events are triggered, tickets are then created in ConnectWise Manage. When alerts are deleted in GMS, the corresponding ticket in ConnectWise Manage are also deleted. See the *FIREWALL: Reports Administration Guide* for additional details on configuring alert settings

To configure alerts in GMS:

1 Navigate to **FIREWALL | Reports | Events > Current Alerts**.



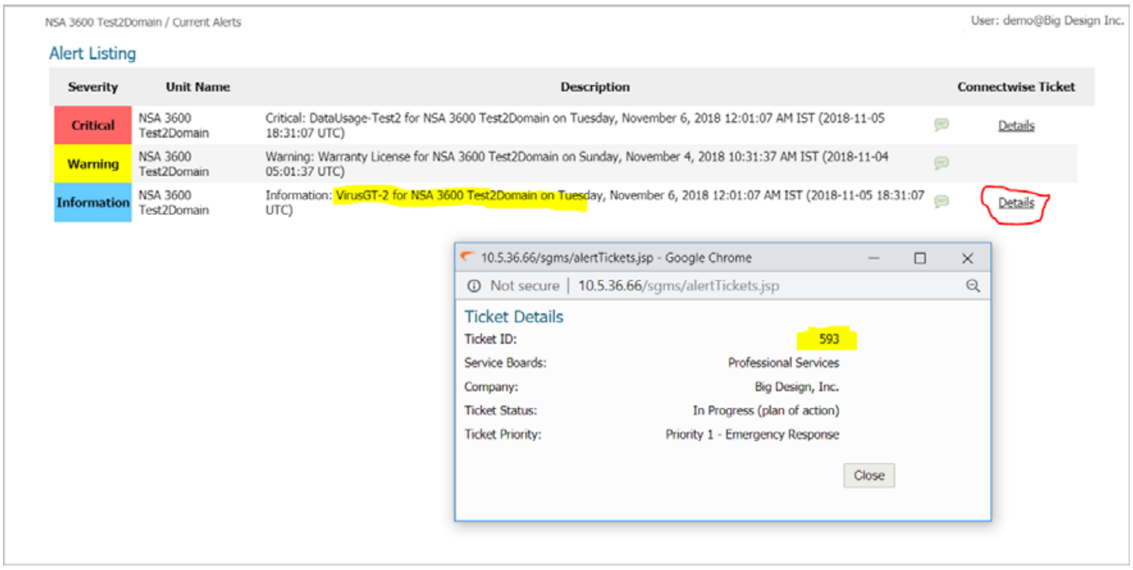
NSA 3600 Test2Domain / Current Alerts

User: demo@Big Design

Alert Listing

Severity	Unit Name	Description	Connectwise Ticket
Critical	NSA 3600 Test2Domain	Critical: DataUsage-Test2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC)	Details
Warning	NSA 3600 Test2Domain	Warning: Warranty License for NSA 3600 Test2Domain on Sunday, November 4, 2018 10:31:37 AM IST (2018-11-04 05:01:37 UTC)	
Information	NSA 3600 Test2Domain	Information: VirusGT-2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC)	Details

2 In Alert Listing, click **Details** to see more information about the generated ticket.



NSA 3600 Test2Domain / Current Alerts

User: demo@Big Design Inc.

Alert Listing

Severity	Unit Name	Description	Connectwise Ticket
Critical	NSA 3600 Test2Domain	Critical: DataUsage-Test2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC)	Details
Warning	NSA 3600 Test2Domain	Warning: Warranty License for NSA 3600 Test2Domain on Sunday, November 4, 2018 10:31:37 AM IST (2018-11-04 05:01:37 UTC)	
Information	NSA 3600 Test2Domain	Information: VirusGT-2 for NSA 3600 Test2Domain on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC)	Details

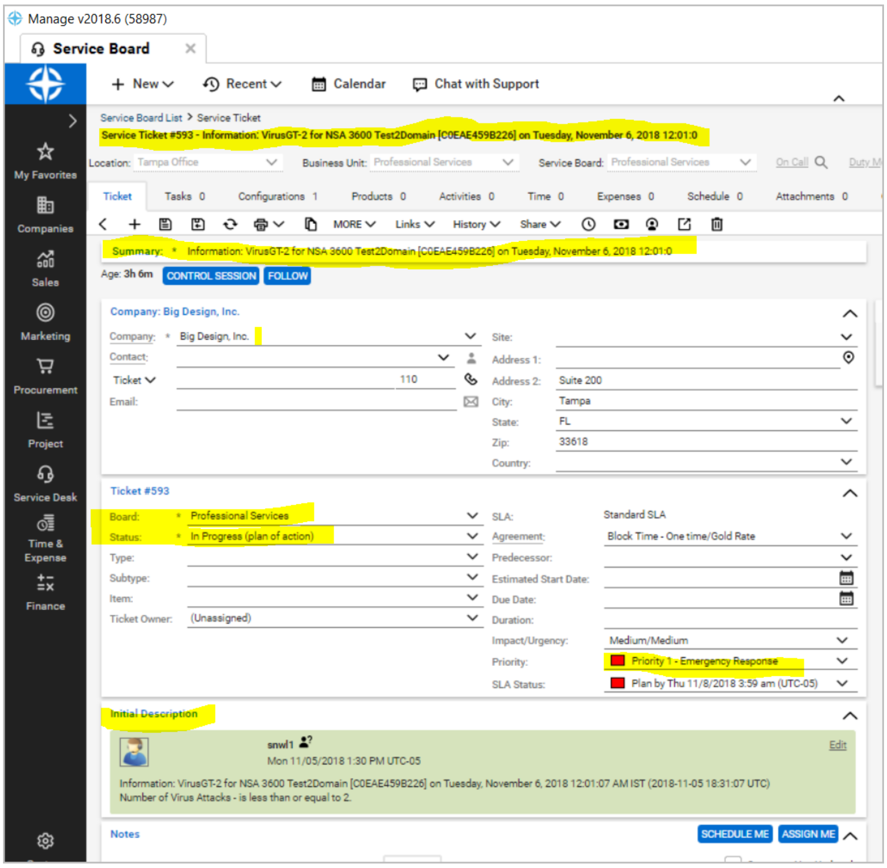
10.5.36.66/sgms/alertTickets.jsp - Google Chrome

Not secure | 10.5.36.66/sgms/alertTickets.jsp

Ticket Details

Ticket ID:	593
Service Boards:	Professional Services
Company:	Big Design, Inc.
Ticket Status:	In Progress (plan of action)
Ticket Priority:	Priority 1 - Emergency Response

3 In ConnectWise Manage at **Service Board List > Service Ticket**, locate the same Ticket ID as found in GMS to view the status, summary, priority, and description of the ticket and related information.



Service Board List > Service Ticket

Service Ticket #593 - Information: VirusGT-2 for NSA 3600 Test2Domain [C0EAE459B226] on Tuesday, November 6, 2018 12:01:0

Location: Tampa Office
Business Unit: Professional Services
Service Board: Professional Services

Summary: * Information: VirusGT-2 for NSA 3600 Test2Domain [C0EAE459B226] on Tuesday, November 6, 2018 12:01:0

Age: 3h 6m

Company: Big Design, Inc.

Company: * Big Design, Inc.
Contact:
Ticket 110
Email:
Site:
Address 1:
Address 2: Suite 200
City: Tampa
State: FL
Zip: 33618
Country:

Ticket #593

Board: * Professional Services
Status: * In Progress (plan of action)
Type:
Subtype:
Item:
Ticket Owner: (Unassigned)
SLA: Standard SLA
Agreement: Block Time - One time/Gold Rate
Predecessor:
Estimated Start Date:
Due Date:
Duration:
Impact/Urgency: Medium/Medium
Priority: 🟥 Priority 1 - Emergency Response
SLA Status: 🟥 Plan by Thu 11/8/2018 3:59 am (UTC-05)

Initial Description

snwl1
Mon 11/05/2018 1:30 PM UTC-05

Information: VirusGT-2 for NSA 3600 Test2Domain [C0EAE459B226] on Tuesday, November 6, 2018 12:01:07 AM IST (2018-11-05 18:31:07 UTC)
Number of Virus Attacks - is less than or equal to 2.

Notes

4 In ConnectWise Manage, make assignments and scheduling solutions and click **Schedule Me** or **Assign Me** as appropriate.

6

Configuring Console Management Settings

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

Topics:

Configuring Management Settings

On the **CONSOLE | Management > Settings** page, you can configure email settings, enable automatic preferences file backup, enable reporting, configure GMS to synchronize with managed units, configure Enhanced Security Access (ESA) settings, enable management of SMA and ES devices, configure GMS for manual signature uploads, download GMS CLI Client, and enable Data Privacy Settings for Reports.

Topics:

GMS Settings

The GMS Settings allow you to show or hide the SMA and Email Security tabs. This section is only visible to administrators @LocalDomain, such as Super Admins.

Configuring Email Settings

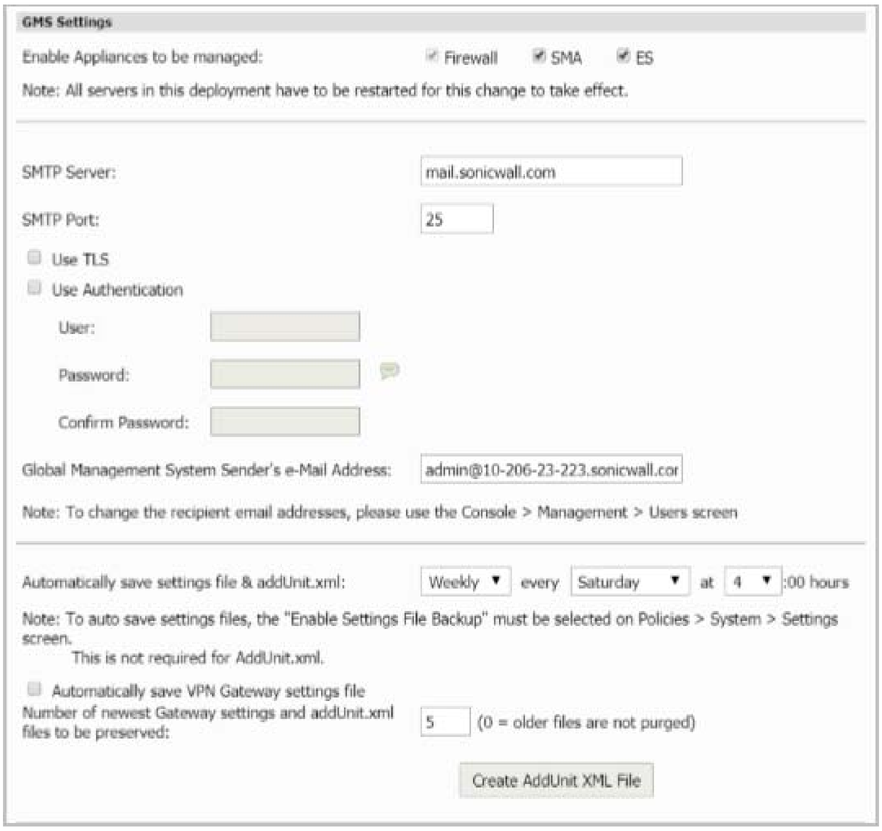
An SMTP server and an email address are required for sending GMS reports.

If the Mail Server settings are not configured correctly, you will not receive important email notifications, such as:

- System alerts for your GMS deployment performance
- Availability of product updates, hot fixes, or patches
- Availability of firmware upgrades for managed appliances
- Alerts on your managed appliances’ status
- Scheduled Reports

To configure these email settings, complete the following steps:

1 Navigate to **CONSOLE | Management > Settings**. The Settings page displays.



GMS Settings

Enable Appliances to be managed: ☑ Firewall ☑ SMA ☑ ES

Note: All servers in this deployment have to be restarted for this change to take effect.

SMTP Server: mail.sonicwall.com

SMTP Port: 25

□ Use TLS

□ Use Authentication

User:

Password:

Confirm Password:

Global Management System Sender's e-Mail Address: admin@10-206-23-223.sonicwall.cor

Note: To change the recipient email addresses, please use the Console > Management > Users screen

Automatically save settings file & addUnit.xml: Weekly every Saturday at 4 :00 hours

Note: To auto save settings files, the "Enable Settings File Backup" must be selected on Policies > System > Settings screen.
This is not required for AddUnit.xml.

□ Automatically save VPN Gateway settings file

Number of newest Gateway settings and addUnit.xml files to be preserved: 5 (0 = older files are not purged)

2 Click any additional management tabs for servers you would like to enable including tabs for Secure Mobile Access (5e) or Email Security (ES). The servers should be restarted for this change to take effect.

3 Type the IP address or the FQDN of the Simple Mail Transfer Protocol (SMTP) server into the **SMTP Server** field. This server can be the same one that is normally used for email in your network. Type in the SMTP Port number to use for email service. This field can accept/display IPv4 and IPv6 addresses.

4 Click **Use TLS** if you would like to use Transport Layer Security (TLS) for your mail server connectivity, such as for Gmail or Office365. TLS ensures privacy between you and communicating applications on the Internet, and that no third-party can eavesdrop or tamper with your messages.

5 If the SMTP server in your deployment is set to use authentication, click **Use Authentication**. This option is necessary for all outgoing GMS emails to properly send to the intended recipients. Enter the username in the **User** field, and enter/confirm the password in the **Password** and **Confirm Password** fields. This is the username/password that is used to authenticate against the SMTP server.

6 Enter the email account name and domain that appears in messages sent from the GMS into the **GMS Sender's e-Mail Address** field.

7 Enter the email account name and domain that appears in messages sent from the GMS into the **GMS Administrator e-Mail Address** field. You can use User Authentication for this user by checking the box.

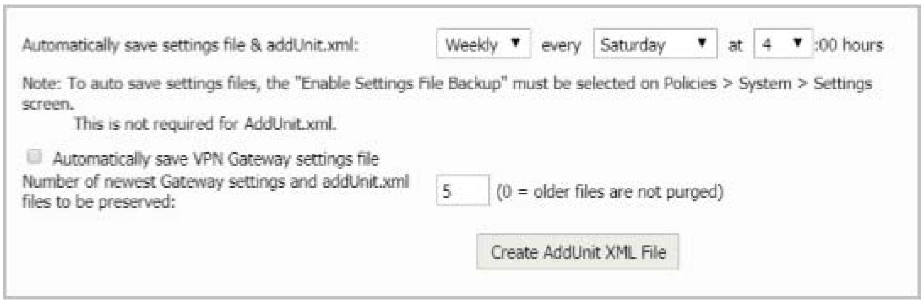
8 When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Configuring Prefs Backup Settings

You can have the system automatically save your firewall preferences files on a regular basis. This includes the addunit.xml file that contains information about the units under GMS management.

To configure the prefs file settings:

1 Navigate to **Console | Management > Settings.** The Settings page displays.



Automatically save settings file & addUnit.xml: Weekly ▼ every Saturday ▼ at 4 ▼ :00 hours

Note: To auto save settings files, the "Enable Settings File Backup" must be selected on Policies > System > Settings screen.
This is not required for AddUnit.xml.

□ Automatically save VPN Gateway settings file

Number of newest Gateway settings and addUnit.xml files to be preserved: 5 (0 = older files are not purged)

2 Select **Daily** or **Weekly** in the **Automatically save settings file & addunit.xml** field, and select a day of the week (if weekly) and a time. This determines how often GMS automatically saves the preferences and addUnit.xml files.

3 To automatically save the VPN Gateway Preferences files for SonicWall appliances, select **Automatically save VPN Gateway Settings file**.

> **NOTE:** The **Enable Settings File Backup** option must also be selected on the **FIREWALL | System > Settings** screen.

4 The **Create AddUnit XML File** link can be used to manually create an AddUnit XML file of the system that can then be imported into another GMS system if necessary, such as during GMS migration. To create an addUnit.xml file to track all units under management, click **Create AddUnit XML File**.

5 When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Enabling Reporting and Synchronization with Managed Units

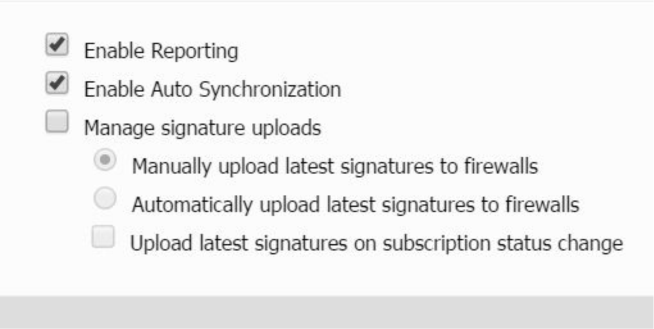
By default, GMS Reporting is enabled.

To enable or disable GMS Reporting, complete the following steps:

1. Navigate to **CONSOLE | Management > Settings.** The Settings page displays.
2. To enable GMS Reporting, select **Enable Reporting**. To disable it, deselect **Enable Reporting** (default: Enabled).
3. To configure GMS to automatically synchronize with the local changes made to the SonicWall appliances, select **Enable Auto Synchronization**.

Managing Signature Uploads Manually

1. For SonicWall appliances that do not have direct access to the Internet, you can instruct GMS to download updates to security service signatures. To do so, navigate to **CONSOLE | Management > Settings** and click on **Manage signature uploads**, as shown in the following image.



☑ Enable Reporting
☑ Enable Auto Synchronization
□ Manage signature uploads
● Manually upload latest signatures to firewalls
○ Automatically upload latest signatures to firewalls
□ Upload latest signatures on subscription status change

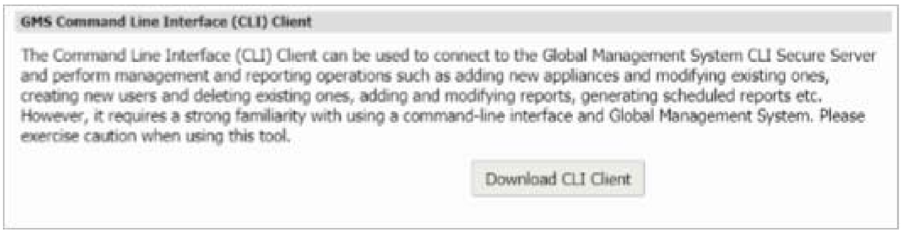
2. Select one of the following radio buttons:
   - **Manually upload latest signatures to firewalls**
   - **Automatically upload latest signatures to firewalls**
   - (optional) **Upload latest signatures on subscription status change**. This option is available when **Manage Signature Uploads** is enabled.

   > **NOTE:** When updated signatures have been downloaded to the GMS, you must then manually upload them to the SonicWall appliances. This action is completed on the **FIREWALL | System > Tools** page. When there are new signatures to be uploaded, **Upload Signatures Now** appears on the Tools page. Click this button to manually upload the signatures.

3. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Command Line Interface (CLI) Client

The CLI client can be downloaded to allow running scripts on a secure server. To download the CLI Client, navigate to **CONSOLE | Management > Settings** and click **Download CLI Client**, as shown in the following image.



GMS Command Line Interface (CLI) Client

The Command Line Interface (CLI) Client can be used to connect to the Global Management System CLI Secure Server and perform management and reporting operations such as adding new appliances and modifying existing ones, creating new users and deleting existing ones, adding and modifying reports, generating scheduled reports etc. However, it requires a strong familiarity with using a command-line interface and Global Management System. Please exercise caution when using this tool.

For more information on using the GMS CLI, see Using the SonicWall GMS CLI on page 912.

Enhanced Security Access Settings

SonicWall's Enhanced Security Access (ESA) feature allows for greater granular control of user access across a GMS network, which is applicable for installations that must comply with stringent regulatory compliance and account management controls as found in such standards as Payment Card Industry (PCI), SOX, or HIPAA.

ⓘ **NOTE:** Enhanced security settings are also available in your browser. For information, refer to Browser Requirements on page 12.

GMS supports these data security standards by providing support for encryption of all passwords and any pre-shared secrets in the database. This includes VPN Security Association pre-shared secrets, encryption keys, authentication keys, and passwords. The following passwords are encrypted in GMS:

- GMS gateway password
- SonicWall firewall appliance passwords for managed units
- Guest account password
- LDAP and RADIUS passwords

Enhanced security compliance also requires a password rotation feature. GMS supports password rotation requirements, including several changes in the management interface. These changes occur on the **CONSOLE** view, in the **CONSOLE | Management** > **Settings** screen and in all screens accessed from the **CONSOLE | Management** > **Users** screen.

To turn on password security enforcement in GMS:

1 Navigate to **CONSOLE | Management > Settings** and click the **Enforce Password Security** box.

2 In the **Number of failed login attempts before user can be locked out** field, enter a value. The default is 6.

3 In the **User lockout minutes** field, enter a value. The default is 30. This is the number of minutes that a user will not be able to log in to GMS after failing to log in correctly for the specified number of attempts. To enforce a permanent account lockout, enter a "-1" value in this field.

4 In the **Number of inactive days to mark user for deletion** field, enter a value. The default is 90. The user's account is deleted if it is not used for the specified number of days.

5 In the **Number of days to force password change** field, enter a value. The default is 90. GMS prompts the user to change his password after the specified number of days.

6 When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset**.

Enabling Data Privacy Settings

The Reports Privacy feature allows a GMS Super Admin to configure the GMS system to mask all IPs, user names, and host names in Reports.

Consider the following before enabling the Data Privacy settings:

- The Data Privacy setting is a system wide setting, and cannot be granularly set for each unit or each domain separately.
- This feature applies only to the Reports on the **CONSOLE | Reports** page and Live Monitor/Syslog Viewer pages on the **MONITOR | Tools > Live Monitor/Syslog Viewer** page. It does not apply to other places in the GMS UI that could have IPs, usernames, and so on. This means the following are not included:
    - Firewall screens such as **FIREWALL | Reports > Data Usage.**
    - Console View screens such as **CONSOLE | Logs**.
- Requires a double-authentication mechanism to unmask identities.
- Unmasking reports through double-authentication is only for on-demand management interface based reports. Other reports, such as Scheduled Reports or Webservices based reports, are sent masked if the global system setting is set for Reports Privacy. The only way to view actual IPs in the Scheduled Reports is by disabling the privacy feature at system level.
- IPs, Hostnames, and User Names are masked for any “private” IPs (such as subnets 192.168.255.255, 172.31.255.255, 10.255.255.255). This happens for both Initiators and Responders, in the Grids and Charts.
- This feature is available only for firewall reports, and not for SMA reports.
- The masked entries do not allow the one-click mechanism to add it to the Filter bar.
- Filter Bar does not allow adding Initiators and Responders filters.
- Any Custom Report that has Initiators or Responders does not generate a report.
- The User Activity report does not generate reports.
- Scheduled Reports always has the above information masked.
- Scheduled Reports containing Custom Reports that have Initiators or Responders will not generate any Customer Report data.

To enable the Data Privacy Settings, complete the following steps:

1. Navigate to **CONSOLE | Management > Settings**. The Settings page displays.
2. Click **Enable Data Privacy**, and then click **Update**.

The IPs, user names, and host names are now masked in the reports.

ⓘ **NOTE:** Privileges to unmask reports can be set for designated users if the Super Admin or User changes the Action Permissions to “Can Unmask Reports.” Those users can then click the **Unmask** icon while viewing a masked report, enter their credentials, and the report displays unmasked. See Configuring Action Permissions on page 55 and Unmask Reports on page 14 for more details.

Domains

A domain in GMS is a logically bound collection of users, authentication servers, managed appliances, policies and reporting data, alerts, and all other related data in manner such that the contents in a domain are only visible within the boundaries of the domain. Data from one domain is not visible to users in other domains. Only the SuperAdmin user can create new domains and can view and edit information from all the domains in the system. All other admin users of each domain have the privilege of managing their own domains in GMS.

Topics:

About Domains

In addition to a built-in LocalDomain with a LocalAuthServer for authentication of users, GMS is able to access and authenticate against popular third-party systems including Active Directory, RADIUS and LDAP in a transparent fashion. By default, GMS maintains its own locally stored database for authentication purposes. This is also referred to as the "LocalAuthServer." GMS also allows simultaneous third-party database authentication that makes use of your existing (and separately maintained) database system(s).

> **NOTE:** Although GMS supports the use of multiple external authentication mechanisms for a single domain, only one instance of a local GMS authentication server — the default GMS "LocalAuthServer" — can exist for each domain.

The user hierarchy of your database (either GMS or third-party) determines what a user's view consists of, and what data they are able to access and/or modify. In the case of Active Directory servers, GMS has the ability to limit access to only specified groups of users. If this functionality is desired, the target groups must be specified.

Creating a New Domain

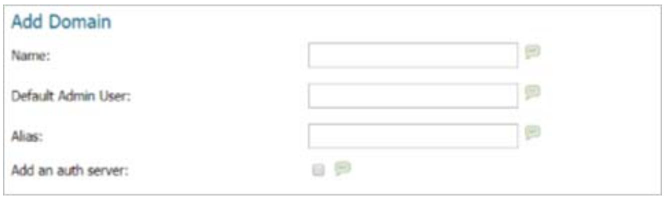
By default, a GMS domain stores user account/passwords/permissions locally inside the GMS database. When users attempt to access resources in GMS, they are authenticated against this local database that determines what their view consists of and data they are able to access and/or modify.

The following procedures assist you in creating a new domain, including configuring that domain to use LDAP/AD/RADIUS for authentication, if required.

> **NOTE:** Every instance of GMS installs with a default domain, named "LocalDomain" even before a domain is created by the administrator. Users of new admin-created domains do not have the ability to view data in other domains.

To create a new domain:

1. Login as the Administrator of the LocalDomain on the SonicWall GMS Login Screen.
2. Navigate to the **CONSOLE | Management** > **Domains** page. You will see a default *LocalDomain*. To create a new domain in SonicWall GMS, click **Add Domain** to complete the configuration parameters for the new remote domain.



Add Domain

Name:

Default Admin User:

Alias:

Add an auth server: □

3. Under **Name**, type in the desired name for the remote domain. This name is visible on the *Domain* pull-down list on the SonicWall GMS Login screen.
4. For **Default Admin User**, specify a valid user account -- this is the default admin account created for the domain. Note that this username must exist in your third-party server, and has administrative privileges in GMS for the newly created domain.
5. Enter a friendly name, or **Alias** for this new Domain.

6 Check the **Add an auth server** option to enable third-party authentication for this domain.

> ⓘ **NOTE:** If your new domain uses only local (GMS) database for user authentication, configuration is complete after this step.If you are planning to authenticate using an existing third-party database, continue to Configuring LDAP or AD Authentication on page 45.

Configuring LDAP or AD Authentication

If you are configuring this domain for use with external LDAP or AD authentication, complete the following steps:

1 Be sure to complete the basic setup procedures in Creating a New Domain on page 44 before continuing.

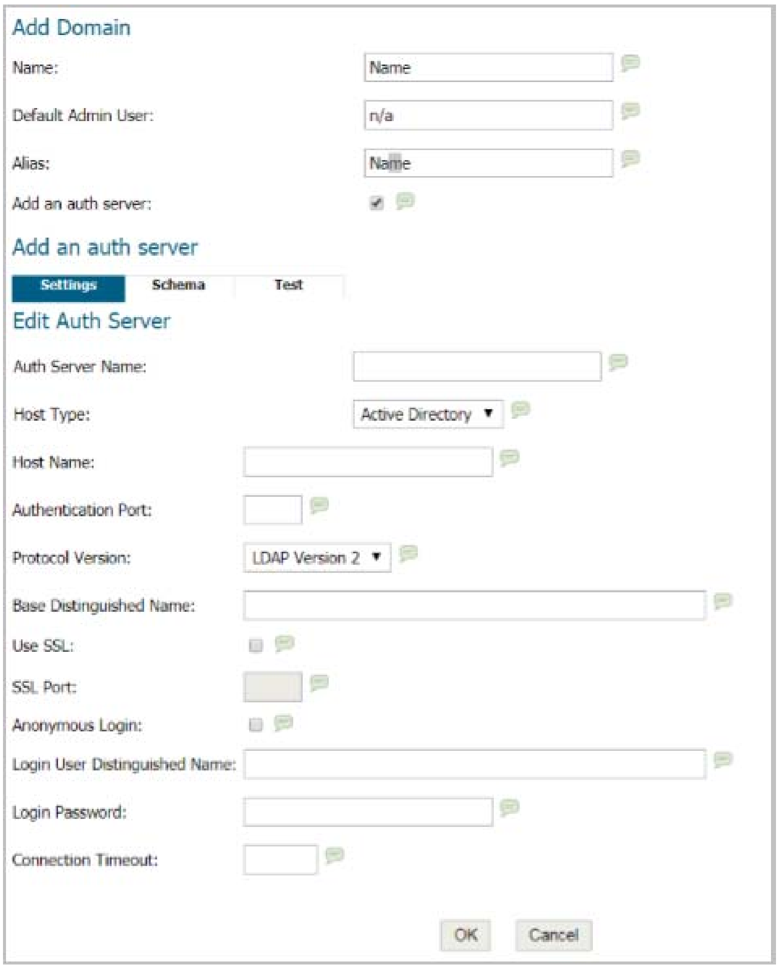
2 Enter a descriptive name of the Auth Server that would be created. This name will be useful in manage the different authentication servers in the domain.

3 Select the **Host Type**. Choose between LDAP server or a RADIUS server.

4 The **Host Name** can either be specified as the IP Address of the remote server, or the fully-qualified domain name. This field can accept/display IPv4 and IPv6 addresses.
The authentication server's Global Catalog can be set as a **Host** in case of a complex directory structure. If using the Global Catalog, SonicWall GMS is able to search through the directory and through all its children nodes.

5 In the **Authentication Port** field, specify the value of the port number on which the third-party server listens for authentication requests.

> ⓘ **NOTE:** The default Authentication Port for LDAP or AD servers is 389. To reach an AD server's global catalog, use port 3268.



Add Domain

Name:	Name
Default Admin User:	n/a
Alias:	Name
Add an auth server:	☑

Add an auth server

Edit Auth Server

Auth Server Name:	
Host Type:	Active Directory ▾
Host Name:	
Authentication Port:	
Protocol Version:	LDAP Version 2 ▾
Base Distinguished Name:	
Use SSL:	□
SSL Port:	
Anonymous Login:	□
Login User Distinguished Name:	
Login Password:	
Connection Timeout:	

6 Select which **Protocol Version** the remote server is running on.

7 The **Base Distinguished Name (Base DN)** is used to identify the root entry in the directory from which SonicWall GMS will execute searches. This should be the node in the authentication system under which all SonicWall GMS users are present. The value is specified as a *distinguished name* (for example, dc=gmseng,dc=com).

8 Click **Use SSL** to use SSL when connecting to the remote server. If you check this check box, you will need to specify the SSL Port on which the remote server is listening for bind requests. By default, this is 636. If connecting to an AD server's global catalog, use port 3269.

> ⓘ **NOTE:** SonicWall recommends using SSL with remote domains. The Certificate Authority (CA) or Root certificate of the LDAP server needs to be imported into GMS JRE using the keytool command.

9 Only select **Anonymous Login** if the authentication system is configured to allow anonymous binds. This option makes the Admin User ID irrelevant. This is not a recommended setting as it reduces security.

10 The **Login User Distinguished Name** is used to authenticate to the third-party server when completing the initial bind. This value is specified as a distinguished name. Type in the matching password for the **Login Password** field.

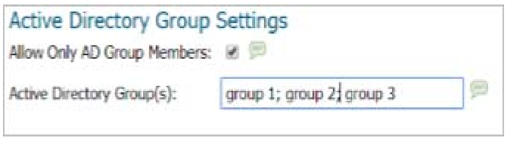
> ⓘ **NOTE:** The Login User Distinguished Name need not correspond with the Admin User ID, but both must exist in the third-party server. The Login User Distinguished Name can be found using any LDAP Browser Tool.

11 In the **Connection Timeout** field, specify the connection timeout period (in milliseconds). After the **Settings** screen is completed, click the **Schema** screen to continue setup of the new remote domain.

12 Under **LDAP Schema**, select which LDAP Server you are using from the pull-down list. Each selection in this list fills in the remaining fields on the Schema screen with default values.

> ⓘ **NOTE:** If the server you are using is not specified in the default list, click **User Defined** to configure your own values and settings.

13 Optional, for AD servers only: Select **Allow Only AD Group Members**. Then specify which groups are allowed to login to GMS from this remote domain. Multiple groups can be specified if they are separated by a semi-colon. All users that are members of the specified AD group must be present below the **Base DN** that was specified in the settings pane.



Active Directory Group Settings

Allow Only AD Group Members: ☑

Active Directory Group(s): group 1; group 2; group 3

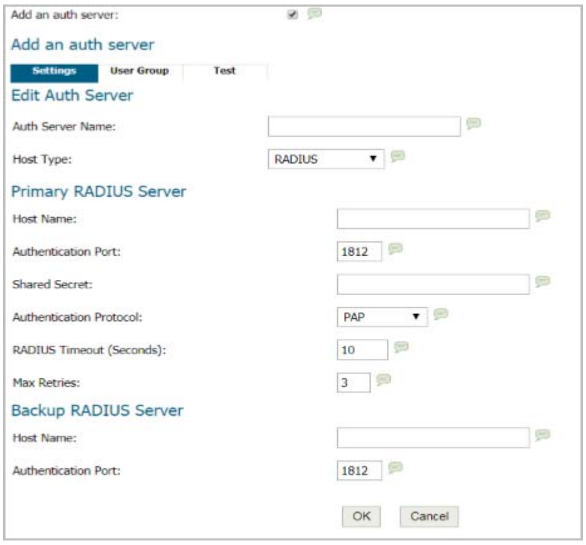
14 Click **OK**.

Configuring RADIUS Authentication

Configure a RADIUS server for authentication in your domain:

Be sure to complete the basic setup procedures in Creating a New Domain on page 44 before continuing.

Configuring the Settings Page



Add an auth server: ☑

Add an auth server

Edit Auth Server

Auth Server Name:

Host Type: RADIUS

Primary RADIUS Server

Host Name:

Authentication Port: 1812

Shared Secret:

Authentication Protocol: PAP

RADIUS Timeout (Seconds): 10

Max Retries: 3

Backup RADIUS Server

Host Name:

Authentication Port: 1812

1 Check the **Add an auth server** option to enable authentication by a third-party server.

2 Enter a descriptive name of the Auth Server that would be created. This name will be useful in managing the different authentication servers in the domain.

3 Choose RADIUS as the **Host Type**.

4 Enter the **Host Name** (or IP address) of the RADIUS server you wish to use for authentication.

5 Enter the **Authentication Port** on which the RADIUS server listens for requests. The default Authentication Port is 1812.

6 Enter the **Shared Secret** to be used between GMS the RADIUS server.

7 Enter the Authentication Protocol used by your RADIUS installation.

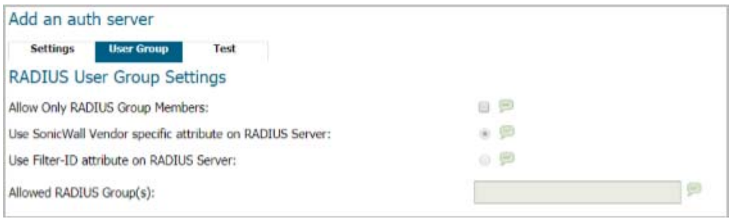
> **NOTE:** SonicWall GMS supports PAP, CHAP, MSCHAP, and MSCHAPv2 protocols for RADIUS authentication.

8 Enter the **RADIUS Timeout (Seconds)**, this specifies the amount of time GMS waits before giving up — or retrying — the authentication attempt. The number of retries is specified next. The default value is 10 seconds.

9 Enter the **Max Retries**, this specifies the number of times GMS attempts to authenticate with the RADIUS server before aborting the attempt. The default value is three tries.

10 Fill in the **Host Name**, **Authentication Port**, and **Shared Secret** values for your backup RADIUS server, if available.

Configuring the User Groups Tab



Add an auth server

RADIUS User Group Settings

Allow Only RADIUS Group Members: □

Use SonicWall Vendor specific attribute on RADIUS Server: ●

Use Filter-ID attribute on RADIUS Server: ○

Allowed RADIUS Group(s):

11 Check the **Allow Only Radius Group Members** option if you plan to limit GMS access to members of select groups. The specific groups are specified later in this tab.

12 If configured, select the **Use SonicWall Vendor specific attribute on RADIUS Server** option to use SonicWall-user-group, and SonicWall-user-groups as RADIUS user group identifiers for GMS authentication.

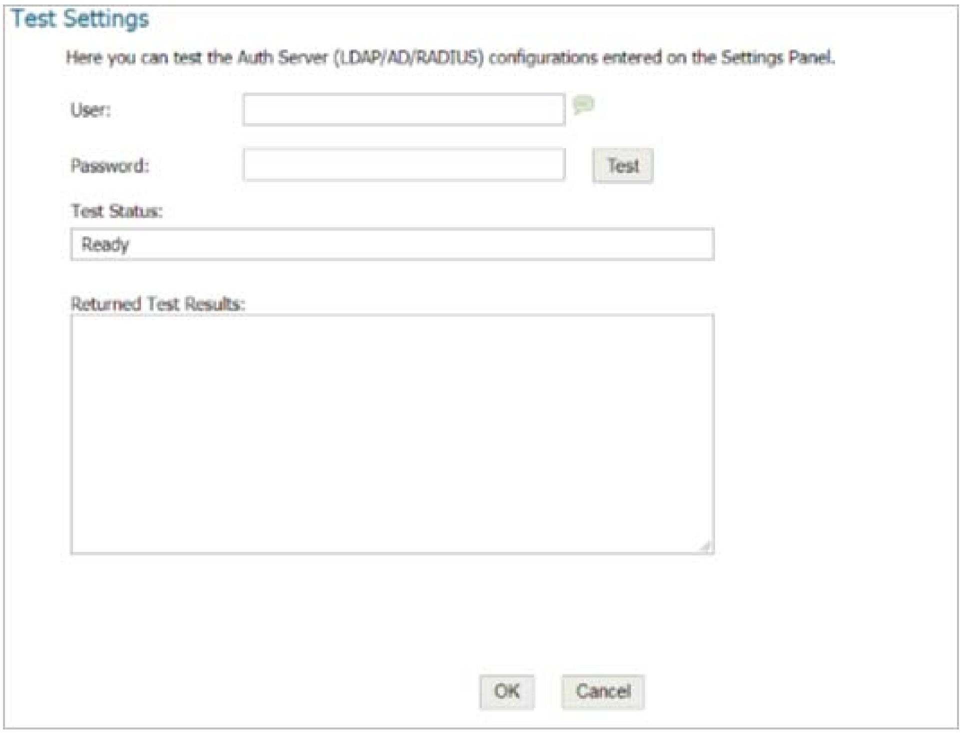
13 If the RADIUS server is configured to return the ‘Filter-ID’ attribute with each user ID, select the **Use Filter-ID attribute on RADIUS Server** option. Henceforth, this value is used as the RADIUS user group identifier.

14 Enter the **Allowed RADIUS Group(s)**, separated by a semi-colon “;”. This field specifies groups, the members of which are allowed to access GMS resources.

Verifying Administrator Third-party Authentication Configuration

On the Add Domain page, select the **Test** page to test and verify the remote domain configurations entered on the **Settings** screen. If there are any errors in your configurations, this screen alerts you and provides information on how to correct them.

To test the third-party authentication feature, specify the credentials of any user in the domain and click **Test**.



Test Settings

Here you can test the Auth Server (LDAP/AD/RADIUS) configurations entered on the Settings Panel.

User:

Password:

Test Status: Ready

Returned Test Results:

You will also see the new domain (local and remote) you have created under **CONSOLE | Management > Domains.** To confirm the configurations for each domain, click the ✎ icon to view or change these settings.

Verifying Third-Party Authentication Server Configuration

If the login was successful, the user is automatically directed to the SonicWall GMS Dashboard default page. At the top of the page, SonicWall GMS no longer displays the user's status as Guest.

Editing a Domain

Any admin-created domain can be edited after initial creation.

To edit a domain:

1. Log in as the Administrator of the LocalDomain on the SonicWall GMS Login Screen.
2. Navigate to the **CONSOLE | Management > Domain** page**.** To delete a domain in SonicWall GMS, select the check box corresponding to the domain you wish to delete and click the **Edit Domain** icon.

ⓘ | **NOTE:** The default LocalDomain which comes pre-installed with GMS systems cannot be edited or deleted.

Users

To operate in complex environments, GMS is designed to support multiple users, each with his or her own set of permissions and access rights.

Topics:

ⓘ **NOTE:** If you do not want to restrict access to SonicWall appliances or SonicWall GMS functions, but want to divide SonicWall GMS 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 complete, users can switch between these views as often as necessary. For more information, refer to Configuring Action Permissions on page 55.

ⓘ **NOTE:** All of the user configuration options are available through the command-line interface. For more information, refer to the *GMS Command-Line Interface Guide*.

Creating User Groups

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

GMS provides three pre-configured groups:

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

To create a new group, complete the following steps:

1. Navigate to **CONSOLE | Management > Users.** The General tab on the User screen displays.
2. In the middle pane, right-click **End Users** and select **Add User** from the pop-up menu. The Add User dialog box displays.
3. In the dialog box, enter the name of the new user, a password, confirm the password, and then click **OK**. The new user is added to the list under End Users.
4. In the right pane, enter any comments regarding the new user group in the **Comments** field.
5. Select a default view for the new user group from the **Default View** pull-down menu. This view is displayed for members of the user group when they first log in to GMS.
6. To force all users in the user group to change their passwords, select **Change Password**.
7. To delete the user when they become inactive, select **Delete Inactive**.
8. To set a date when the user type will become inactive, click in the **Active Until** field and then select a date from the popup calendar.
9. To keep the user type active at all times without an end date, select **Always Active**.
10. Select the schedule for when the user group is active from the pull-down list in the **Schedule** field.

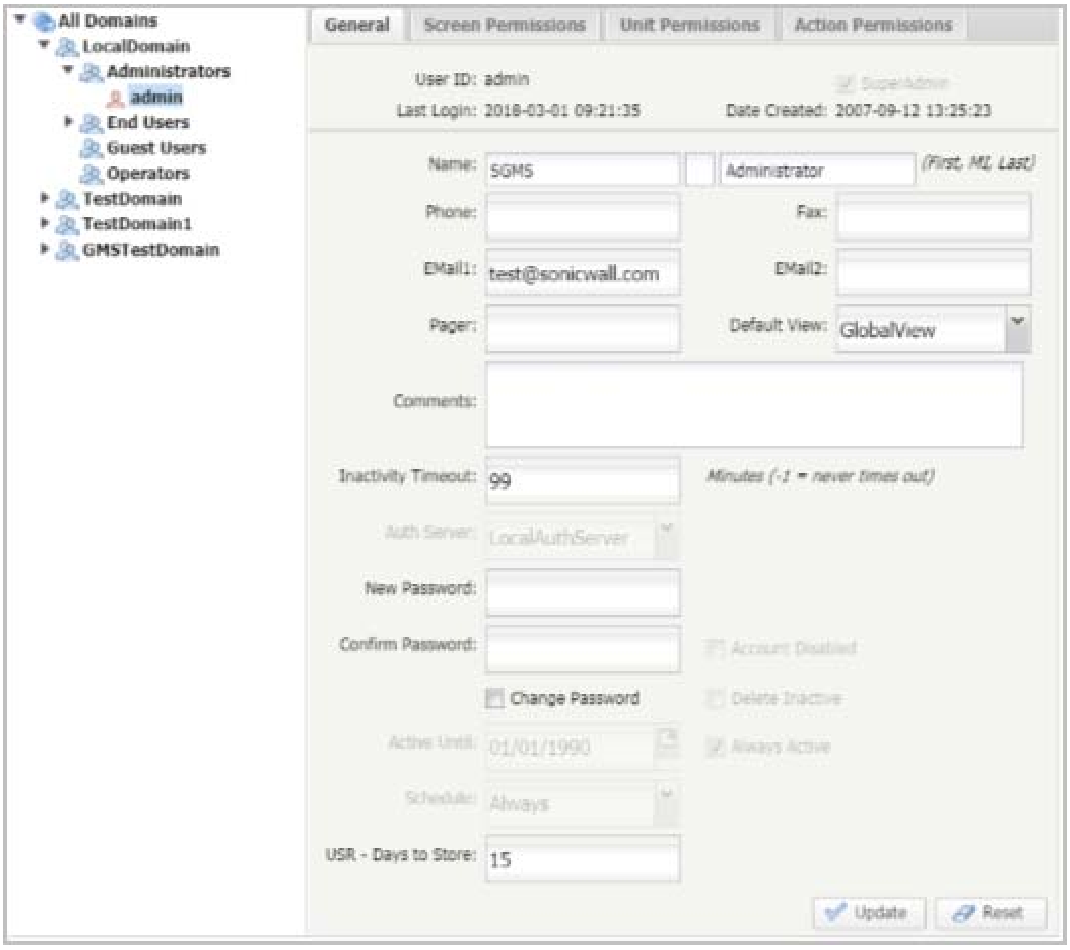
11 Click **Update**. The new user group is added. By default, the new group has no privileges. To configure screen access settings, refer to Moving a User on page 52.

Adding Users

This section describes how to create a new user. Although the user inherits all group settings, individual user settings overrides the group settings.

To add a new user, complete the following steps:

1 Navigate to **CONSOLE | Management > Users.** The General Page of the User configuration screen displays.



User ID: admin

☑ Super Admin

Last Login: 2018-03-01 09:21:35

Date Created: 2007-09-12 13:25:23

Name: SGMS Administrator (First, MI, Last)

Phone:

Fax:

EMail1: test@sonicwall.com

EMail2:

Pager:

Default View: GlobalView

Comments:

Inactivity Timeout: 99 Minutes (-1 = never times out)

Auth Server: LocalAuthServer

New Password:

Confirm Password:

□ Account Disabled

□ Change Password

□ Delete Inactive

Active Until: 01/01/1990

☑ Always Active

Schedule: Always

USR - Days to Store: 15

2 In the middle pane, right-click **Administrators**, **End Users, or Guest Users** and select **Add User** from the pop-up menu. The Add User dialog box displays.

3 In the dialog box, enter the name of the new user, a password, confirm the password, and then click **OK**. The new user is added to the list under End Users.

4 In the right pane, enter any comments regarding the new user group in the **Comments** field.

5 Select a default view for the new user group from the **Default View** pull-down menu. This view is displayed for members of the user group when they first log in to GMS.

6 To force all users in the user group to change their passwords, select **Change Password**.

7 To delete the user when they become inactive, select **Delete Inactive**.

8 To set a date when the user type will become inactive, click in the **Active Until** field and then select a date from the popup calendar.

9 To keep the user type active at all times without an end date, select **Always Active**.

10 Select the schedule for when the user group is active from the pull-down list in the **Schedule** field.

11 Click **Update**. The new user group is added. By default, the new group has no privileges. To configure screen access settings, refer to Moving a User on page 52.

12 From the **General** tab, select the new user.

13 Enter the full name of the user in the **Name** field.

14 Enter contact information for the user in the **Phone**, **Fax**, **Pager**, and **Email** fields.

15 Select the default view for the user from the **Default View** list box.

16 Enter any comments regarding the new user in the **Comments** field.

17 Check **SuperAdmin** to enable privileges for this user across all domains.

> ⓘ **NOTE:** By default, permissions for users exist only within the domain to which they belong. By checking the SuperAdmin option, permissions are extended across all domains.

18 Enter the number of minutes that the user can be inactive on his computer before the session times out in the **Inactivity Timeout** field. Enter **-1** to never time out.

19 To change the password for the user, type in the password in the **New Password** field, and then type it again in **Confirm Password**.

20 To disable the user without deleting the entire entry, select **Account Disabled**.

21 To force the user to change his password, select **Change Password**.

22 To delete the user when the account becomes inactive, select **Delete Inactive**.

23 To set a date when the user becomes inactive, click in the **Active Until** field and select a date from the popup calendar.

24 To keep the user active without an end date, select **Always Active**. If this is selected, the date in the **Active Until** field is ignored.

25 Select a schedule when the user is active from the pull-down list in the **Schedule** field.

26 Do one of the following:

- Click **Inherit Permissions from Group**. The user inherits the permissions from the group that you right-clicked to begin this procedure.
- Click **Update**. The new user is added. You must configure the user's permissions. See Moving a User on page 52 and Configuring Appliance Access on page 54.
- Click **Reset** to change all fields in this screen to their default values and start over.

> ⓘ **NOTE:** To temporarily disable a user account, select **Account Disabled** and click **Update**.

Moving a User

When new users log in to SonicWall GMS for the first time, they are considered guest users and have only limited access.

To change a SonicWall GMS user's group:

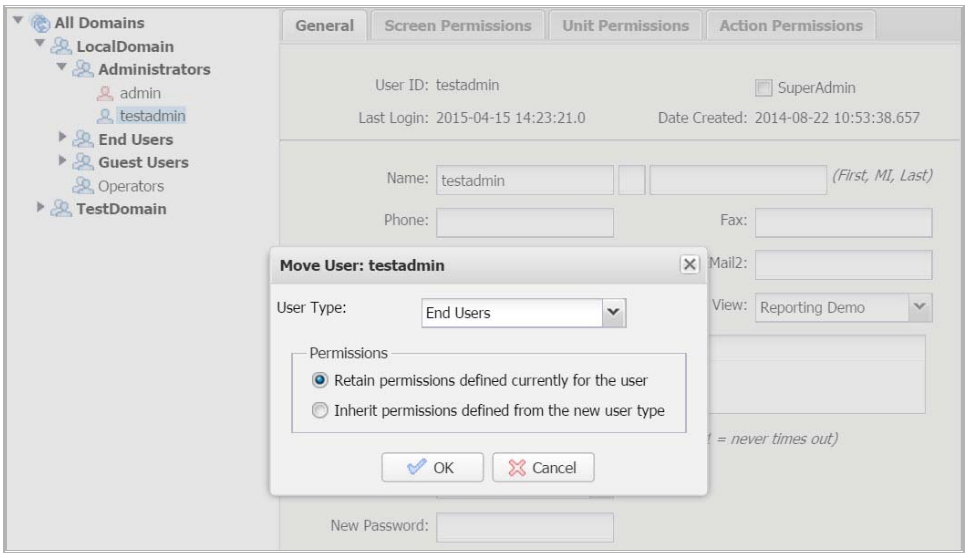
1 Log in as the remote domain's administrator.

2 Navigate to **CONSOLE | Management > Users**. The Users page appears.

3 Select the user to be moved from the user list.

4 Right-click the user's name in the user list and select **Move User** from the context menu.

5 In the **Move User** dialog box, select the appropriate new level for the new user, and select **Inherit permissions defined from the new user type** permission.



User ID: testadmin

□ SuperAdmin

Last Login: 2015-04-15 14:23:21.0

Date Created: 2014-08-22 10:53:38.657

Name: testadmin (First, MI, Last)

Phone:

Fax:

Mail2:

View: Reporting Demo

= never times out)

New Password:

Move User: testadmin

User Type: End Users

Permissions

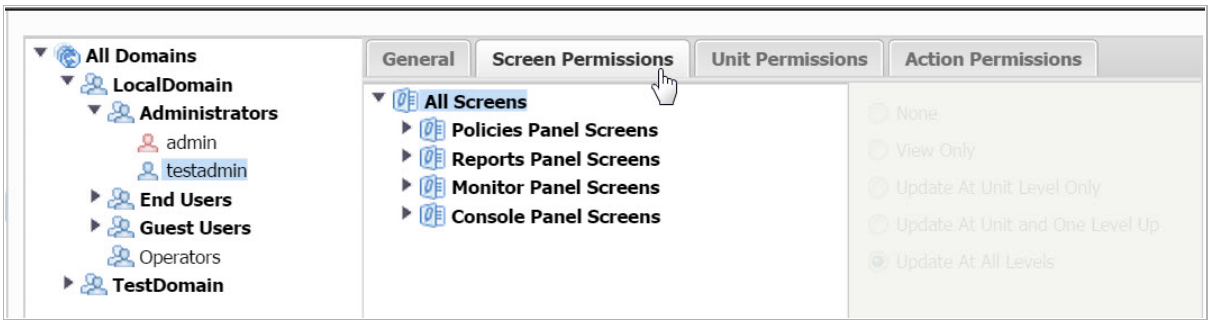
● Retain permissions defined currently for the user

○ Inherit permissions defined from the new user type

6 Click **OK**.

Configuring Screen Access

The Screen Permissions page contains a hierarchical list of all screens that appear within GMS. 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.



○ None

○ View Only

○ Update At Unit Level Only

○ Update At Unit and One Level Up

● Update At All Levels

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

To configure screen access settings for a user or user group, complete the following steps:

1 Navigate to **CONSOLE | Management** > **Users**. The Users configuration page appears.

2 Select a user or user group under **All Users**.

3 Click the **Screen Permissions** tab.

4 Under **All Screens**, select a panel, section, or screen. For example, for REPORTS_PANEL, you can select the whole panel, the unit type section such as Firewall, SMA, or Email Security (ES), 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**.

The panel object is now preceded by a ☑.

> **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 Appliance Access

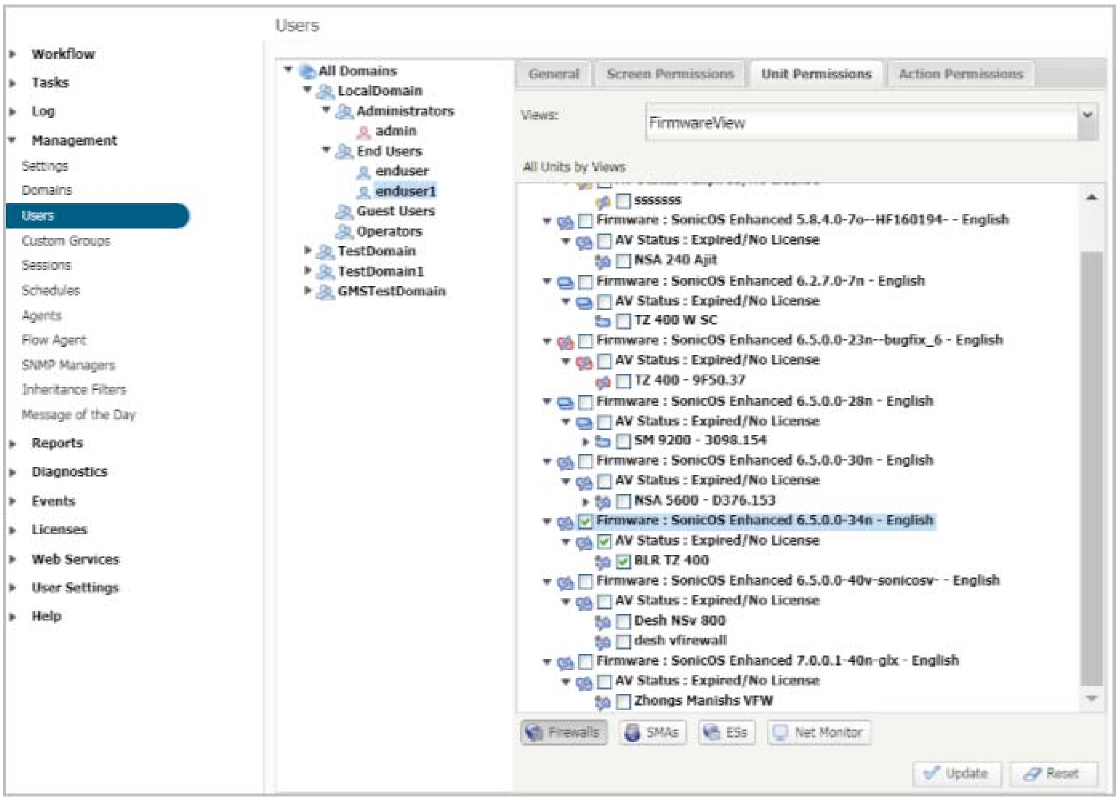
The Appliance Permissions page contains a hierarchical list of all SonicWall appliances that appear within GMS. From this screen, you can control access to SonicWall groups or individual SonicWall appliances.

To configure appliance access settings for a user, complete the following steps:

1 Navigate to **CONSOLE | Management** > **Users**. The Users configuration page appears.

2 Select a user.

3 Click the **Unit Permissions** tab.


Users
Workflow
Tasks
Log
Management
Settings
Domains
Users
Custom Groups
Sessions
Schedules
Agents
Flow Agent
SNMP Managers
Inheritance Filters
Message of the Day
Reports
Diagnostics
Events
Licenses
Web Services
User Settings
Help
All Domains
LocalDomain
Administrators
admin
End Users
enduser
enduser1
Guest Users
Operators
TestDomain
TestDomain1
GMSTestDomain
General
Screen Permissions
Unit Permissions
Action Permissions
All Units by Views
□ sssssss
□ Firmware : SonicOS Enhanced 5.8.4.0-7o--HF160194- - English
□ AV Status : Expired/No License
□ NSA 240 Ajit
□ Firmware : SonicOS Enhanced 6.2.7.0-7n - English
□ AV Status : Expired/No License
□ TZ 400 W SC
□ Firmware : SonicOS Enhanced 6.5.0.0-23n--bugfix_6 - English
□ AV Status : Expired/No License
□ TZ 400 - 9F50.37
□ Firmware : SonicOS Enhanced 6.5.0.0-28n - English
□ AV Status : Expired/No License
□ SM 9200 - 3098.154
□ Firmware : SonicOS Enhanced 6.5.0.0-30n - English
□ AV Status : Expired/No License
□ NSA 5600 - D376.153
☑ Firmware : SonicOS Enhanced 6.5.0.0-34n - English
☑ AV Status : Expired/No License
☑ BLR TZ 400
□ Firmware : SonicOS Enhanced 6.5.0.0-40v-sonicosv- - English
□ AV Status : Expired/No License
□ Desh NSv 800
□ desh vfirewall
□ Firmware : SonicOS Enhanced 7.0.0.1-40n-glx - English
□ AV Status : Expired/No License
□ Zhongs Manishs VFW
Firewalls
SMAs
ESs
Net Monitor
Update
Reset

Views: FirmwareView

4 Select a View from the **Views** pull-down menu.

5 To provide the user with access to a SonicWall group or appliance, select 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, deselect 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

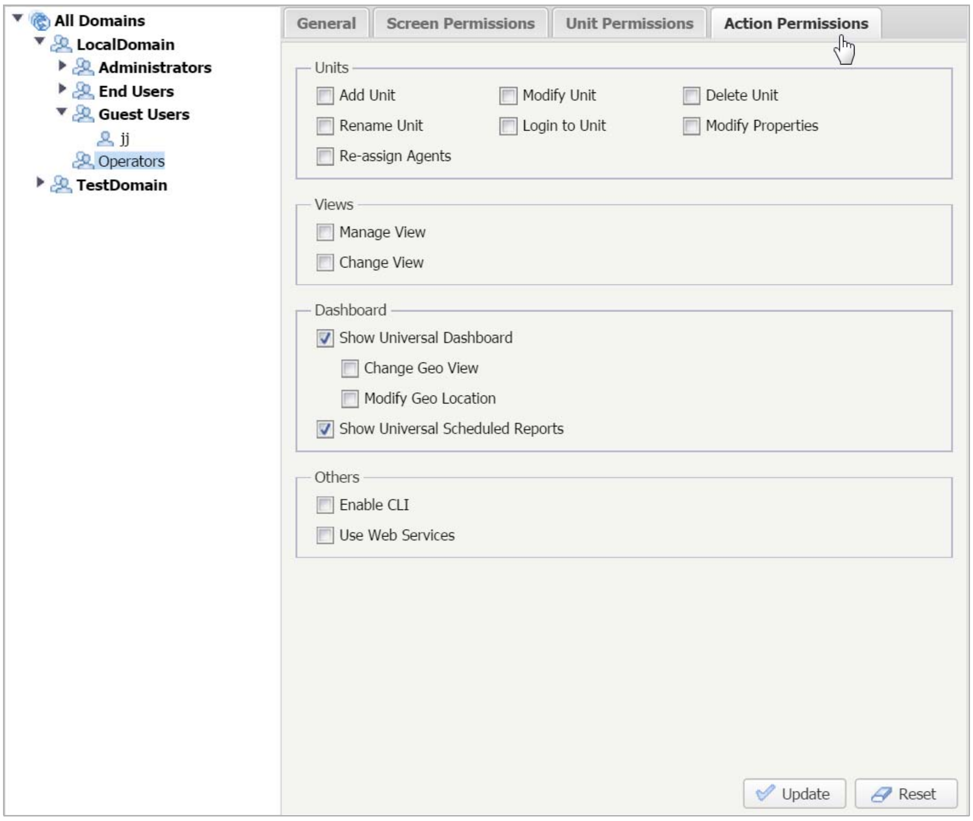
The Action Permissions tab contains a list of action and view options that can be enabled/disabled for a group or user.

To configure the action permissions, complete the following steps:

1 Navigate to **CONSOLE | Management > Users**. The Users page appears.

2 Select the user or group.

3 Click the **Action Permissions** tab.



Units

□ Add Unit □ Modify Unit □ Delete Unit

□ Rename Unit □ Login to Unit □ Modify Properties

□ Re-assign Agents

Views

□ Manage View

□ Change View

Dashboard

☑ Show Universal Dashboard

□ Change Geo View

□ Modify Geo Location

☑ Show Universal Scheduled Reports

Others

□ Enable CLI

□ Use Web Services

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 GMS management specifications of managed units.
Rename Unit	Renames the unit.
Login to Unit	Gains access to the managed unit’s interface through the GMS.
Modify Properties	Modifies the properties of the managed units.
Re-assign Agents	Moves units between the agents.

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 Select the **Dashboard** options for the group or user.

Available Dashboard Options

Name	Description
Show Universal Dashboard	Makes the Universal Dashboard visible to the selected user or group.
Change Geo View	Changes the Geo view of the Dashboard map.
Modify Geo Location	Changes the location of the view on the Dashboard map.
Show Universal Scheduled Reports	Makes the Universal Scheduled Reports available to the selected user or group.

7 Select any remaining options for the group or user in the **Others** section.

Other Options

Name	Description
Enable CLI	Manage using the command line interface (CLI).
Use Web Services	Configure and use the Web Services feature.

8 Click **Update**.

Custom Groups

The GMS 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

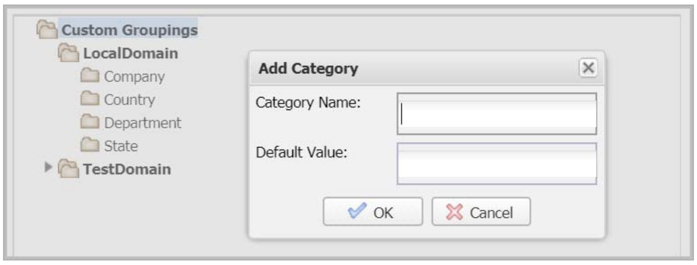
When first configuring GMS, you must create custom fields that are entered for each SonicWall appliance. GMS supports up to ten custom fields.

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

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

To add fields, complete the following steps:

1 Navigate to **CONSOLE | Management > Custom Groups**. The Custom Groups page appears.



Category Name:

Default Value:

2 Right-click **Custom Groupings** in the right pane.

3 Select **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 Group** 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 on page 55.

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

Configuring Management Sessions

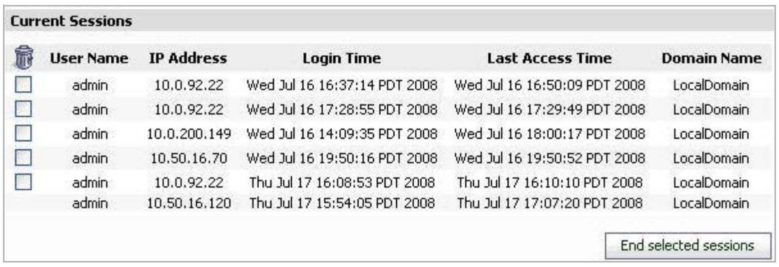
The Sessions page of the Management section of the GMS Console allows you to view session statistics for currently logged in GMS users and to end selected sessions.

Managing Sessions

On occasion, it might be necessary to log off other user sessions.

To do this, complete the following steps:

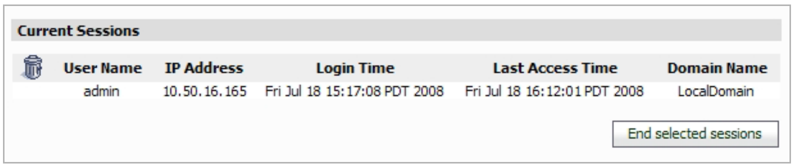
1 Navigate to **CONSOLE | Management > Sessions**. The Sessions page displays.



Current Sessions

	User Name	IP Address	Login Time	Last Access Time	Domain Name
□	admin	10.0.92.22	Wed Jul 16 16:37:14 PDT 2008	Wed Jul 16 16:50:09 PDT 2008	LocalDomain
□	admin	10.0.92.22	Wed Jul 16 17:28:55 PDT 2008	Wed Jul 16 17:29:49 PDT 2008	LocalDomain
□	admin	10.0.200.149	Wed Jul 16 14:09:35 PDT 2008	Wed Jul 16 18:00:17 PDT 2008	LocalDomain
□	admin	10.50.16.70	Wed Jul 16 19:50:16 PDT 2008	Wed Jul 16 19:50:52 PDT 2008	LocalDomain
□	admin	10.0.92.22	Thu Jul 17 16:08:53 PDT 2008	Thu Jul 17 16:10:10 PDT 2008	LocalDomain
	admin	10.50.16.120	Thu Jul 17 15:54:05 PDT 2008	Thu Jul 17 17:07:20 PDT 2008	LocalDomain

2 When more than one session is active, a check box is displayed next to each row. Select the check box of each user to log off and click **End selected sessions**. The selected users are logged off.



Current Sessions

	User Name	IP Address	Login Time	Last Access Time	Domain Name
	admin	10.50.16.165	Fri Jul 18 15:17:08 PDT 2008	Fri Jul 18 16:12:01 PDT 2008	LocalDomain

NOTE: This page can accept/display IPv4 and IPv6 addresses.

Schedules and Group Schedules

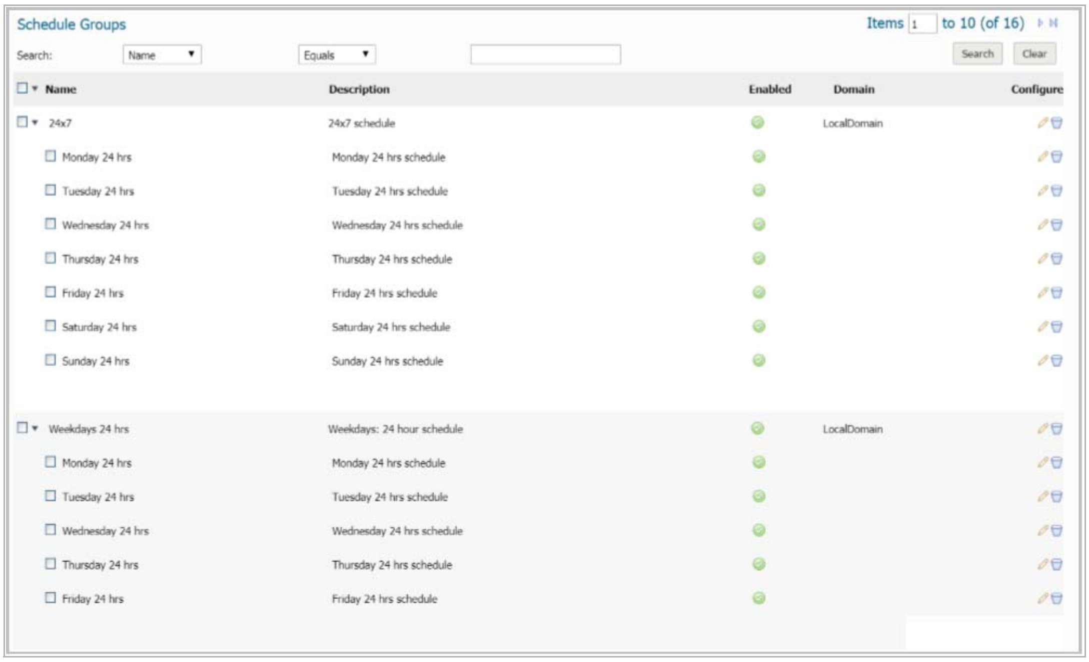
The Schedules page allows you to create and manage schedules and schedule groups for enforcing schedule times.

Topics:

- Managing Group Schedules on page 59
- Managing Schedules on page 62

Managing Group Schedules

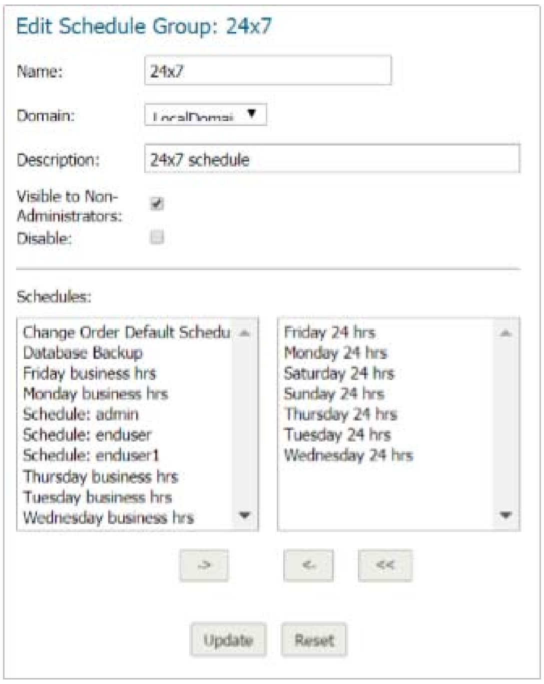
The Group Schedules table displays all your predefined and custom schedules. In the Group Schedules table, there are four default group schedules from which to choose: **Daily 24x7**, **Weekdays 24x7**, **8x5 Work Hours**, and **Weekend Hours**.



□ ▾ Name	Description	Enabled	Domain	Configure
□ ▾ 24x7	24x7 schedule	●	LocalDomain	✎ 🗑
□ Monday 24 hrs	Monday 24 hrs schedule	●		✎ 🗑
□ Tuesday 24 hrs	Tuesday 24 hrs schedule	●		✎ 🗑
□ Wednesday 24 hrs	Wednesday 24 hrs schedule	●		✎ 🗑
□ Thursday 24 hrs	Thursday 24 hrs schedule	●		✎ 🗑
□ Friday 24 hrs	Friday 24 hrs schedule	●		✎ 🗑
□ Saturday 24 hrs	Saturday 24 hrs schedule	●		✎ 🗑
□ Sunday 24 hrs	Sunday 24 hrs schedule	●		✎ 🗑
□ ▾ Weekdays 24 hrs	Weekdays: 24 hour schedule	●	LocalDomain	✎ 🗑
□ Monday 24 hrs	Monday 24 hrs schedule	●		✎ 🗑
□ Tuesday 24 hrs	Tuesday 24 hrs schedule	●		✎ 🗑
□ Wednesday 24 hrs	Wednesday 24 hrs schedule	●		✎ 🗑
□ Thursday 24 hrs	Thursday 24 hrs schedule	●		✎ 🗑
□ Friday 24 hrs	Friday 24 hrs schedule	●		✎ 🗑

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.



Edit Schedule Group: 24x7

Name: 24x7

Domain: LocalDomai

Description: 24x7 schedule

Visible to Non-Administrators: ☑

Disable: □

Schedules:

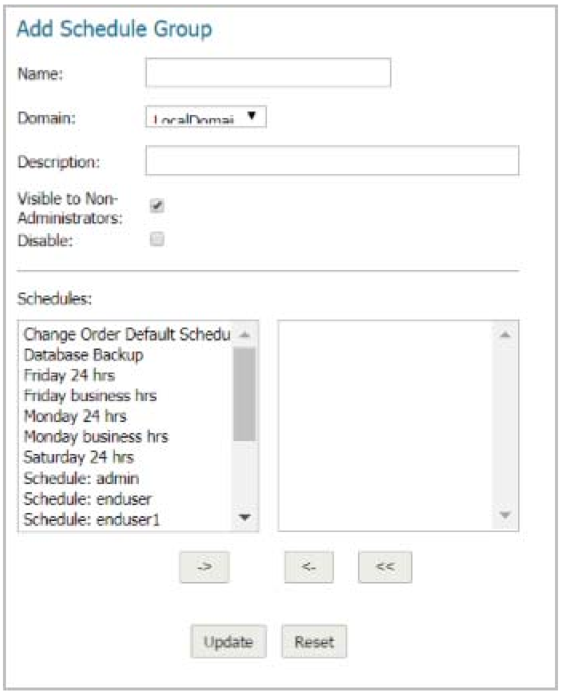
Change Order Default Schedu
Database Backup
Friday business hrs
Monday business hrs
Schedule: admin
Schedule: enduser
Schedule: enduser1
Thursday business hrs
Tuesday business hrs
Wednesday business hrs

Friday 24 hrs
Monday 24 hrs
Saturday 24 hrs
Sunday 24 hrs
Thursday 24 hrs
Tuesday 24 hrs
Wednesday 24 hrs

Adding Schedule Groups

To add a schedule group, complete the following steps:

1 Navigate to **CONSOLE | Management > Schedules** and click **Add Schedule Group**. The **Add Schedule Group** page is displayed.



Add Schedule Group

Name:

Domain: LocalDomai

Description:

Visible to Non-Administrators: ☑

Disable: □

Schedules:

Change Order Default Schedu
Database Backup
Friday 24 hrs
Friday business hrs
Monday 24 hrs
Monday business hrs
Saturday 24 hrs
Schedule: admin
Schedule: enduser
Schedule: enduser1

2 Enter a descriptive name for the group schedule in the **Name** field.

3. Enter a group schedule description in the **Description** field.
4. Click **Visible to Non-Administrators** if you would like to make the schedule viewable by the public.
5. 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.
6. 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 a event schedule group. See Schedules and Group Schedules on page 59.

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.

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

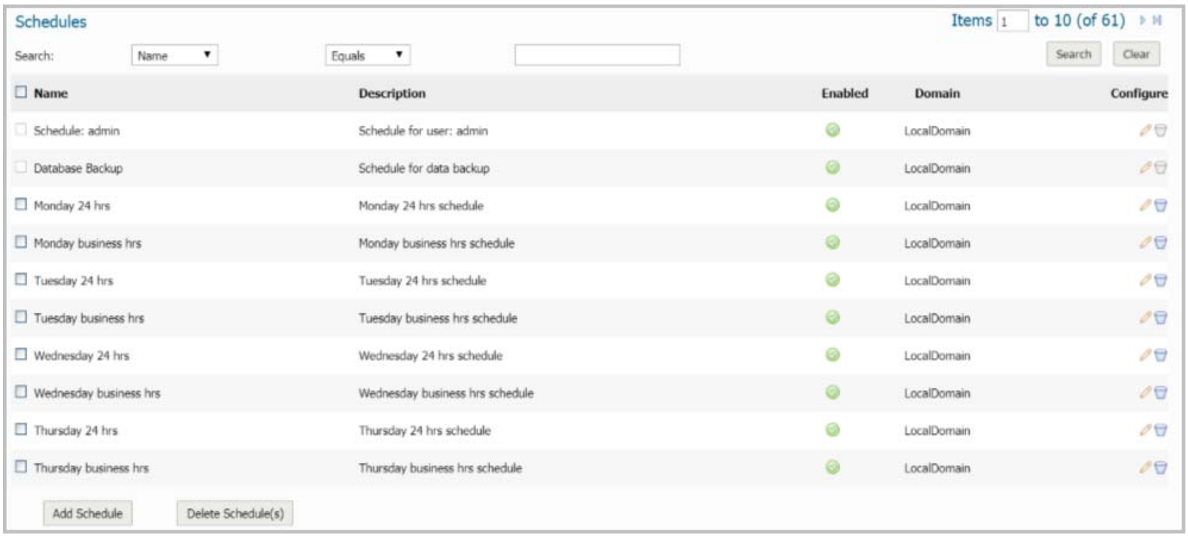
To delete a schedule group, complete the following steps:

1. Navigate to **CONSOLE | 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.



Schedules

Items 1 to 10 (of 61)

Search: Name ▾ Equals ▾ Search Clear

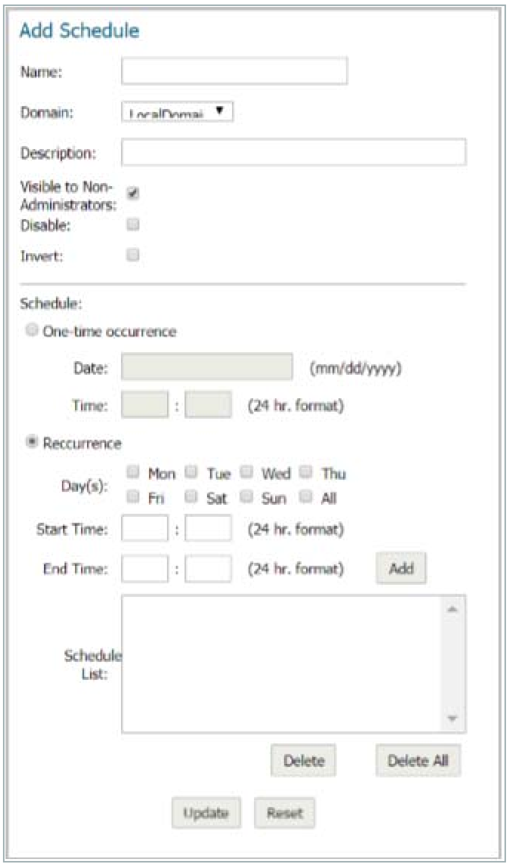
☐ Name	Description	Enabled	Domain	Configure
☐ Schedule: admin	Schedule for user: admin	●	LocalDomain	✎ 🗑
☐ Database Backup	Schedule for data backup	●	LocalDomain	✎ 🗑
☐ Monday 24 hrs	Monday 24 hrs schedule	●	LocalDomain	✎ 🗑
☐ Monday business hrs	Monday business hrs schedule	●	LocalDomain	✎ 🗑
☐ Tuesday 24 hrs	Tuesday 24 hrs schedule	●	LocalDomain	✎ 🗑
☐ Tuesday business hrs	Tuesday business hrs schedule	●	LocalDomain	✎ 🗑
☐ Wednesday 24 hrs	Wednesday 24 hrs schedule	●	LocalDomain	✎ 🗑
☐ Wednesday business hrs	Wednesday business hrs schedule	●	LocalDomain	✎ 🗑
☐ Thursday 24 hrs	Thursday 24 hrs schedule	●	LocalDomain	✎ 🗑
☐ Thursday business hrs	Thursday business hrs schedule	●	LocalDomain	✎ 🗑

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, complete the following steps:

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 on page 62.

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, perform the following steps:

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)**.

Agents

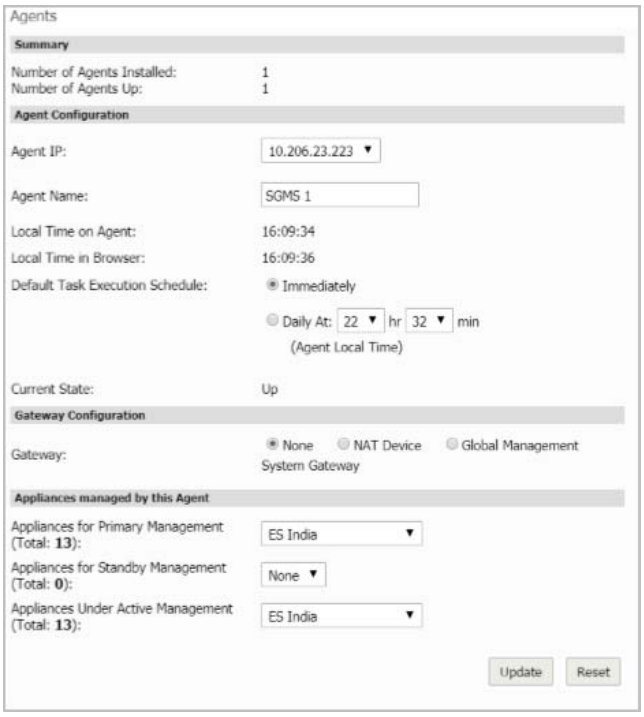
The Agents page provides information for the GMS primary and backup agent servers that are managing the SonicWall appliances. Including a summary of the Agents, Agent configuration, gateway configuration, and appliances managed by the Agent. You can also schedule all the tasks for each agent server to be executed during a specified time period.

ⓘ **NOTE:** This page can be used to remove agents, but they cannot be managing any firewalls.

Managing Agent Configurations

To configure the Agents page, complete the following steps:

1 Navigate to **CONSOLE | Management > Agents**. The Agents page appears.



Agents

Summary

Number of Agents Installed: 1
Number of Agents Up: 1

Agent Configuration

Agent IP: 10.206.23.223 ▼

Agent Name: SGMS 1

Local Time on Agent: 16:09:34
Local Time in Browser: 16:09:36

Default Task Execution Schedule: ● Immediately
○ Daily At: 22 ▼ hr 32 ▼ min
(Agent Local Time)

Current State: Up

Gateway Configuration

Gateway: ● None ○ NAT Device ○ Global Management System Gateway

Appliances managed by this Agent

Appliances for Primary Management (Total: **13**): ES India ▼
Appliances for Standby Management (Total: **0**): None ▼
Appliances Under Active Management (Total: **13**): ES India ▼

The Summary screen displays the number of installed and running agents.

2 In the **Agent Configuration** screen, select the IP address of the Agent you want to view from the **Agent IP** drop-down menu. This field can accept/display IPv4 and IPv6 addresses.

The **Agent Name** text-field populates the name of the selected Agent. The agent name can be modified by editing this text-field.

3 To specify when tasks run, access the **Default Task Execution Schedule** field and select one of the following radio buttons:

- **Immediately**— Runs tasks immediately (selected by default).
- **Daily At**— Provides Hour and Minute drop-down menus to select the start time. The time is based on the GMS appliance’s local time.

4 In the **Gateway Configuration** screen select on of the following radio buttons to configure the gateway for Agents:

- **None**— No gateway is specified. The agent is facing the unit directly without any device between them. If you do not wish to configure a gateway for the Agent, click **None**.
- **NAT Device**— Use this option when a NAT device is configured as the gateway. The GMS appliance does not have to login to the unit for any reason and all NAT configurations are taken care of by the network Administrator directly through the device’s management interface.

To configure the NAT device, complete the following steps:

1 Under Gateway, select the **NAT Device** radio button.

2 Enter the **NAT Device WAN IP** address. This is the external IP address of the device.

3 Enter the **NAT Device Syslog Port**. This is the Syslog port used for Syslogs sent from the managed units.

- **GMS Gateway**— Use this option when a SonicWall device is acting as a Gateway. The GMS appliance needs to be able to login to the unit and pull additional information such as the WAN IP of the device. This type of device is typically used when Units managed by the Agent are either on the management tunnel or an existing tunnel. In the case of SSL, a GMS gateway is really not necessary. Using a SonicWall is recommended, but can be setup as a NAT Device if all units are managed using SSL.

To configure the GMS Gateway, complete the following steps:

1 Under Gateway, select the **GMS Gateway** radio button.

2 Click the **GMS Gateway IP** text-field, then enter the internal IP address of the device.
If you change the GMS gateway IP address or password, you must also change the settings on this page.

3 Click the **GMS Gateway Port** text-field, then enter the management port used to sign into the device.

4 Click the **GMS Gateway Username** text-field, then enter the username used to sign into the device.

5 Click the **GMS Gateway Password** text-field, then enter the password used to sign into the device.

6 Click the **GMS Gateway Syslog Port** text-field, then enter the Syslog port used for syslogs sent from the managed units.

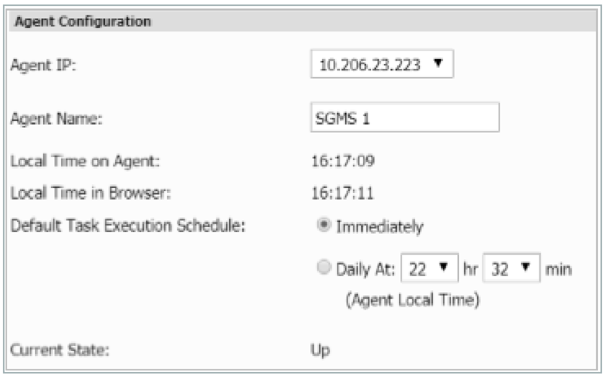
7 For each agent server, the **Firewalls for Primary Management** drop-down menu lists the SonicWall appliances that are assigned to the agent server for primary management. The total number is also displayed.

8 For each agent server, the **Firewalls for Standby Management** drop-down menu lists the SonicWall appliances that are assigned to the agent server for backup management. The total number is also displayed.

9 For each agent server, the **Firewalls Under Active Management** drop-down manu lists the SonicWall appliances that are actively being managed by the agent server. The total number is also displayed.

10 When you are finished, click **Update**. The settings are changed. To clear the settings and start over, click **Reset**.

> **NOTE:** This screen also allows you to hide an Agent from showing up if that Agent is not managing an Appliance that has a current state of **Down**.



Agent Configuration

Agent IP: 10.206.23.223 ▼

Agent Name: SGMS 1

Local Time on Agent: 16:17:09

Local Time in Browser: 16:17:11

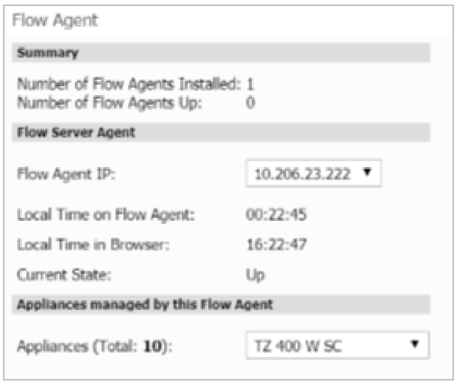
Default Task Execution Schedule: ● Immediately

○ Daily At: 22 ▼ hr 32 ▼ min (Agent Local Time)

Current State: Up

Flow Agent

The Flow Agent page displays a summary of the flow agents and appliances managed by the flow agent, and has flow agent configuration options.



Flow Agent

Summary

Number of Flow Agents Installed: 1
Number of Flow Agents Up: 0

Flow Server Agent

Flow Agent IP: 10.206.23.222 ▼

Local Time on Flow Agent: 00:22:45

Local Time in Browser: 16:22:47

Current State: Up

Appliances managed by this Flow Agent

Appliances (Total: **10**): TZ 400 W SC ▼

Summary

The Flow agent Summary includes the following:

- **Number of Flow Agent Installed**— Displays the number of Flow Agents installed in your deployment.
- **Number of Flow Agent Up**— Displays the number of Flow Agents that are running.

Flow Agent Configuration

The following Flow Agent Configuration options are available:

- **Flow Agent IP**— Displays the Flow Agent IP address. Click the drop-down menu to select a different flow agent.
- **Local Time on Flow Agent** — Displays the local time on the Flow Agent.
- **Local Time in Browser**— Displays the local time from the browser.
- **Current State**— Displays the current state of the Flow Agent.

Appliances Managed by this Flow Agent

The Appliances managed by this Flow Agent section provides the following option:

- **Appliances**— Click the drop-down menu to display a list of appliances managed by the Flow Agent.

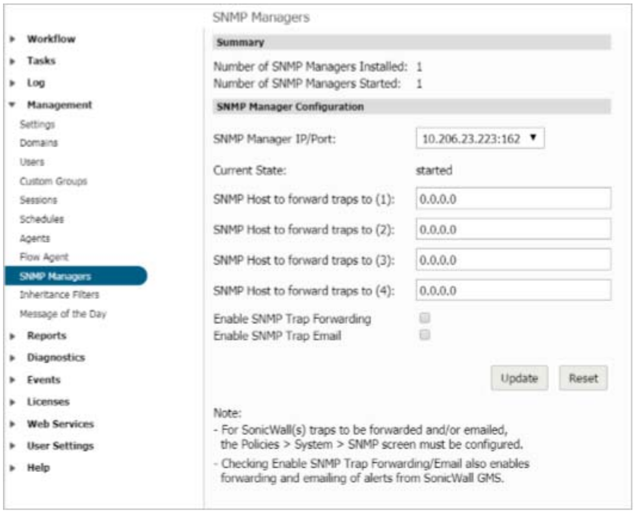
SNMP Managers

The SNMP Managers page enables you to specify SNMP Managers to which GMS sends SNMP Traps.

Configuring SNMP Settings

To configure the SNMP Managers page, complete the following steps:

1 Navigate to **CONSOLE | Management** > **SNMP Managers**. The SNMP Managers page displays.



SNMP Managers

Summary

Number of SNMP Managers Installed: 1
Number of SNMP Managers Started: 1

SNMP Manager Configuration

SNMP Manager IP/Port: 10.206.23.223:162 ▼
Current State: started
SNMP Host to forward traps to (1): 0.0.0.0
SNMP Host to forward traps to (2): 0.0.0.0
SNMP Host to forward traps to (3): 0.0.0.0
SNMP Host to forward traps to (4): 0.0.0.0
Enable SNMP Trap Forwarding □
Enable SNMP Trap Email □

Note:
- For SonicWall(s) traps to be forwarded and/or emailed, the Policies > System > SNMP screen must be configured.
- Checking Enable SNMP Trap Forwarding/Email also enables forwarding and emailing of alerts from SonicWall GMS.

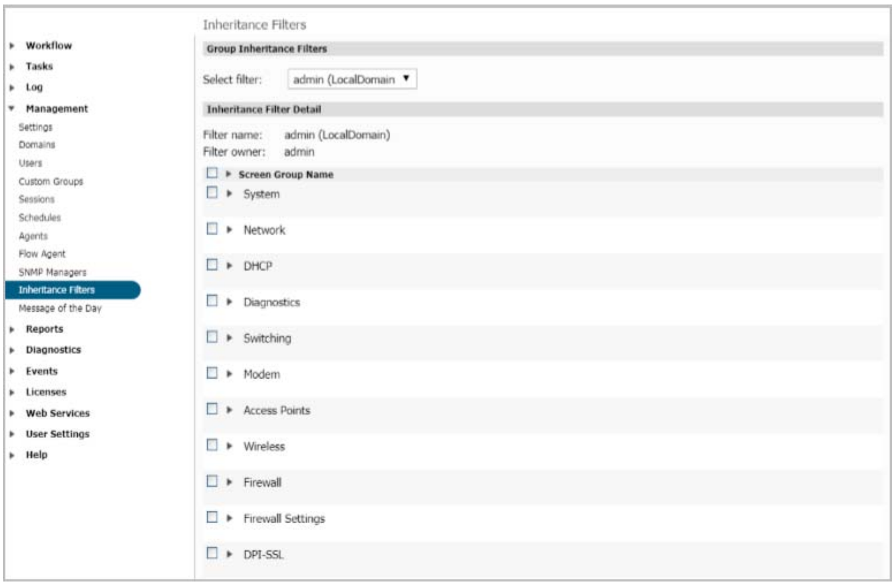
2. Select the IP address and port of the SNMP Manager from the **SNMP Manager IP/Port** fields. This field can accept/display IPv4 and IPv6 addresses.
3. Specify the IP addresses of SNMP Hosts to which traps are forwarded in the **SNMP Host to forward traps to** fields. These fields can accept/display IPv4 and IPv6 addresses.
4. To enable trap forwarding, select **Enable SNMP Trap Forwarding**.
5. To enable trap email, select **Enable SNMP Trap Email**.
6. When you are finished, click **Update**. The settings are changed. To clear the settings and start over, click **Reset**.

Inheritance Filters

The Inheritance Filters page specifies which settings are inherited from the group when adding a new SonicWall appliance. To create a new filter, enter a name for this filter in the “Name” field. Then check the boxes next to the screens, or screen groups, you wish to inherit. This screen is enhanced to automatically select or deselect dependent data screens, based upon the related screens chosen by you.

To configure the SNMP Inheritance Filter page, complete the following steps:

1 Navigate to **CONSOLE | Management > Inheritance Filters**. The Inheritance Filters page displays.



Inheritance Filters

Group Inheritance Filters

Select filter: admin (LocalDomain ▾

Inheritance Filter Detail

Filter name: admin (LocalDomain)

Filter owner: admin

- □ ▸ Screen Group Name
- □ ▸ System
- □ ▸ Network
- □ ▸ DHCP
- □ ▸ Diagnostics
- □ ▸ Switching
- □ ▸ Modem
- □ ▸ Access Points
- □ ▸ Wireless
- □ ▸ Firewall
- □ ▸ Firewall Settings
- □ ▸ DPI-SSL

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 GMS user group from the **Access for each UserType** section.

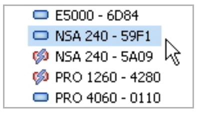
5 When you are finished, click **Add** for a new filter or click **Update** for an existing filter. The settings are changed. To clear the settings and start over, click **Reset**.

Applying Inheritance Settings

Administrators often work to define and test policies at the appliance level, and then painstakingly attempt to replicate those policies on other appliances. Using this simple process for inheritance, you can capitalize on the valuable time spent building a unit's well-configured firewall policies, by then seamlessly replicating those policies through the hierarchy.

1 To inherit some or all of an appliance's settings, go to the **Firewall > System > Tools** screen within the GMS management interface.

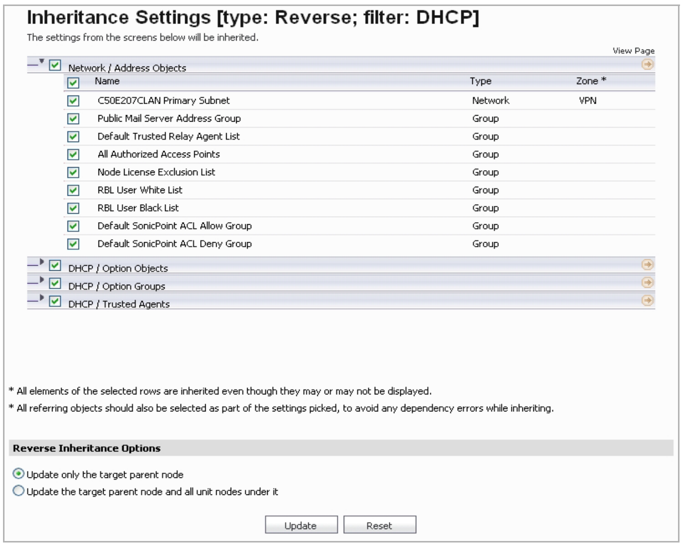
2 In the left pane, click the appliance with the settings you wish to inherit.



3 Under the screen section heading, "Inherit Settings at Unit," select either forward or reverse inheritance by clicking the respective radio button.

4 From the "Filter" drop down menu, select the inheritance filter to apply. If a desired filter is not listed and must be created, refer to Inheritance Filters on page 68

5 After the desired inheritance filter is selected, click **Preview**. A Preview screen opens to allow you to review the settings to be inherited. You might continue with all of the default screens selected for inheritance or select only specific screens for inheritance by checking boxes next to the desired settings.



Inheritance Settings [type: Reverse; filter: DHCP]

The settings from the screens below will be inherited.

View Page

☑ Network / Address Objects

☑	Name	Type	Zone *
☑	C50E207CLAN Primary Subnet	Network	VPN
☑	Public Mail Server Address Group	Group	
☑	Default Trusted Relay Agent List	Group	
☑	All Authorized Access Points	Group	
☑	Node License Exclusion List	Group	
☑	RBL User White List	Group	
☑	RBL User Black List	Group	
☑	Default SonicPoint ACL Allow Group	Group	
☑	Default SonicPoint ACL Deny Group	Group	

☑ DHCP / Option Objects

☑ DHCP / Option Groups

☑ DHCP / Trusted Agents

* All elements of the selected rows are inherited even though they may or may not be displayed.

* All referring objects should also be selected as part of the settings picked, to avoid any dependency errors while inheriting.

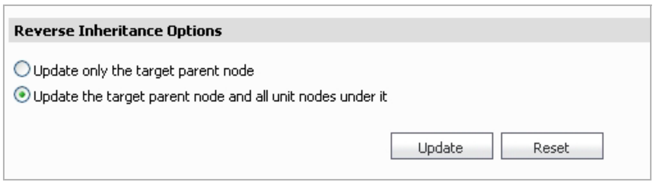
Reverse Inheritance Options

● Update only the target parent node

○ Update the target parent node and all unit nodes under it

NOTE: The Preview screen footer states, "All referring objects should also be selected as part of the settings picked, to avoid any dependency errors while inheriting." If you deselect dependent screen data, the settings will not inherit properly.

6 If you are attempting forward inheritance, you might click "Update" to proceed. If you are attempting to reverse inherit settings, an additional selection must be made at the bottom of the Preview screen. You must select either to update the chosen settings to only the target parent node, or to update the target parent node along with all unit nodes under it. After you make this selection, you can click "Update" to proceed, or "Reset" to edit previous selections.

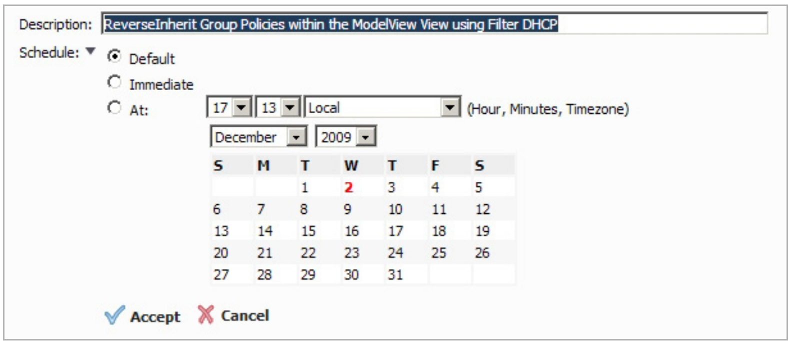


Reverse Inheritance Options

○ Update only the target parent node

● Update the target parent node and all unit nodes under it

7 If you select to update the target parent node and all unit nodes, a "Modify Task Description and Schedule" screen opens in place of the Preview screen. (This screen does not appear if you select "Update only target parent node"). If the "Modify Task Description and Schedule" screen opens, you can edit the task description in the "Description" field. You can also adjust the schedule for inheritance, or continue with the default scheduling. If you choose to edit the timing by clicking the arrow next to "Schedule," a calendar expands allowing you to click a radio button for "Immediate" execution, or to select an alternate day and time for inheritance to occur. After completing any edits, select either "Accept" or "Cancel" to execute or cancel the scheduled inheritance, respectively.



Description: ReverseInherit Group Policies within the ModelView View using Filter DHCP

Schedule: ▼

● Default

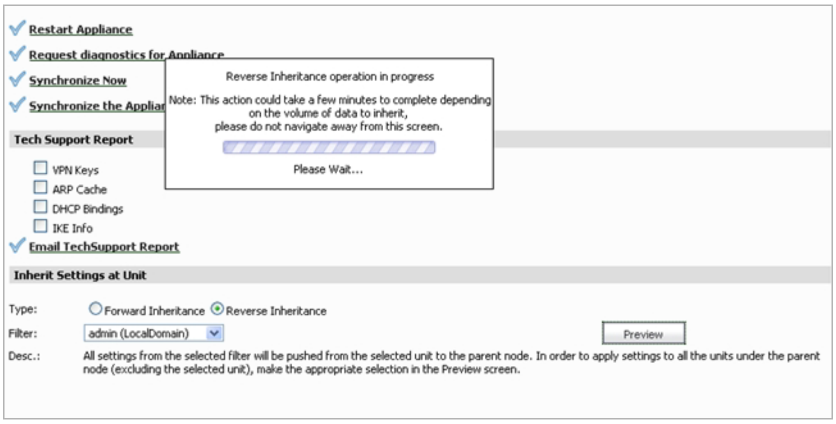
○ Immediate

○ At: 17 13 Local (Hour, Minutes, Timezone)

December 2009

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

After the inheritance operation begins, a progress bar appears, along with text stating the operation might take a few minutes, depending on the volume of data to be inherited, as shown in the following figure:



✓ Restart Appliance

✓ Request diagnostics for Appliance

✓ Synchronize Now

✓ Synchronize the Applian

Reverse Inheritance operation in progress

Note: This action could take a few minutes to complete depending on the volume of data to inherit, please do not navigate away from this screen.

Please Wait...

Tech Support Report

□ VPN Keys
□ ARP Cache
□ DHCP Bindings
□ IKE Info

✓ Email TechSupport Report

Inherit Settings at Unit

Type: ○ Forward Inheritance ● Reverse Inheritance

Filter: admin (LocalDomain)

Desc.: All settings from the selected filter will be pushed from the selected unit to the parent node. In order to apply settings to all the units under the parent node (excluding the selected unit), make the appropriate selection in the Preview screen.

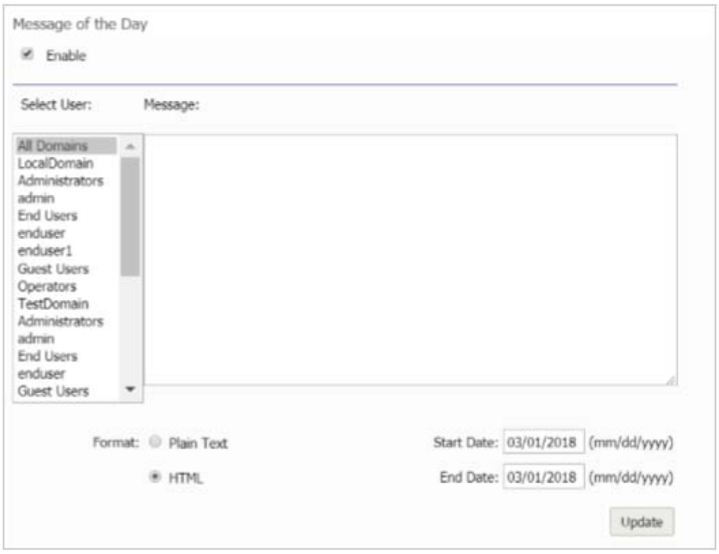
After the inheritance operation is complete, the desired settings from the unit or group node should now be updated and reflected in the parent node's settings, as well as in the settings of all other units, if selected.

Message of the Day

The Message of the Day page displays a message when GMS users log on to GMS.

To configure the Message of the Day page, complete the following steps:

1 Navigate to **CONSOLE | Management > Message of the Day**. The Message of the Day page displays.



Message of the Day

☑ Enable

Select User:

All Domains
LocalDomain
Administrators
admin
End Users
enduser
enduser1
Guest Users
Operators
TestDomain
Administrators
admin
End Users
enduser
Guest Users

Message:

Format: ○ Plain Text ● HTML

Start Date: 03/01/2018 (mm/dd/yyyy)

End Date: 03/01/2018 (mm/dd/yyyy)

2 Select all users, a user group, or an individual user.

3 Enter message text in the **Message** field.

4 Select whether the message text is displayed in plain text or HTML.

5 Select the start and end date of the message (default: current day).

6 When you are finished, click **Update**. The settings are changed.

7 Repeat this procedure for each group or user for which this message is displayed.

7

Managing Reports in the Console Tab

This chapter describes how to configure reporting settings in the GMS Console view. These include how often the summary information is updated, the number of days that summary information is stored, and the number of days that raw data is stored.

Topics:

Summarizer

Topics:

About Summary Data in Reports

These reports are constructed from the most current available summary data. In order to create summary data, the GMS Reporting Module must parse the raw data files.

When configuring GMS Reporting using the screens on **CONSOLE | Reports**, you can select the amount of summary information to store. These settings affect the database size, be sure there is adequate disk space to accommodate the settings you choose.

Additionally, you can select the number of days that raw syslog data is stored. The raw data is made up of information for every connection. Depending on the amount of traffic, this can quickly consume an enormous amount of space in the database. Be very careful when selecting how much raw information to store.

Configuring the Data Deletion Schedule Settings

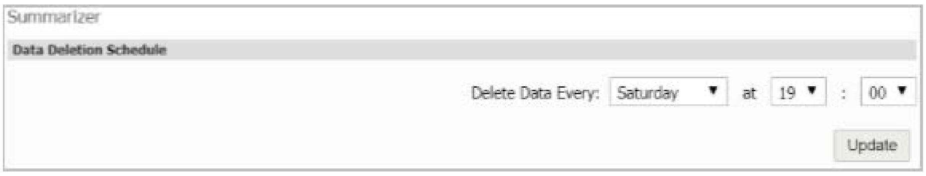
Syslog files sent from SonicWall appliances are stored on the GMS Summarizer system, and are consolidated into the syslog database. The Summarizer processes the syslog data and stores the processed data in the summary database. After the configured period of syslog storage, the syslog data can be periodically deleted from the system. This is necessary, as the syslog files and database can consume a lot of space on the file system.

This section of the Summarizer page also provides a way to delete summarized data for a certain date. For example, if summarized data is kept for a long time, such as 90 days, then you could use this option to remove some summarized data from a particular date within the 90 day period if the stored data was becoming too large.

ⓘ **TIP:** Run your database maintenance jobs soon after the completion of the scheduled tasks configured on this page for summarizing data and deleting old syslog data.

To configure the syslog and summarized data deletion settings, complete the following steps:

1 Navigate to **CONSOLE | Reports > Summarizer**. The Summarizer page appears.



Summarizer

Data Deletion Schedule

Delete Data Every: Saturday ▼ at 19 ▼ : 00 ▼

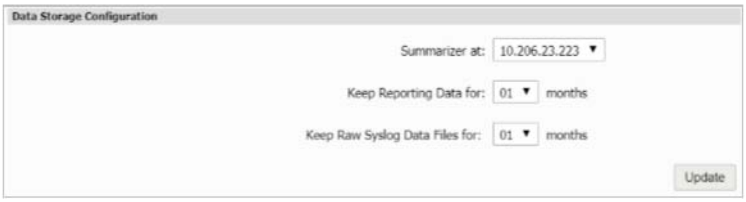
ⓘ **NOTE:** It is recommended that the Data Deletion Schedule be configured to run after the data has been backed up. Navigate to **FIREWALL |Appliance > System > Schedules** to review the current backup schedule.

2 Under **Data Deletion Schedule**, select the day and time for deletion in the hour and minute **widget**. Syslog data is deleted at this time only after being stored for the number of days configured. You specify how long to keep the data in **Data Storage Configuration**.

3 Click **Update** to the right of this field.

Configuring Data Storage

Sets the amount of time that reporting data and raw syslog data is stored.



Data Storage Configuration

Summarizer at: 10.206.23.223 ▼

Keep Reporting Data for: 01 ▼ months

Keep Raw Syslog Data Files for: 01 ▼ months

1 Click the **Summarizer at:** drop-down menu, then select the desired summarizer IP address.

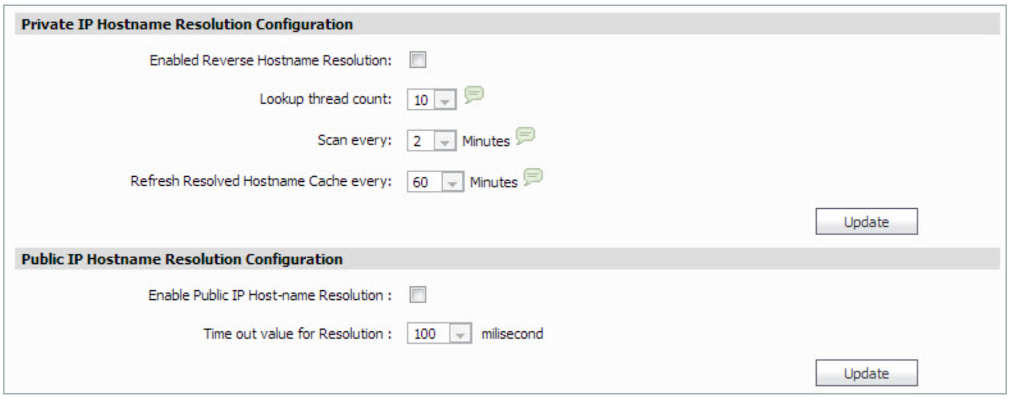
2 Click the **Keep Reporting Data for** drop-down menu, then select the number of months to archive the data. Reporting data can be archived for a minimum of one month and a maximum of 36 months.

3 Click the **Keep Raw Syslog Data Files for** drop-down menu, then select the number of months to archive the data files. To disable the archiving of raw syslog data files, set the value to zero. The maximum amount of time to store raw syslog data files is 36 months.

> **TIP:** If you would like to store data for longer than 36 months, you can create scheduled scripting to move data that has been processed and stored in “//syslog/ArchivedSyslog/*.zip …” to a mapped network share for long-term storage.

Configuring Private IP Hostname Resolution

Hostname Resolution is configured for source IP addresses with missing hostnames while inserting the data in the database. This means that the reports show both the initiator IP address and the initiator hostname in the reports whenever applicable.



Private IP Hostname Resolution Configuration

Enabled Reverse Hostname Resolution: □

Lookup thread count: 10

Scan every: 2 Minutes

Refresh Resolved Hostname Cache every: 60 Minutes

Update

Public IP Hostname Resolution Configuration

Enable Public IP Host-name Resolution : □

Time out value for Resolution : 100 milisecond

Update

- **Enable Reverse Hostname Resolution** — Reverse Hostname Lookup is disabled by default, enable this option for GMS to lookup for missing hostnames.

  > **NOTE:** Enabling hostname lookup increases the time taken to process syslogs. All syslogs that need resolution are processed separately in parallel to normal syslog processing. This might slow down summarizer and increase memory and consume more CPU cycle. Also the memory and CPU are impacted further by changing the default configurations of Lookup thread count, Scan every, and Refresh Resolved Hostname Cache every. Any changes to the Hostname Resolution Configuration takes effect during the next summarizer run.

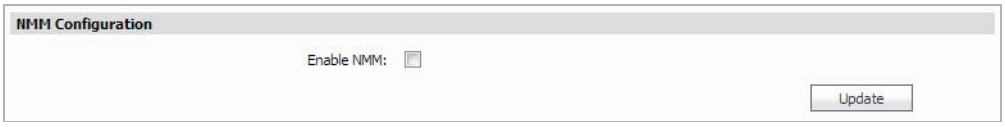
- **Refresh Resolved Hostname Cache every** — The hostname that is looked up for an IP address is cached. This time indicates how long the hostname is kept in the cache, after that it looks up the hostname again for that IP address.
- **Scan every** — Signifies the time intervals at which the lookup is triggered.
- **Lookup thread count** — Signifies how many threads are processing the lookup in parallel. The larger the number, the faster the processing.

  > **NOTE:** Increasing this number also increases the load on the summarizer instance.

- **Update** — Click this button when you are finished configuring the settings.
- **Enable Public IP Host-name Resolution** — Public IP hostname resolution is disabled by default, enable this option for GMS to lookup for missing public IP hostnames.
- **Time out value for resolution** — Select the timeout period (in milliseconds) if the hostname is not resolved.

NMM Configuration

When the NMM option is enabled, the GMS creates NMM files that are sent with the syslog messages.



NMM Configuration

Enable NMM: □

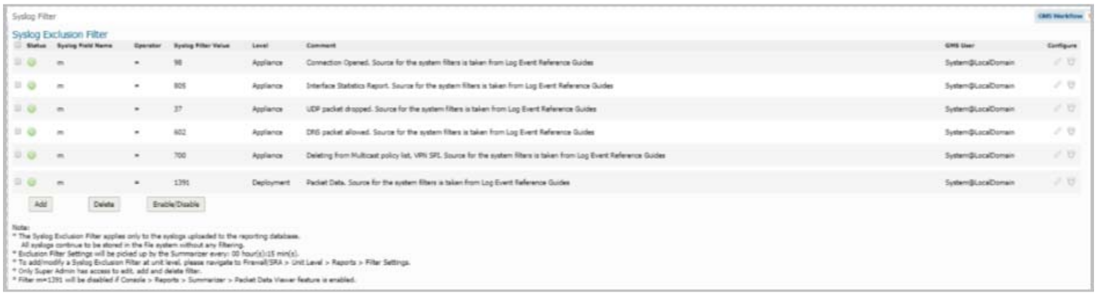
Syslog Exclusion Filter

The Syslog Exclusion Filter allows you to select what fields and operators to use for filtering the syslog database. It is picked up by the Summarizer every 15 minutes and applied to the global syslog settings.

The Syslog Exclusion Filters function in a manner similar to applying an exclusion filter to a single Firewall or SMA appliance, but are applied to all GMS appliances, or all appliances in a Firewall or SMA group.

To add a filter, complete the following steps:

1 Navigate to **CONSOLE | Reports** > **Syslog Filter**. The Syslog Filter page appears.

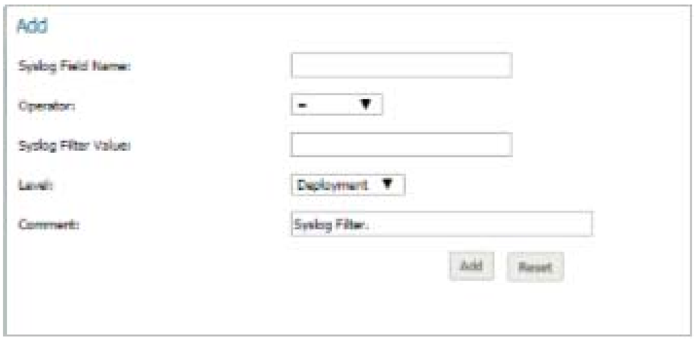


Syslog Exclusion Filter

□	Status	Syslog Field Name	Operator	Syslog Filter Value	Level	Comment	GMS User	Configure
□	●	m	=	98	Appliance	Connection Opened. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
□	●	m	=	805	Appliance	Interface Statistics Report. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
□	●	m	=	37	Appliance	UDP packet dropped. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
□	●	m	=	602	Appliance	DNS packet allowed. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
□	●	m	=	700	Appliance	Deleting from Multicast policy list. VPN SPI. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	
□	●	m	=	1391	Deployment	Packet Data. Source for the system filters is taken from Log Event Reference Guides	System@LocalDomain	

Note:
* The Syslog Exclusion Filter applies only to the syslogs uploaded to the reporting database.
  All syslogs continue to be stored in the File system without any Filtering.
* Exclusion Filter Settings will be picked up by the Summarizer every: 00 hour(s):15 min(s).
* To add/modify a Syslog Exclusion Filter at unit level, please navigate to Firewall/SRA > Unit Level > Reports > Filter Settings.
* Only Super Admin has access to edit, add and delete filter.
* Filter m=1391 will be disabled if Console > Reports > Summarizer > Packet Data Viewer feature is enabled.

2 Click **Add**. The Add menu appears.



Add

Syslog Field Name:

Operator: =

Syslog Filter Value:

Level: Deployment

Comment: Syslog Filter.

3 Enter the syslog field name, an operator, and syslog filter value, for the field you wish to exclude. Then select the Level of Deployment: Appliance, Agent, or full Deployment.

If you select Appliance, you are prompted for the type of appliance: Firewall or SMA. If you select Agent, you are prompted to select from a list of SGMS agents.

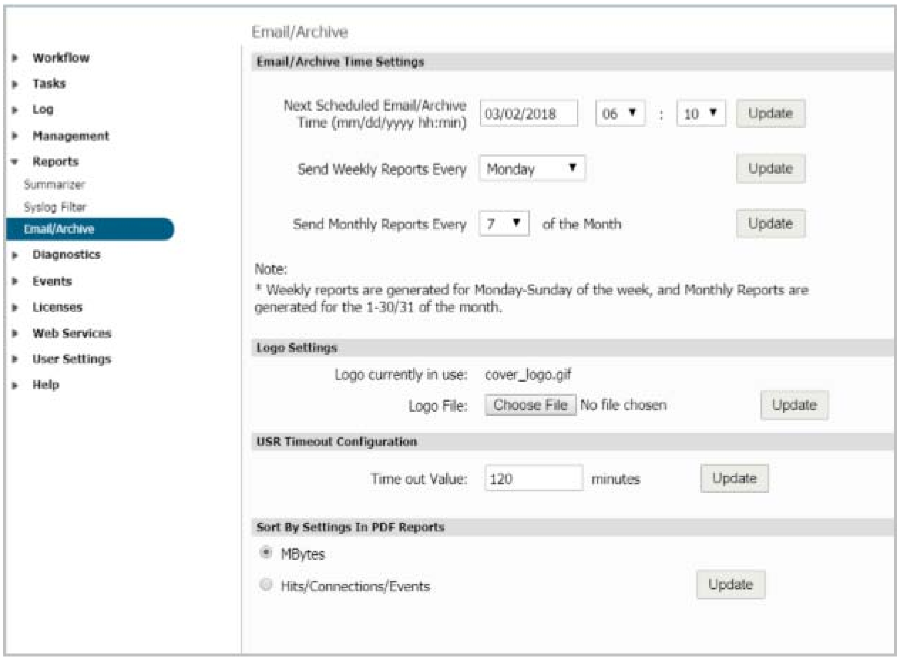
4 Click **Add**.

You can also click the pencil in the Configure column to edit an existing filter setting. If no values appear in the Configure column, the filter is a default system filter. These defaults cannot be configured or deleted.

Syslogs are stored in the database without filtering, so the filters in the Syslog Exclusion Filter apply only to values displayed in Reports.

Email/Archive

The **CONSOLE | Reports** > **Email/Archive** page provides global options for setting the time and interval for emailing/archiving scheduled reports, and global settings for the Web server, logo, and PDF sorting options.



Email/Archive

Email/Archive Time Settings

Next Scheduled Email/Archive Time (mm/dd/yyyy hh:min): 03/02/2018 06 : 10

Send Weekly Reports Every: Monday

Send Monthly Reports Every: 7 of the Month

Note:
* Weekly reports are generated for Monday-Sunday of the week, and Monthly Reports are generated for the 1-30/31 of the month.

Logo Settings

Logo currently in use: cover_logo.gif

Logo File: No file chosen

USR Timeout Configuration

Time out Value: 120 minutes

Sort By Settings In PDF Reports

● MBytes

○ Hits/Connections/Events

Configuring Email/Archive Settings

To configure Email/Archive and Web server settings, complete the following steps:

1. Navigate to **CONSOLE |Reports > Email/Archive**. The Email/Archive page displays.
2. To set the next archive time, enter the date and time in the **Next Scheduled Email/Archive Time** fields and click **Update**.
3. To specify the day to send weekly reports, select the day from the **Send Weekly Reports Every** drop-down menu and click **Update**.
4. To specify the date to send monthly reports, select the date from the **Send Monthly Reports Every** drop-down menu and click **Update**.
5. If the Web server address, port, or protocol has changed because SonicWall GMS was installed, the new values automatically appear in the **Email/Archive Configuration** section. These settings can be modified on the System Interface, and cannot be modified here.
6. Under Logo Settings, you can select a logo to be used on reports. By default, the SonicWall logo is used. To select another logo, click **Choose File** next to the **Logo File** field and select the file or type the path and filename into the field, and then click **Open**. Click **Update** to save changes.
7. Under USR Timeout Configuration, enter a value in the USR - Days to Store field, then click **Update**.

USR schedules are managed under the Dashboard Tab. For more information on USR scheduling, refer to Using the Universal Scheduled Reports Application.

ⓘ **NOTE:** High-traffic systems can generate reports that consume large amounts of memory, disk space and CPU time. Set your Number of Days to Archive and Scheduled Archive Time accordingly.

Managing Legacy Reports

Reports generated by pre 7.0 releases of GMS are still available for viewing, but require careful management. GMS 7.0 Reporting is not compatible with earlier versions, but reports generated by earlier versions are still accessible under the current reporting structure.

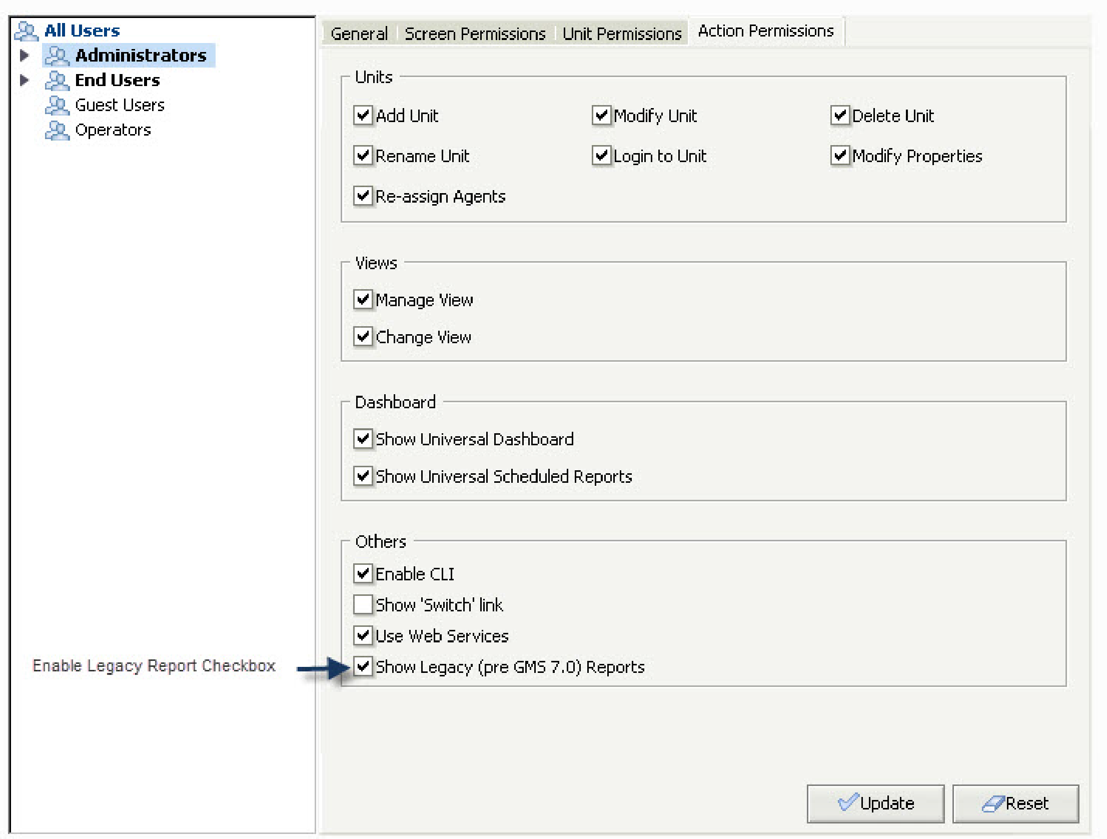
Because it is not possible to view both 7.0 and pre-7.0 reports in the same session, we advise creating a separate Login for accessing Legacy reports. This allows switching back and forth, as you can only view 7.0 or pre 7.0 reports in a session. By creating a separate login, you can switch between viewing modes.

1 Create a new User or Administrator login. An Administrator login (with a name like Admin_Legacy) is recommended, as this login has full privileges. For more information on configuring Legacy reports for new user, refer to the Console Management section.

2 Navigate to **CONSOLE | Management > Users > Action Permissions**. The Action Permissions page appears.

3 Set the flag in **Show Legacy (pre GMS 7.0) Reports**. Click **Update** to save changes.

ⓘ **NOTE:** This check box is only available if GMS 6.0 Reports exist in the system.



Units

☑ Add Unit ☑ Modify Unit ☑ Delete Unit

☑ Rename Unit ☑ Login to Unit ☑ Modify Properties

☑ Re-assign Agents

Views

☑ Manage View

☑ Change View

Dashboard

☑ Show Universal Dashboard

☑ Show Universal Scheduled Reports

Others

☑ Enable CLI

□ Show 'Switch' link

☑ Use Web Services

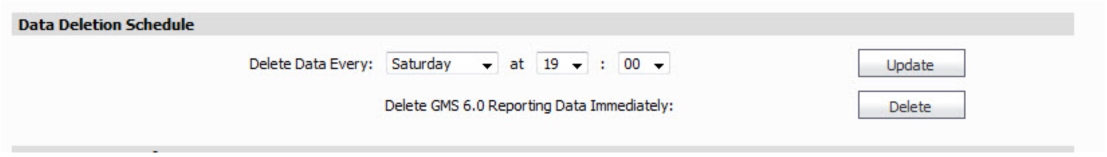
☑ Show Legacy (pre GMS 7.0) Reports

4 Log out. Log back in using the new Login created in Step 1.

If Legacy Reports are no longer needed, you can delete them.

5 Navigate to **CONSOLE | Reports > Summarizer**. The Summarizer page appears.

6 Under the **Data Deletion Schedule**, you will see a box for **Delete 6.0 Reporting Data Immediately**. Click **Delete** to delete the Legacy reports.



Data Deletion Schedule

Delete Data Every: Saturday at 19 : 00

Delete GMS 6.0 Reporting Data Immediately:

NOTE: If you delete pre-7.0 reporting data, the Legacy data check boxes under the Action Permissions and Summarizer tabs are no longer available, going forward.

8

Using Diagnostics

This chapter describes the diagnostic information that GMS provides, including log settings for debugging, system snapshots for troubleshooting, and summarizer status information.

Topics:

Debug Log Settings

Debug Log Settings are included with GMS to help you diagnose issues you might encounter with your log data.

⚠ **WARNING: The Debug Log Settings are intended for use only under the direction of SonicWall Tech Support.**

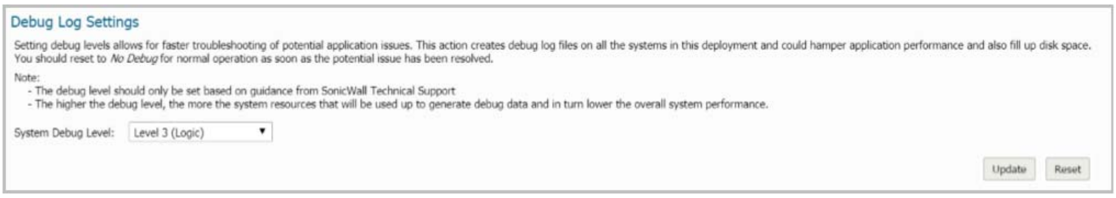
Configuring Debug Log Settings

Setting debug levels allows for faster troubleshooting of potential application issues. This action creates debug log files on all the systems in this deployment and could hamper application performance and also fill up disk space. You should reset to “No Debug” for normal operation as soon as the potential issue has been resolved.

ⓘ **NOTE:** The debug level should only be set based on guidance from SonicWall Technical Support. The higher the debug level, the more the system resources that are used up to generate debug data and in turn lower the overall system performance.

To set the debug level when instructed by SonicWall Technical Support, complete the following steps:

1 Navigate to **CONSOLE | Diagnostics > Debug Log Settings**. The Debug Log Settings page displays.



Debug Log Settings

Setting debug levels allows for faster troubleshooting of potential application issues. This action creates debug log files on all the systems in this deployment and could hamper application performance and also fill up disk space. You should reset to *No Debug* for normal operation as soon as the potential issue has been resolved.

Note:
- The debug level should only be set based on guidance from SonicWall Technical Support
- The higher the debug level, the more the system resources that will be used up to generate debug data and in turn lower the overall system performance.

System Debug Level: Level 3 (Logic)

2 Click the **System Debug Level** drop-down menu, then select one of the following:

- **Level 1 (Codepath)**

    - **Level 2 (Simple)**
    - **Level 3 (Logic)**
    - **Level 4 (Detailed)**
    - **Level 5 (Highly Detailed)**

3. Click **Update**.

Request Snapshot

In order for a technical support representative to troubleshoot a problem, you might be asked to take a snapshot of GMS or you might want to view the configuration yourself.

Performing a System Snapshot

A system snapshot provides a detailed information about GMS, the GMS database, the system environment, licensing, and firewalls. This information includes:

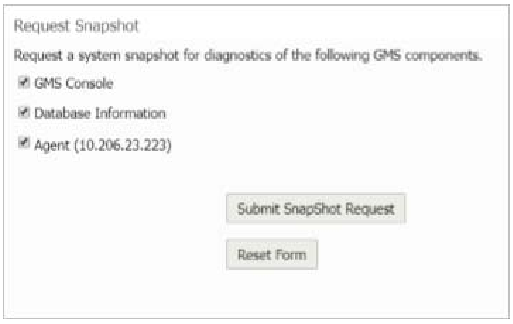
- Data from the sgmsConfig.xml file (Console or Agent only)
    - Debug state
    - Build number
    - Version
    - Product Code
    - Database type
    - Database driver string
    - Database dbuser
    - Database password
    - Database URL
- Server state (Console or Agent only)—whether a database connection could be established
- Environment information
    - CLASSPATH, PATH variables
    - Web server listening port (Console only)
    - Country
    - Language
    - Operating System
    - IP Address
    - MAC Address
    - Machine data (memory size and so on.)
- Latte/Licensing (Console or Agent only)
    - Connectivity to Latte backend
    - Latte username/password

    - MS license information (Console only)
- Agent specific data
    - Managed units
    - Units states (active or standby)
    - Gateway firmware version
    - Gateway state
    - Ports (syslog, syslog parsing, and so on)
- Firewall data (Gateway or Unit only)
    - IP address
    - Data from status.xml
    - VPNs present (Gateway only)
    - Latte information (if registered)

Performing the Snapshot

To take a snapshot of the system, complete the following steps:

1 Navigate to **CONSOLE | Diagnostics > Request Snapshot**. The Request Snapshot page displays.



Request Snapshot

Request a system snapshot for diagnostics of the following GMS components.

☑ GMS Console

☑ Database Information

☑ Agent (10.206.23.223)

2 To take a snapshot of the GMS console, select **GMS Console**.

3 To take a snapshot of one or more GMS agents, select **Agent**. This field displays IPv4 and IPv6 addresses.

4 To take a snapshot of the GMS Gateway, select **Gateway**.

5 Click **Submit Snapshot Request**. GMS takes the snapshot.

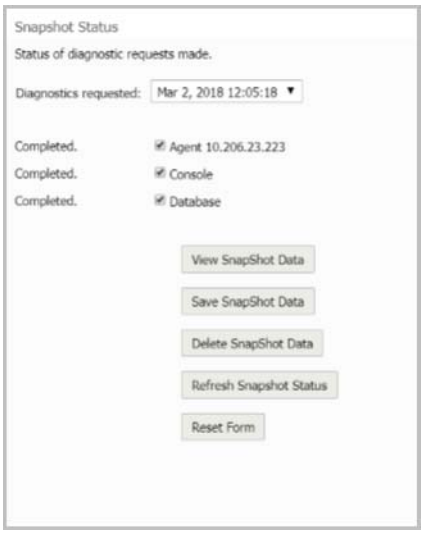
6 To view the snapshot, see Viewing the Snapshot or Diagnostics on page 82.

Snapshot Status

Viewing the Snapshot or Diagnostics

To view a snapshot or SonicWall diagnostics, complete the following steps:

1 Navigate to **CONSOLE | Diagnostics > Snapshot Status**. The Snapshot Status page displays.



Snapshot Status

Status of diagnostic requests made.

Diagnostics requested: Mar 2, 2018 12:05:18 ▼

Completed. ☑ Agent 10.206.23.223

Completed. ☑ Console

Completed. ☑ Database

2 Select the snapshot or diagnostics that you want to view from the **Diagnostics requested** drop-down menu.

3 To view the information, click **View Snapshot Data**.

4 To save the information to a file that you can send to technical support, click **Save Snapshot Data**.

5 To delete the information, click **Delete Snapshot Data**.

6 To refresh the information, click **Refresh Snapshot Data**.

7 To reset the form, click **Reset Form.**

Summarizer Status

The **Summarizer Status** page displays overall summarizer utilization information for the deployment including database and syslog file statistics, and details on the current status of the summarizer.

The Summarizer Status screen provides performance metrics for your network administrator to plan, design, and expand your GMS server deployment. This feature has information on the Syslog Collector and Summarizer metrics. The metrics displayed are daily averages collected over the last 7 days.

You can receive alert emails when Summarizer Status shows any abnormalities.

To reach the Summarizer Status screen, navigate to **CONSOLE |Diagnostics > Summarizer Status**.

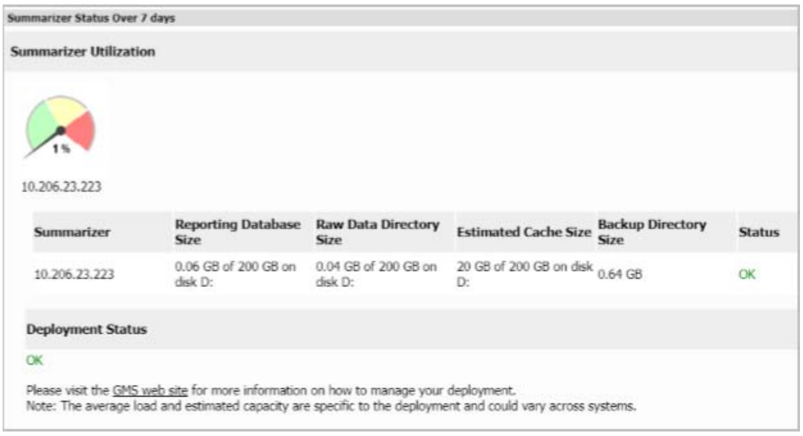
The Summarizer Status page is divided into a section showing the overall deployment-wide summarizer status and sections with details for each summarizer.

Topics:

- Summarizer Status Over 7 Days on page 83
- Details for Summarizer at <IP Address> on page 84
- Syslogs Sent by Appliances that Are Not Under Reporting and Management on page 85

Summarizer Status Over 7 Days

The Summarizer Status Over 7 Days section displays overall summarizer utilization information for the deployment including database and syslog file statistics. Results are calculated over the last seven days.



Summarizer Status Over 7 days

Summarizer Utilization

10.206.23.223

Summarizer	Reporting Database Size	Raw Data Directory Size	Estimated Cache Size	Backup Directory Size	Status
10.206.23.223	0.06 GB of 200 GB on disk D:	0.04 GB of 200 GB on disk D:	20 GB of 200 GB on disk D:	0.64 GB	OK

Deployment Status

OK

Please visit the GMS web site for more information on how to manage your deployment.
Note: The average load and estimated capacity are specific to the deployment and could vary across systems.

Summarizer Utilization

The top Summarizer Utilization section shows the average utilization of the summarizer over the applicable time period. The Dial Charts show the percent of total capacity used by the Summarizer. The following metrics are also displayed in the Summarizer Utilization section:

- **Summarizer**: Displays the IP address of the Summarizer.
- **Reporting Database Size**: Displays the size of the reporting database in gigabytes.
- **Raw Data Directory Size**: Displays the size of the raw syslog directory in gigabytes.
- **Estimated Cache Size**: Displays the estimated size of the cache in gigabytes.
- **Backup Directory Size**: Displays the size of the backup directory in gigabytes.
- **Status**: Displays the status of the Summarizer. There are three different status notifications:
  - **OK**: The system is operating normally.
  - **High Capacity**: The average load is greater than 90 percent of capacity.
  - **Low Disk Space**: There is less that 5GB of space left on the disk.

Deployment Status

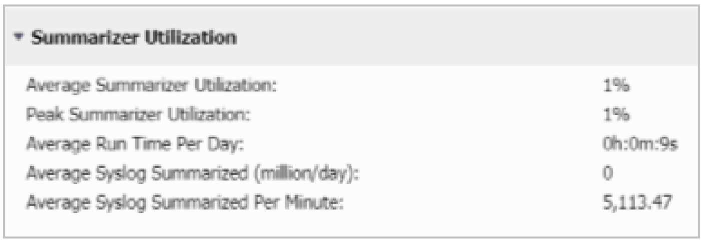
The Deployment Status tells the user how the deployment should be sized, if it is not performing well. The user might need to reassign some units to a different agent, add another agent, or add more disk space

Details for Summarizer at <IP Address>

This sections details the Summarizer Utilization for the applicable IP address.

Summarizer Utilization

The Summarizer Utilization section for a specific summarizer shows not only the information at deployment level, but also provides granular details of the summarizer’s operation and current status for each individual summarizer.



▾ Summarizer Utilization

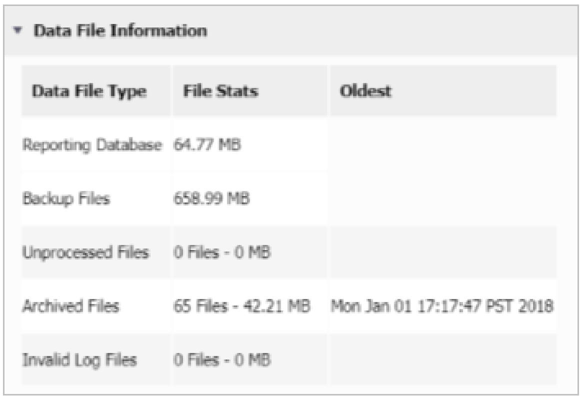
Average Summarizer Utilization:	1%
Peak Summarizer Utilization:	1%
Average Run Time Per Day:	0h:0m:9s
Average Syslog Summarized (million/day):	0
Average Syslog Summarized Per Minute:	5,113.47

- **Average Summarizer Utilization**: The average percentage of Summarizer utilization.
- **Peak Summarizer Utilization**: The percentage of peak Summarizer utilization.
- **Average Run Time Per Day**: The total amount of time spent generating summarization statistical data and results over the time period of one day.
- **Average Syslog Summarized (million/day)**: The total number of syslogs summarized, displayed in millions per day.
- **Average Syslog Summarized per minute**: The average number of syslogs summarized per minute over the applicable time period.

ⓘ **NOTE:** Not all syslogs are summarized. Some syslogs are discarded based on criteria defined at the **CONSOLE | Reports > Syslog Filter** and **Unit > Reports > Configuration > Syslog Filter** pages.

Data File Information

This section displays syslog file details for the selected summarizer.



▾ Data File Information

Data File Type	File Stats	Oldest
Reporting Database	64.77 MB	
Backup Files	658.99 MB	
Unprocessed Files	0 Files - 0 MB	
Archived Files	65 Files - 42.21 MB	Mon Jan 01 17:17:47 PST 2018
Invalid Log Files	0 Files - 0 MB	

The Data File Information table is divided into three columns:

- **Data File Type**: The type of files being reported on.

  There are five main data file types:

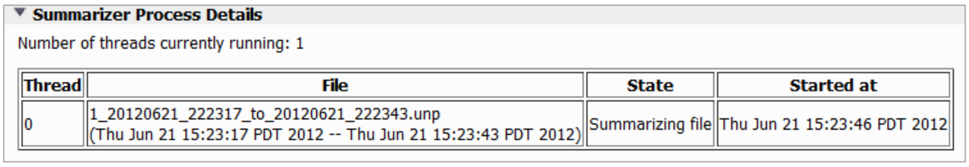
  - Reporting Database Files: The files in the reporting database.
  - Backup Files: The backup snapshot.

    - Unprocessed Files: The data files in the summarizer's processing queue.
    - Archived Files: The processed data files.
    - Invalid Log Files: Data files with processing errors.
- **File Stats**: The number of syslog files in the category and their size in Megabytes.
- **Oldest**: The date and time on the oldest file in the category.

Summarizer Process Details

The Summarizer Process Details section shows what tasks the summarizer is performing at the moment the **CONSOLE | Diagnostics > Summarizer Status** page displays. Refresh your browser display or leave the page and return to it to update the information.

If the summarizer is currently running, the page displays the thread, appliance identifier, file being used, and state of the summarizer.

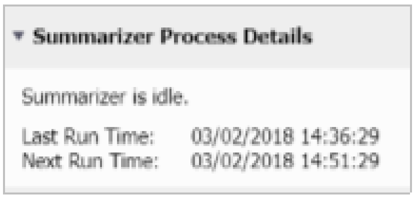


▼ Summarizer Process Details

Number of threads currently running: 1

Thread	File	State	Started at
0	1_20120621_222317_to_20120621_222343.unp (Thu Jun 21 15:23:17 PDT 2012 -- Thu Jun 21 15:23:43 PDT 2012)	Summarizing file	Thu Jun 21 15:23:46 PDT 2012

If the summarizer is currently idle, the page displays the last run time and next run time.



▼ Summarizer Process Details

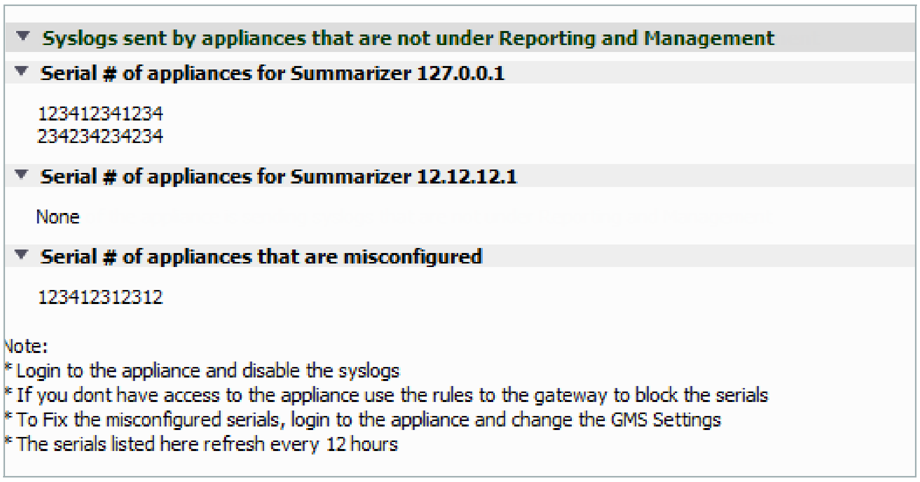
Summarizer is idle.

Last Run Time: 03/02/2018 14:36:29
Next Run Time: 03/02/2018 14:51:29

Syslogs Sent by Appliances that Are Not Under Reporting and Management

Appliances that are no longer managed by GMS might still send syslog messages, impacting the performance of the summarizer. The syslogs from such appliances are dropped and not stored in archivedSyslogs or badSyslogs folders.

This feature displays a list (refreshed every 12 hours) of the appliances that are still sending syslogs messages even though they are no longer managed by GMS, as well as appliances that are incorrectly configured:



▼ Syslogs sent by appliances that are not under Reporting and Management

▼ Serial # of appliances for Summarizer 127.0.0.1

123412341234
234234234234

▼ Serial # of appliances for Summarizer 12.12.12.1

None

▼ Serial # of appliances that are misconfigured

123412312312

Note:
* Login to the appliance and disable the syslogs
* If you dont have access to the appliance use the rules to the gateway to block the serials
* To Fix the misconfigured serials, login to the appliance and change the GMS Settings
* The serials listed here refresh every 12 hours

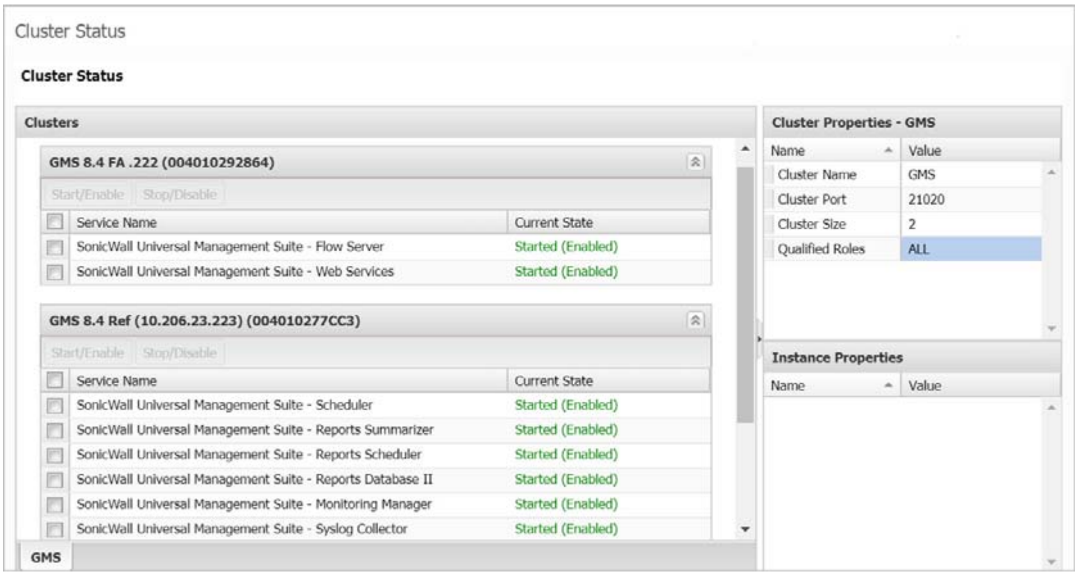
If your GMS has a list of appliances in these fields, try the following to correct the issue:

- Login to the appliance and disable the syslogs.
- If you do not have access to the appliance, use the rules to the gateway to block the serial numbers.
- To fix the misconfigured appliances, login to the appliance and change the GMS settings.

Cluster Status

1 Navigate to the **CONSOLE | Diagnostics > Cluster Status** page.

The **Cluster Status** page displays.



Cluster Status

Cluster Status

Clusters

GMS 8.4 FA .222 (004010292864)

	Service Name	Current State
□	SonicWall Universal Management Suite - Flow Server	Started (Enabled)
□	SonicWall Universal Management Suite - Web Services	Started (Enabled)

GMS 8.4 Ref (10.206.23.223) (004010277CC3)

	Service Name	Current State
□	SonicWall Universal Management Suite - Scheduler	Started (Enabled)
□	SonicWall Universal Management Suite - Reports Summarizer	Started (Enabled)
□	SonicWall Universal Management Suite - Reports Scheduler	Started (Enabled)
□	SonicWall Universal Management Suite - Reports Database II	Started (Enabled)
□	SonicWall Universal Management Suite - Monitoring Manager	Started (Enabled)
□	SonicWall Universal Management Suite - Syslog Collector	Started (Enabled)

Cluster Properties - GMS

Name	Value
Cluster Name	GMS
Cluster Port	21020
Cluster Size	2
Qualified Roles	ALL

Instance Properties

Name	Value

2 Click the check box next to the service cluster you would to control. the Cluster Properties in the right column display the status of each cluster.

3 Click **Start/Enable** or **Stop/Disable** depending on your requirements.

9

Granular Event Management

This chapter describes how to configure and use the Granular Event Management (GEM) feature in a GMS environment.

Topics:

Granular Event Management Overview

Granular Event Management (GEM) provides a customized and controlled manner in which events are managed and alerts are created. In the Console view, GEM allows you to systematically configure each sub-component of your alert in order for the alert to best accommodate your needs.

The GEM alert has multiple sub-components, some of which have further subcomponents. It is not necessary to configure all sub-components prior to creating an alert.

- **Severities**: Severity is used to tag an alert as Critical, Warning, Information, or a custom severity level. You can create your own preferred severities and assign the order of importance to them from lowest to highest. When using a custom severity, you must define it before creating a threshold that uses it.
- **Thresholds**: A threshold defines the condition that must be matched to trigger an event and send an alert. Each threshold is associated with a Severity to tag the generated alert as critical, warning, or information. You must define a threshold prior to creating an alert that uses it.

  One or more threshold elements are defined within a threshold. Each threshold element includes an Operator, a Value, and a Severity. When a value is received for an alert type, the GEM framework examines threshold elements to find a match for the specified condition. If a match is found (one or more conditions match), the threshold with the highest severity containing a matching element is used to trigger an event.
- **Schedules**: You can use Schedules to specify the day(s) and time (intervals) in which to send an alert. You can also invert a schedule, which means that the schedule is the opposite of the time specified in it. For example:
  - Send an alert during weekdays only, or weekends only, or only during business hours.
  - Do not send an alert during a time period when the unit, network, or database are down for maintenance.
- **Destinations**: You can use Destinations to define where the alerts are sent. The destination(s) for an alert are specified in the Add Alert or Edit Alert screen. You can specify up to five destinations for an alert, such as multiple email addresses. For example:

- Send an alert to the Unit owner all the time.
- Send an alert to a GMS user during business hours.
- Send an alert to the admin also during non-business hours for immediate attention.

- **Alert types**: Alert Types are pre-defined, static parameters and are not customizable. Alert types are used with threshold elements that define conditions that can trigger an event. Some example alert types are:
  - Unit Status Report
  - Database Info

You must configure three of these components in order to create alerts:

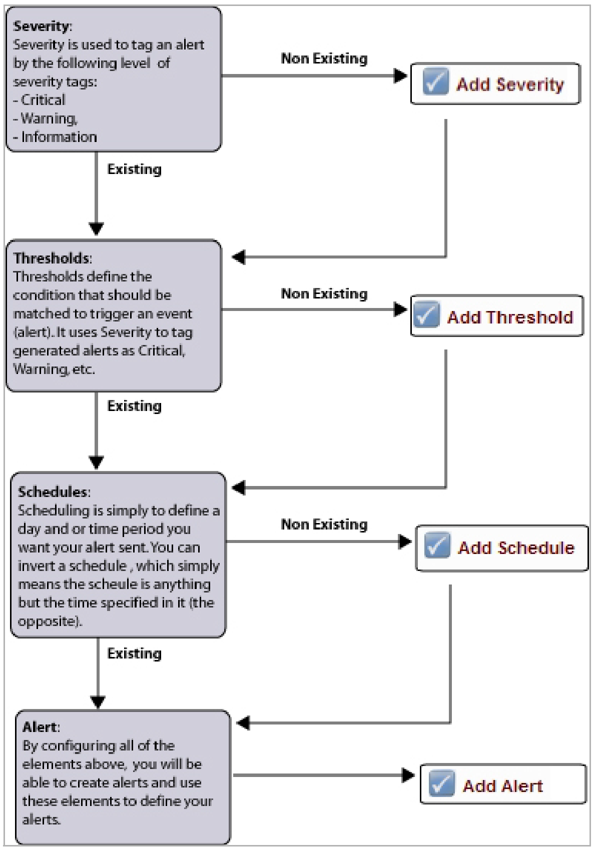
- **Severities** - You can use the pre-defined defaults or create your own Severities.
- **Thresholds** - You can use the pre-defined defaults or create your own thresholds.
- **Schedules** - You can use the pre-defined defaults or create your own Schedules.

These can be configured in **CONSOLE |Events > Severity** or **CONSOLE |Events > Alert Settings > Add Alert** screens. After you configure these elements in **CONSOLE | Events**, you can also create alerts in the **FIREWALL**, **SMA,** and **EMAIL SECURITY (ES)** views.

The Super Admin (admin@LocalDomain) user is able to add a new Severity, Threshold, Schedule, Schedule Group, or Alert into any domain. Other administrative users might only create/edit objects within their own domain.

The GEM process flow is illustrated below. As you can see, you begin by configuring Severities and end with creating Alerts.

GEM Process


Severity:
Severity is used to tag an alert by the following level of severity tags:
- Critical
- Warning,
- Information

Thresholds:
Thresholds define the condition that should be matched to trigger an event (alert). It uses Severity to tag generated alerts as Critical, Warning, etc.

Schedules:
Scheduling is simply to define a day and or time period you want your alert sent. You can invert a schedule , which simply means the scheule is anything but the time specified in it (the opposite).

Alert:
By configuring all of the elements above, you will be able to create alerts and use these elements to define your alerts.

What is Granular Event Management?

The purpose of Granular Event Management is to provide all the event handling and alerting functionality for GMS. The GMS management interface provides screens for centralized event management on the **CONSOLE | Events > Settings**, **Severity**, **Threshold**, **Schedule**, and **CONSOLE | Events > Alert Settings** pages. The **FIREWALL**, **SMA**, and **EMAIL SECURITY (ES)** views also provide a screen where you can add, delete, enable, or configure alerts that relate to either policies or reports.

You can create or update an alert at the global, group, or unit level in GMS. At the group or global level, the alert is then applied to all units in the group or globally. Whenever you add a new unit to GMS management, the alerts set at the global level are applied to the new unit. Group level alerts are not automatically applied to the new unit, but when you update an alert at the group level, the update applies the alert to the entire group including any new units.

Benefits

Granular Event Management offers a significant improvement in control over the way different events are handled. You now have more flexibility when deciding where and when to send alerts, and you can configure event thresholds, severities, schedules, and alerts from a centralized location in the management interface rather than configuring these on a per-unit basis.

How Does Granular Event Management Work?

The Granular Event Management framework provides customized event, including email alerting on the status of specific VPN tunnels, alerting based on schedules (such as 8am to 5pm, or 24 hours a day), and alerting to specific email destinations based on severity and functionality handling. You can also configure GEM to send an alert when changes are made to a managed appliance by a local administrator through the appliance management interface rather than through GMS. This is a predefined alert available in the Policies view. For a list of the predefined alerts, see Using Granular Event Management on page 89.

Using Granular Event Management

For convenience and usability, a number of default settings are predefined for severities, schedules, thresholds, and alerts. You can edit the predefined values to customize these settings, or you can create your own at the global, group, or unit level. To create your own, start by navigating to **CONSOLE | Events > Alert Settings** and and add custom components where needed. Then continue with the **| Events > Alerts Settings** screens in the **FIREWALL**, **SMA,** and **EMAIL SECURITY (ES)** views. The predefined defaults for the **CONSOLE** view are as follows:

GEM Predefined Default Objects

View	Screens	Predefined Default Objects
CONSOLE	Events > Severities	Information
		Warning
		Critical
CONSOLE	Events > Thresholds	Disk Space Used
		Capacity in Percentage
		Unit HF Status
		Monitor by Percentage (Anti)

GEM Predefined Default Objects (Continued)

View	Screens	Predefined Default Objects
		Monitor by Percentage
		Agent Quota Reached
		Unit Locally Changed
		Unit WAN Status
		VPN Tunnel Status
		Monitor CPU
CONSOLE	**Events > Alert Settings > Add Alert > Schedule**	Schedule Groups:
		24x7
		Weekdays 24 hours
		8x5
		Weekend
		Schedules:
		Schedule: admin
		Database Backup
		Monday 24 hours
		Monday business hours
		Tuesday 24 hours
		Tuesday business hours
		Wednesday 24 hours
		Wednesday business hours
		Thursday 24 hours
		Thursday business hours
		Friday 24 hours
		Friday business hours
		Saturday 24 hours
		Sunday 24 hours
CONSOLE	**Events > Alert Settings**	Unit Status Report
		Database Information
		New Firmware Availability
		Database Size Status
		System Files Backed-Up Status
		Disk Space Utilization Status

About Alerts

The **Events > Alert Settings** screens are available in the **CONSOLE**, **FIREWALL**, **SMA**, **EMAIL SECURITY (ES)** views. You can create and edit alerts on these screens. In the alert settings screens, you can combine all of the previous elements (severity, threshold, and schedule) that you have configured in the Console view.

The GEM framework provides different types of alert types for the respective areas of the GMS application:

- Policies view: Alert settings for Management
- Reports view: Alert settings for Reporting
- Console view: Alert settings for the GMS application

GEM Alert Types

Tab Location	Available Alert Types
Console	Backed up Syslog Files
	Database Information
	Disk Space Utilization Status
	New Firmware Availability
	Unit Status Report
Reports	Bandwidth Usage (Billing Cycle)
	Bandwidth Usage (Daily)
	Data Usage (Billing Cycle)
	Data Usage (Daily)
	Events/Hits Total (Daily)
	Number of Attacks (Daily)
	Number of Threats (Daily)
Policies	Unit HF Status
	Unit Locally Changed
	Unit Status
	Unit WAN Status
	VPN Tunnel Status
	Agent Quota Reached
	Agent Unsuccessful Backups
	Appliance Capacity Status
	CPU Status
	Offsite Capacity Status

Duplicate Alerts

Duplicate alerts are allowed in GMS. A duplicate alert uses the same alert type that is already used in an existing alert. You do not need to create a duplicate alert if you want to add to or change an existing alert. Normally, you would avoid creating a duplicate alert by editing an existing alert to add another threshold element, destination, or other component. For example, you can have two or more threshold elements in the same alert to trigger under different conditions.

At times there are benefits to creating a duplicate alert. As an example, only five destinations are allowed per alert, so a duplicate alert could include additional destinations. Or, you could create a duplicate alert that sends SNMP traps while the original alert sends email notifications. Also, if a threshold is being shared and you do not want to modify it, you can create a separate threshold and use it in a duplicate alert.

GMS displays a warning when you try to create a duplicate alert. The warning serves as a reminder in case you forget that an alert already exists using the same alert type.

ⓘ **NOTE:** Duplicate alerts use more resources from the alerting agent, but do not have a large impact on performance. You will receive two alert emails instead of one if the destinations are identical.

Configuring Granular Event Management

To set up the Granular Event Management (GEM) environment after installing GMS, navigate to **CONSOLE | Events**. You should examine each **Events** screen and make any necessary configuration changes. Then you can configure alerts in the **CONSOLE | Events > Settings** and **CONSOLE | Events > Alert Settings** pages.

Topics:

- Configuring Events in the Console View on page 92
- Configuring Alerts in the Console View on page 100

Configuring Events in the Console View

To experience the benefits of GEM, you must configure alerts for important events. In the **CONSOLE | Events** screens, you can configure the frequency of subscription expiration and task failure notifications, as well as severities, thresholds, schedules, and alerts for handling events.

Topics:

- Configuring Event Alert Settings on page 92
- Configuring Event Severities on page 93
- Configuring Event Thresholds on page 95
- Configuring Alerts in the Console View on page 100

Configuring Event Alert Settings

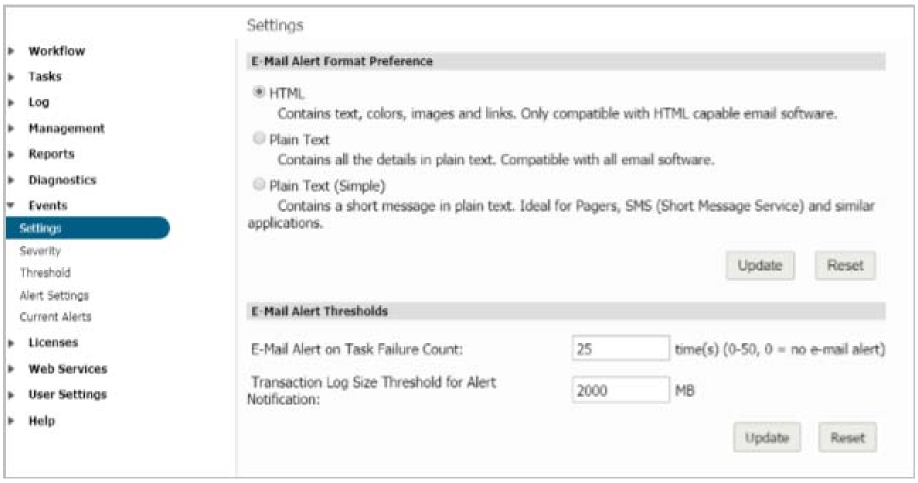
In the **CONSOLE | Events > Settings** page, you can specify the following:

- Email Alert Format, such as HTML (the default), text, or text for a pager
- Email Alert Frequencies and Thresholds

To configure Event Settings, complete the following steps:

1. Navigate to **CONSOLE | Events > Settings**. The settings page appears.
2. Under **Email Alert Format Preferences**, select whether the email alert will be 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.

   ⓘ **NOTE:** To assist in your decision for choosing a type of alert format, refer to Email Alert Formats on page 105 to view the appearance of the types of Email Alert Format Preferences.



Settings

E-Mail Alert Format Preference

● HTML
Contains text, colors, images and links. Only compatible with HTML capable email software.

○ Plain Text
Contains all the details in plain text. Compatible with all email software.

○ Plain Text (Simple)
Contains a short message in plain text. Ideal for Pagers, SMS (Short Message Service) and similar applications.

Update Reset

E-Mail Alert Thresholds

E-Mail Alert on Task Failure Count: 25 time(s) (0-50, 0 = no e-mail alert)

Transaction Log Size Threshold for Alert Notification: 2000 MB

Update Reset

3 Click **Update**.

Configuring Event Severities

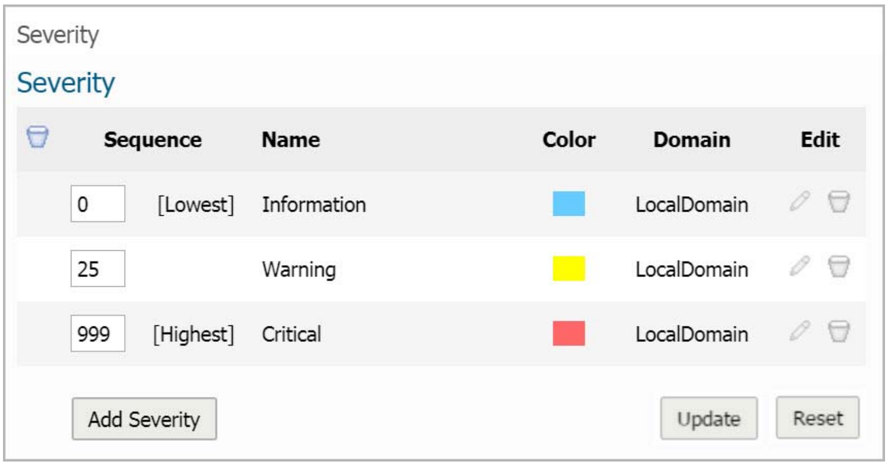
In the **CONSOLE |Events > Severity** screen, you can create your own severity levels or use predefined severity levels. You can delete severity levels in this screen as well. Defining the severity priority can also be performed in this screen. Users with permissions to the Severity screen can create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

GMS 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, complete the following steps:

1 Navigate to **CONSOLE | Events > Severity**. The Severity page appears. On this screen, you can resequence the severities in importance by entering a severity sequence number in each field.



Severity

Severity

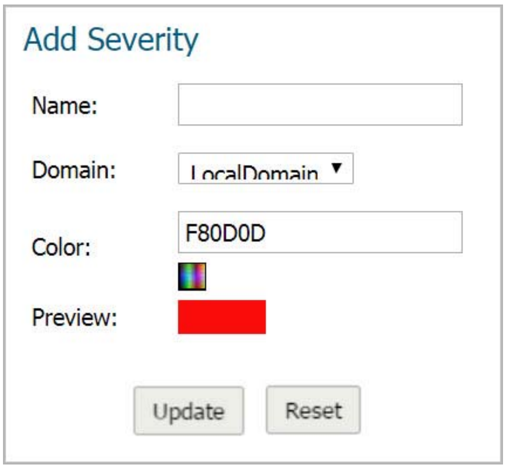
🗑	Sequence	Name	Color	Domain	Edit
	0 [Lowest]	Information	🟦	LocalDomain	✎ 🗑
	25	Warning	🟨	LocalDomain	✎ 🗑
	999 [Highest]	Critical	🟥	LocalDomain	✎ 🗑

2 Do one of the following:

- To re-order existing severities with the new sequence numbers that you entered, click **Update**.
- To add a new severity level, click **Add Severity**.

3 In the **Add Severity** dialog box, type a name for the new severity level in the **Name** field. The **Domain** pull-down list is only available for a Super Admin.

4 Choose the color associated with this severity level by selecting a color from the Color Chooser dialog. You can see a preview of the color you selected in the **Preview** field.



Add Severity

Name:	
Domain:	LocalDomain ▼
Color:	F80D0D
Preview:	🟥

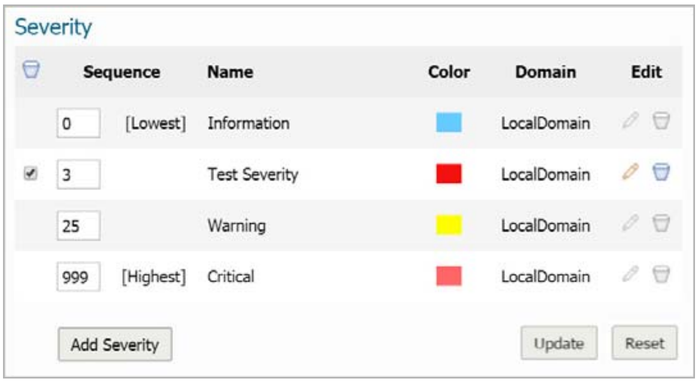
5 Click **Update**.

6 In the **CONSOLE | Events > Severity** screen, assign the level for the new severity you created by changing the numbering in the **Sequence** column of the Severity table.

7 Click **Update**.

To edit or delete a Severity, complete the following steps:

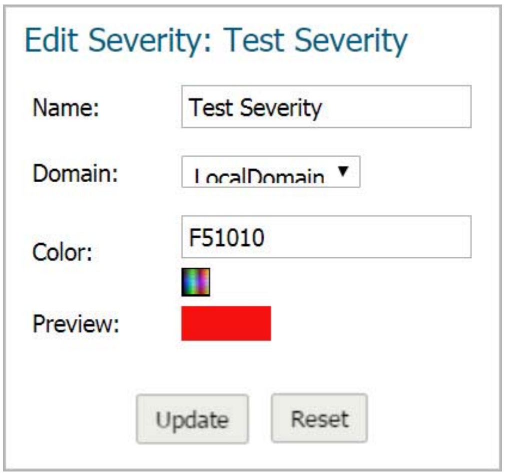
1 To edit a Severity, click the **Edit** icon.



Severity

🗑	Sequence		Name	Color	Domain	Edit
	0	[Lowest]	Information	🟦	LocalDomain	✎ 🗑
☑	3		Test Severity	🟥	LocalDomain	✎ 🗑
	25		Warning	🟨	LocalDomain	✎ 🗑
	999	[Highest]	Critical	🟥	LocalDomain	✎ 🗑

The Edit Severity pop-up window displays.



Edit Severity: Test Severity

Name: Test Severity

Domain: LocalDomain ▼

Color: F51010

Preview: 🟥

2 Configure the Severity Settings, then click **Update**.

3 To delete a Severity(s), select the check box(es) for the severity(s) you wish to delete, then click **Update**. You can also click **Delete** in the Edit column, to delete a single report.

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

Configuring Event Thresholds

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.

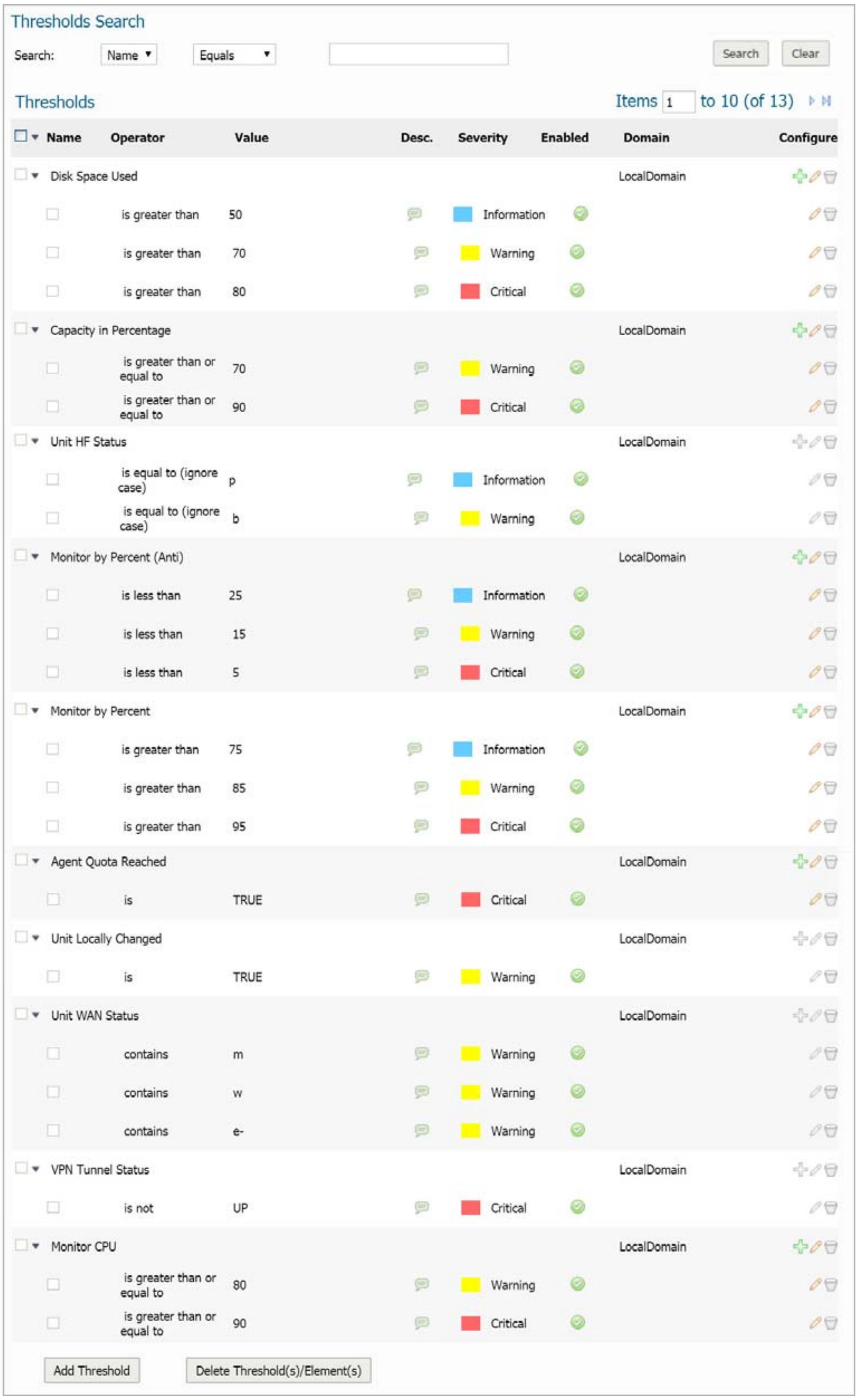
Topics:

- Adding a Custom Threshold on page 96
- Adding a Threshold Element on page 97
- Editing a Custom or Existing Threshold on page 98
- Editing an Threshold Element on page 98
- Enabling/Disabling Thresholds and Threshold Elements on page 99
- Deleting a Threshold and Threshold Elements on page 100

Adding a Custom Threshold

To add a custom threshold, complete the following steps:

1 Navigate to **CONSOLE | Events > Threshold**. The threshold page appears.



Thresholds Search

Search: Name ▾ Equals ▾ [Search] [Clear]

Thresholds   Items 1 to 10 (of 13)

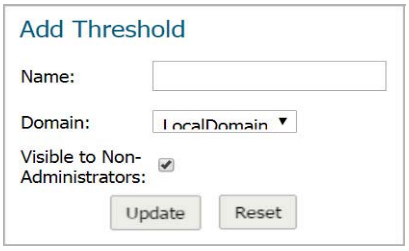
□ Name	Operator	Value	Desc.	Severity	Enabled	Domain	Configure
□ ▾ Disk Space Used						LocalDomain	
□	is greater than	50		🟦 Information	✓		
□	is greater than	70		🟨 Warning	✓		
□	is greater than	80		🟥 Critical	✓		
□ ▾ Capacity in Percentage						LocalDomain	
□	is greater than or equal to	70		🟨 Warning	✓		
□	is greater than or equal to	90		🟥 Critical	✓		
□ ▾ Unit HF Status						LocalDomain	
□	is equal to (ignore case)	p		🟦 Information	✓		
□	is equal to (ignore case)	b		🟨 Warning	✓		
□ ▾ Monitor by Percent (Anti)						LocalDomain	
□	is less than	25		🟦 Information	✓		
□	is less than	15		🟨 Warning	✓		
□	is less than	5		🟥 Critical	✓		
□ ▾ Monitor by Percent						LocalDomain	
□	is greater than	75		🟦 Information	✓		
□	is greater than	85		🟨 Warning	✓		
□	is greater than	95		🟥 Critical	✓		
□ ▾ Agent Quota Reached						LocalDomain	
□	is	TRUE		🟥 Critical	✓		
□ ▾ Unit Locally Changed						LocalDomain	
□	is	TRUE		🟨 Warning	✓		
□ ▾ Unit WAN Status						LocalDomain	
□	contains	m		🟨 Warning	✓		
□	contains	w		🟨 Warning	✓		
□	contains	e-		🟨 Warning	✓		
□ ▾ VPN Tunnel Status						LocalDomain	
□	is not	UP		🟥 Critical	✓		
□ ▾ Monitor CPU						LocalDomain	
□	is greater than or equal to	80		🟨 Warning	✓		
□	is greater than or equal to	90		🟥 Critical	✓		

[Add Threshold] [Delete Threshold(s)/Element(s)]

2 Click **Add Threshold** to add a new threshold.

3 In the Add Threshold dialog box, provide a name for the threshold value in the **Name** field.

> ⓘ **NOTE:** The Domain pull-down list is only available for a Super Admin.



Add Threshold

Name:

Domain: LocalDomain ▾

Visible to Non-Administrators: ☑

4 Select **Visible to Non-Administrators** if you want the threshold to be visible to non-administrators. If this is selected, anyone can view the threshold elements and use the threshold in customized reports.

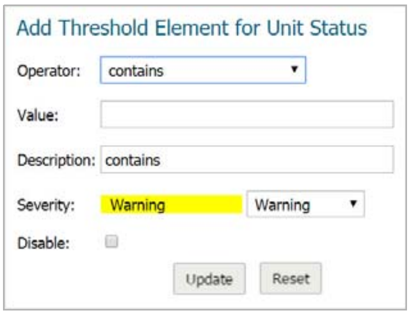
> ⓘ **NOTE:** If the Visible to Non-Administrators is unchecked, only users from the Administrator group or the threshold creator is able to view, use, edit, and delete the threshold. Whether this is selected or not, only the users from the Administrator group and the threshold creator is able to edit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

1 To add a threshold element to the threshold, click the plus icon ✚ in the Configure column of the **CONSOLE | Events > Threshold** page. The Add Threshold Element window displays.



Add Threshold Element for Unit Status

Operator: contains ▾

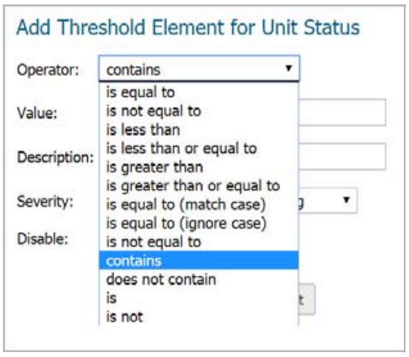
Value:

Description: contains

Severity: Warning | Warning ▾

Disable: □

2 In the **Operator** drop-down menu, select from the list of operators.



Add Threshold Element for Unit Status

Operator: contains ▾

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.

6 **Disable** allows you to temporarily disable the threshold without deleting it. Select **Disable** if you want to disable the threshold. For more information about the enabling and disabling feature, see Enabling/Disabling Thresholds and Threshold Elements on page 99.

7 Click **Update**.

Editing a Custom or Existing Threshold

To edit your custom or existing threshold, complete the following steps:

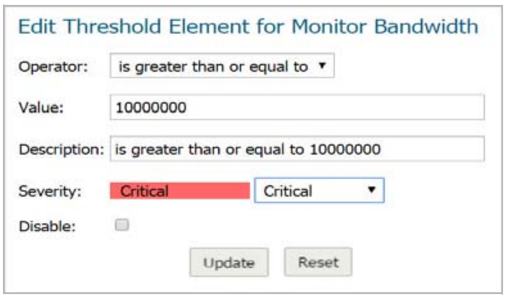
1 Navigate to **CONSOLE | Events > Threshold** and click the **Edit** icon ✎ in the Configure row. The Edit Threshold window displays. In this window, you can edit the name of your threshold as well as allow this threshold to be visible to non-administrators. For more information on the visible to non-administrators feature, see Adding a Custom Threshold on page 96.

2 Click **Update**.

Editing an Threshold Element

To edit an existing element of a Threshold, complete the following steps:

1 Navigate to **CONSOLE | Events > Threshold** and click the **Edit** icon ✎ located in the Configure column in the element row. The Edit Threshold pop-up window appears.



Edit Threshold Element for Monitor Bandwidth

Operator: is greater than or equal to ▾

Value: 10000000

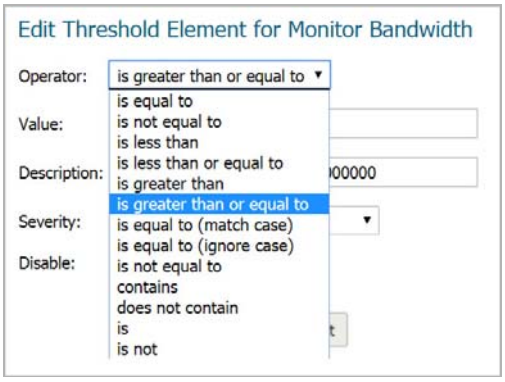
Description: is greater than or equal to 10000000

Severity: Critical | Critical ▾

Disable: □

Some alerts created by certain Alert Types contain predefined Thresholds that might not be edited. Alert Types: Unit HF Status, Unit WAN Status, Unit Locally Changed, and Thresholds with the same name in the Console tab.

2 In the **Operator** field, select from the drop-down menu the type of operator to apply to your threshold element.



Edit Threshold Element for Monitor Bandwidth

Operator: is greater than or equal to

Value:

Description: 00000

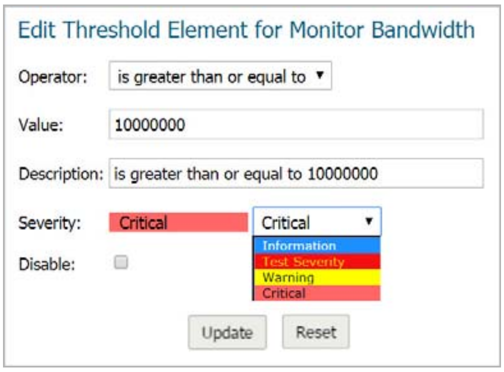
Severity:

Disable:

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.



Edit Threshold Element for Monitor Bandwidth

Operator: is greater than or equal to

Value: 10000000

Description: is greater than or equal to 10000000

Severity: Critical | Critical

Disable: □

6 To disable the threshold element, check the **Disable** box. See Enabling/Disabling Thresholds and Threshold Elements on page 99.

7 Click **Update**.

Enabling/Disabling Thresholds and Threshold Elements

The GEM 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 is beneficial because of the time invested in creating it. 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.

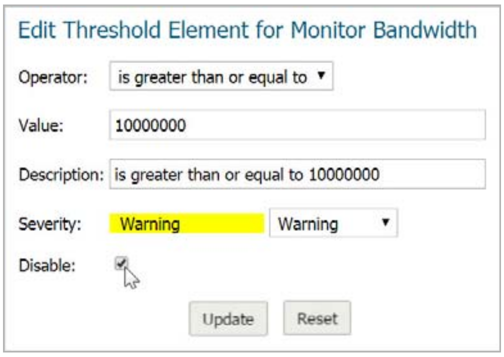
To enable or disable Thresholds and/or their elements, complete the following steps:

1 Navigate to **CONSOLE | Events > Threshold**. On this screen, you are able to view existing Thresholds. You can also view existing elements within those thresholds by clicking the expand button by a 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 To enable or disable a threshold and/or elements, click the edit icon ✎ that is on the element level.

3 Select the check box next to **Disable** to disable the element or de-select **Disable** to enable the element.



Edit Threshold Element for Monitor Bandwidth

Operator:	is greater than or equal to ▾
Value:	10000000
Description:	is greater than or equal to 10000000
Severity:	Warning | Warning ▾
Disable:	☑

4 Click **Update**.

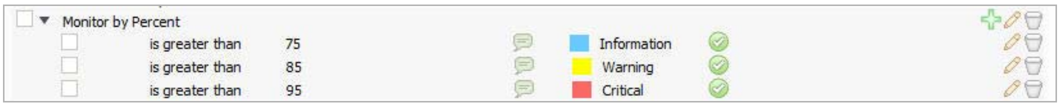
Deleting a Threshold and Threshold Elements

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, complete the following steps:

1 On the **CONSOLE | Events > Threshold** screen, optionally expand the threshold to view the individual elements.

2 To delete a threshold, click the check box to the left of the threshold name. You will see that its elements are automatically selected as well.



□ ▾ Monitor by Percent					
□	is greater than	75	🟦 Information	✓	
□	is greater than	85	🟨 Warning	✓	
□	is greater than	95	🟥 Critical	✓	

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)**.

Configuring Alerts in the Console View

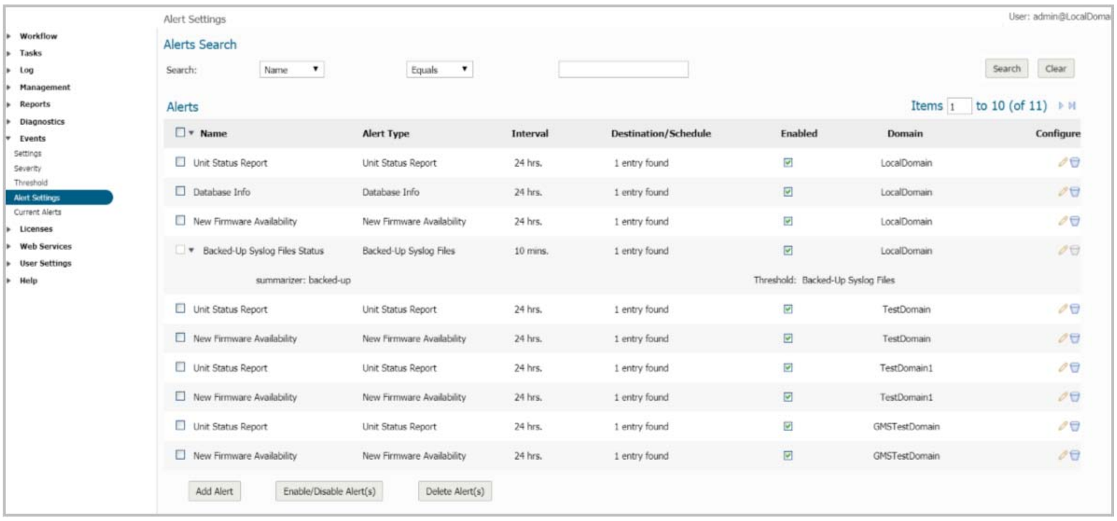
The **CONSOLE | Events > Alert Settings** screen provides predefined alerts that apply to GMS as a whole. These are status type alerts, and do not use thresholds. You can hover your mouse over these to display information about them. You can configure the predefined alerts to use different destinations and schedules.

Add Alert

In the Add Alert panel you can enter an alert name and description, select the options for visible to non-administrators and disable, and enter the polling interval.

To add an alert, complete the following steps:

1 Navigate to **CONSOLE | Events** > **Alert Settings.** The Alert Settings page appears.



Alert Settings

Alerts Search

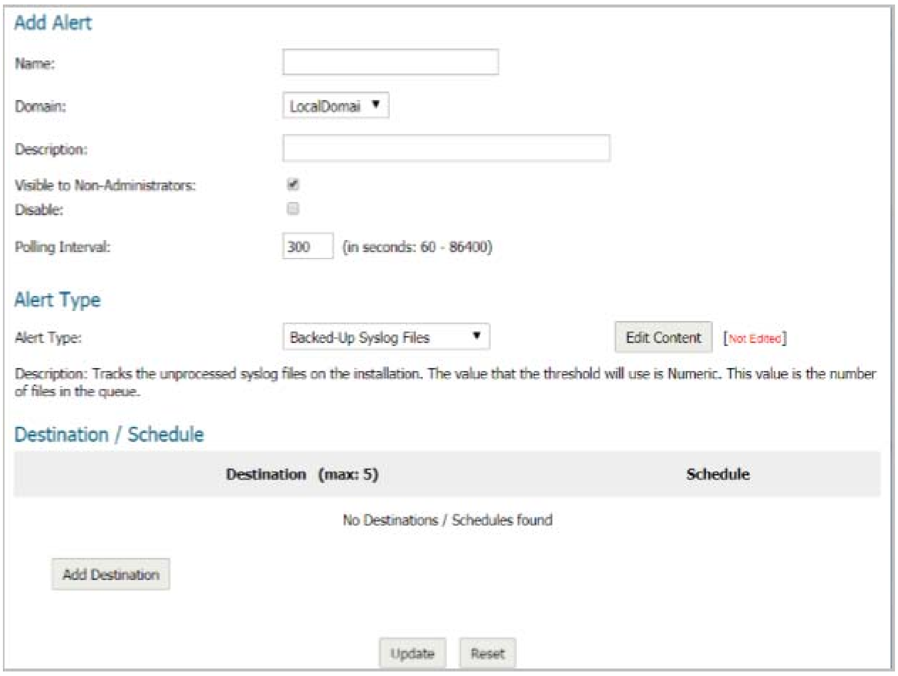
Search: Name ▾ Equals ▾ Search Clear

Alerts Items 1 to 10 (of 11)

□ Name	Alert Type	Interval	Destination/Schedule	Enabled	Domain	Configure
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	LocalDomain	
□ Database Info	Database Info	24 hrs.	1 entry found	☑	LocalDomain	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	LocalDomain	
□ ▾ Backed-Up Syslog Files Status	Backed-Up Syslog Files	10 mins.	1 entry found	☑	LocalDomain	
summarizer: backed-up				Threshold: Backed-Up Syslog Files		
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	TestDomain	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	TestDomain	
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	TestDomain1	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	TestDomain1	
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	GMSTestDomain	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	GMSTestDomain	

Add Alert Enable/Disable Alert(s) Delete Alert(s)

2 Click **Add Alert**. The Add Alert screen displays.



Add Alert

Name:	
Domain:	LocalDomai ▾
Description:	
Visible to Non-Administrators:	☑
Disable:	□
Polling Interval:	300 (in seconds: 60 - 86400)

Alert Type

Alert Type: Backed-Up Syslog Files ▾ Edit Content [Not Edited]

Description: Tracks the unprocessed syslog files on the installation. The value that the threshold will use is Numeric. This value is the number of files in the queue.

Destination / Schedule

Destination (max: 5)	Schedule
No Destinations / Schedules found	

Add Destination

Update Reset

3 Enter a **Name** and **Description** for your alert.

4 Enable **Visible to Non-Administrators** if you want your alert to be visible to non-administrators.

5 Enable **Disable** to disable this alert.

6 Enter a **Polling Interval** value (in seconds: 60-86400)

Alert Type

In the Alert Type panel you can select an alert type from the provided list and view the definitions of each alert type.

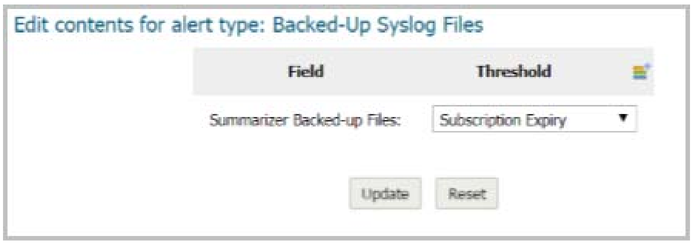
To configure an Alert Type, complete the following steps:

1. Click the **Alert Type** pull-down list and select an alert type.

   > **NOTE:** When an alert type is selected, a description for that alert is displayed in the Alert Type panel.

   Most of the Alert Types require you to edit content. Editing Contents allows the user to pick additional information, in a granular fashion, on which the alerting has to be performed.

2. Click the **Edit Content** link. The Edit Contents for Alert Type Unit Status pop-up window displays.



Edit contents for alert type: Backed-Up Syslog Files

Field	Threshold
Summarizer Backed-up Files:	Subscription Expiry ▼

3. Click the **Threshold** pull-down list and select a threshold.

   > **NOTE:** You can create a new threshold on-the-fly by clicking the icon. Only one new threshold can be created in this feature.

   > **NOTE:** If you select another Alert Type before you click Update in the Add Alert dialog box, or if you click Reset, you lose the on the fly Threshold that you created and the Edit Content status becomes Not Edited.

4. Click **Update**. To reset the settings, click **Reset**.

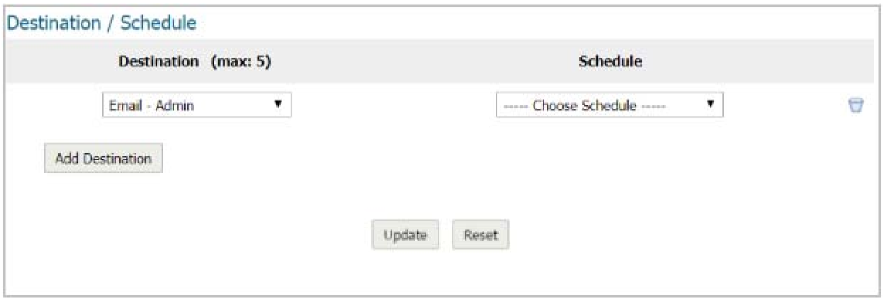
Destination / Schedule

In the Destination / Schedule panel you can add up to five destinations and set a schedule for each.

To add a destination and set a schedule, complete the following steps:

> **NOTE:** Every selected destination is required to have a schedule set.

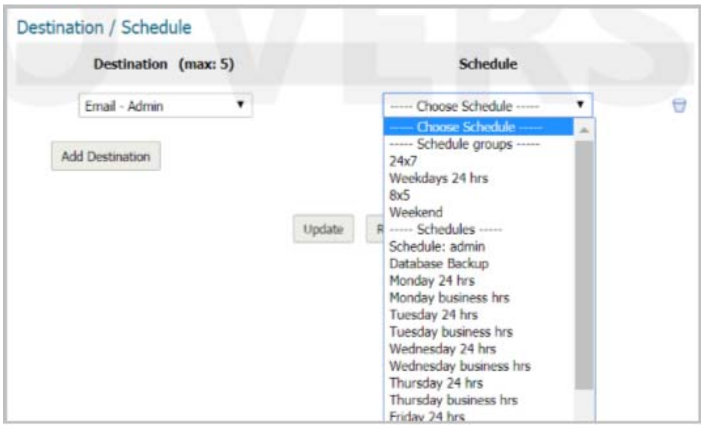
1. Click the **Add Destination** link under the Destination/Schedule section. The Destination field designates where you want alerts to be sent. You have a maximum number of five destinations.



Destination / Schedule

Destination (max: 5)	Schedule
Email - Admin ▼	----- Choose Schedule ----- ▼

2 Click the **Schedule** pull-down list, then select a schedule type. The Schedule field designates the frequency of when you want alerts to be sent to the destination(s).



3 Click **Update** to finish adding an alert.

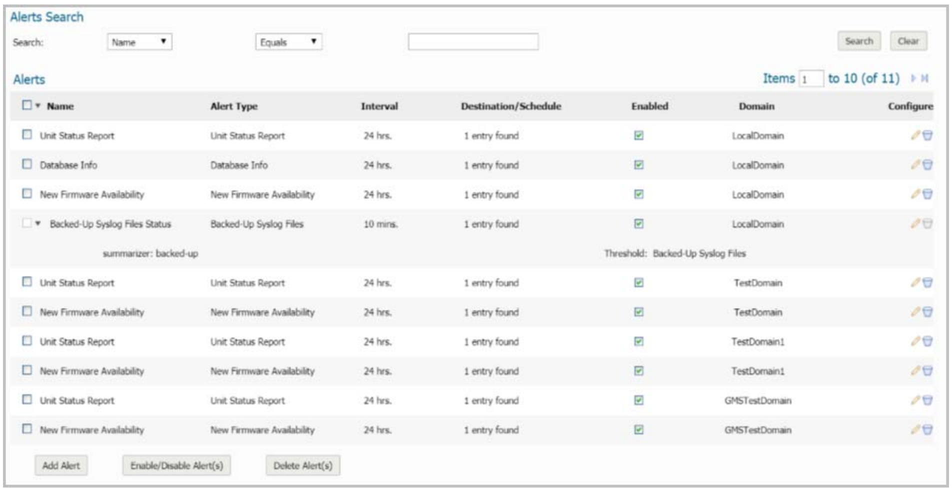
Enabling/Disabling Alerts

To enable and disable an alert, complete the following steps:

Enabling a Alert

1 Select the **Enabled** check-box next to the alert(s) you wish to enable.

2 Click the **Enable/Disable Alert(s)** link. A confirmation window displays. Click **OK** to enable or disable.

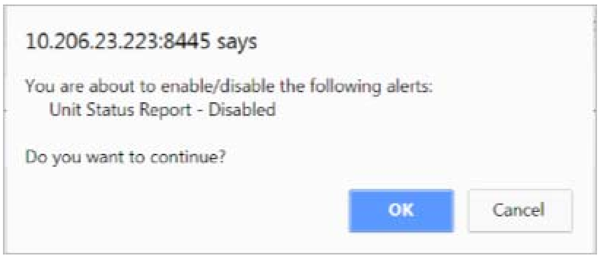


□ Name	Alert Type	Interval	Destination/Schedule	Enabled	Domain	Configure
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	LocalDomain	
□ Database Info	Database Info	24 hrs.	1 entry found	☑	LocalDomain	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	LocalDomain	
□ ▾ Backed-Up Syslog Files Status	Backed-Up Syslog Files	10 mins.	1 entry found	☑	LocalDomain	
summarizer: backed-up				Threshold: Backed-Up Syslog Files		
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	TestDomain	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	TestDomain	
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	TestDomain1	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	TestDomain1	
□ Unit Status Report	Unit Status Report	24 hrs.	1 entry found	☑	GMSTestDomain	
□ New Firmware Availability	New Firmware Availability	24 hrs.	1 entry found	☑	GMSTestDomain	

Disabling an Alert

1 Deselect **Enabled** of the alert(s) you wish to disable.

2 Click the **Enable/Disable Alert(s)** link. A confirmation window displays. Click **OK** to enable or disable.



10.206.23.223:8445 says

You are about to enable/disable the following alerts:
Unit Status Report - Disabled

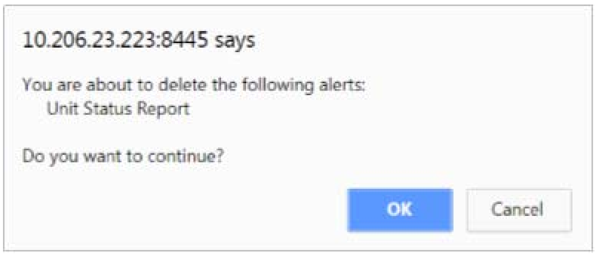
Do you want to continue?

Deleting Alerts

To delete an alert, complete the following steps:

1 Select the check box(es) of the Alert(s) you wish to delete.

2 Click the **Delete Alert** link. A confirmation window displays.



10.206.23.223:8445 says

You are about to delete the following alerts:
Unit Status Report

Do you want to continue?

3 Click **OK** to delete.

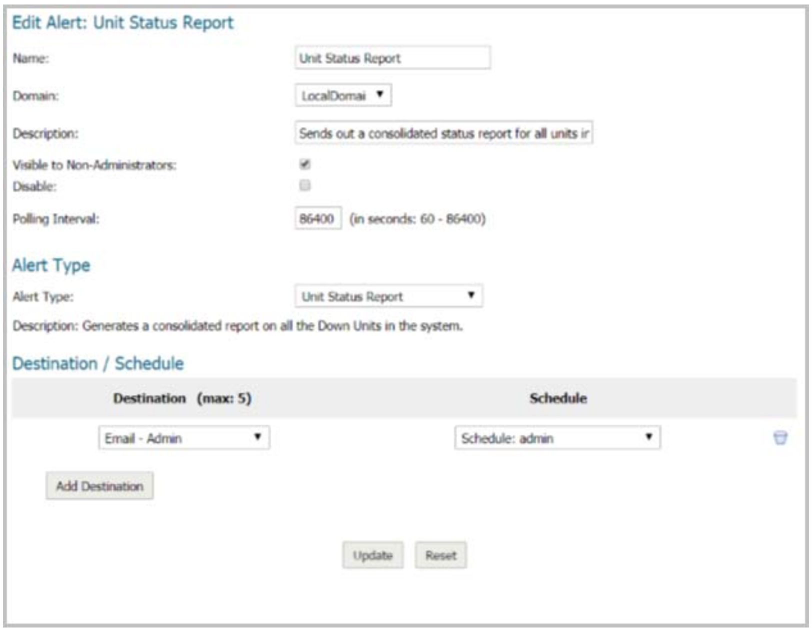
ⓘ **NOTE:** You can also delete an alert by clicking the Delete icon under the Configure section of the alert you wish the delete.

Editing Alerts

After an alert is created, you can go back and edit it at any time.

To edit an alert, complete the following steps:

1. Click the **Configure** icon of the alert you wish to edit. The **Edit Alert** page displays.



Edit Alert: Unit Status Report

Name:	Unit Status Report
Domain:	LocalDomai
Description:	Sends out a consolidated status report for all units ir
Visible to Non-Administrators:	☑
Disable:	□
Polling Interval:	86400 (in seconds: 60 - 86400)

Alert Type

Alert Type: Unit Status Report

Description: Generates a consolidated report on all the Down Units in the system.

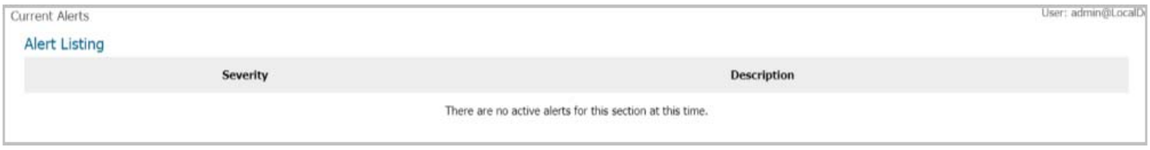
Destination / Schedule

Destination (max: 5)	Schedule
Email - Admin	Schedule: admin

2. Refer to Add Alert on page 100 and follow the configuration procedures to edit your existing Alert.

Viewing Current Alerts

You can view a list of current alerts on the **| Events > Current Alerts** page on the **CONSOLE**, **FIREWALL**, **SMA**, or **EMAIL SECURITY (ES)** views. Select a global view, group, or unit to view current alerts for your selection.



Current Alerts

User: admin@LocalD

Alert Listing

Severity	Description

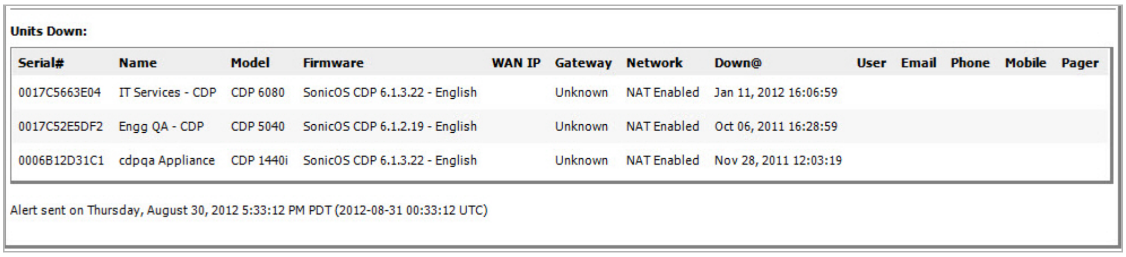
There are no active alerts for this section at this time.

Email Alert Formats

The types of alert emails are available in the following formats:

- HTML
- Plain Text
- Plain Text (simple)

HTML Email Alert Format

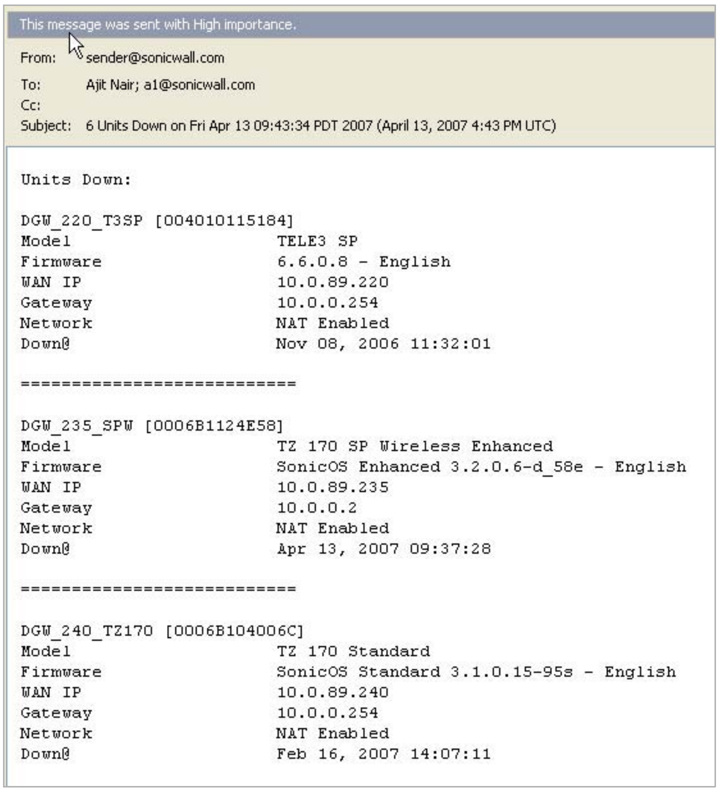


Units Down:

Serial#	Name	Model	Firmware	WAN IP	Gateway	Network	Down@	User	Email	Phone	Mobile	Pager
0017C5663E04	IT Services - CDP	CDP 6080	SonicOS CDP 6.1.3.22 - English		Unknown	NAT Enabled	Jan 11, 2012 16:06:59					
0017C52E5DF2	Engg QA - CDP	CDP 5040	SonicOS CDP 6.1.2.19 - English		Unknown	NAT Enabled	Oct 06, 2011 16:28:59					
0006B12D31C1	cdpqa Appliance	CDP 1440i	SonicOS CDP 6.1.3.22 - English		Unknown	NAT Enabled	Nov 28, 2011 12:03:19					

Alert sent on Thursday, August 30, 2012 5:33:12 PM PDT (2012-08-31 00:33:12 UTC)

Plain Text



This message was sent with High importance.

From: sender@sonicwall.com

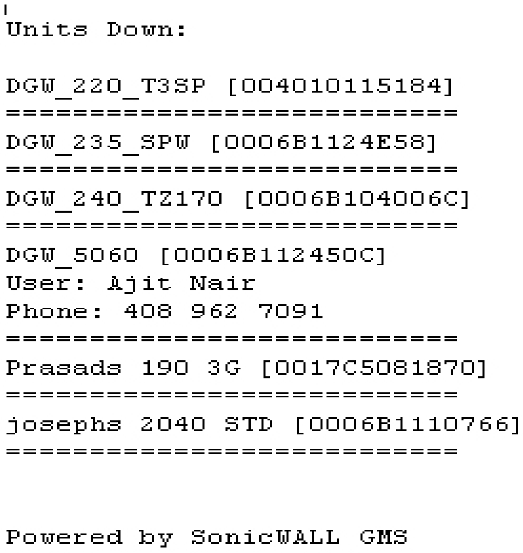
To: Ajit Nair; a1@sonicwall.com

Cc:

Subject: 6 Units Down on Fri Apr 13 09:43:34 PDT 2007 (April 13, 2007 4:43 PM UTC)

```
Units Down:

DGW_220_T3SP [004010115184]
Model                    TELE3 SP
Firmware                 6.6.0.8 - English
WAN IP                   10.0.89.220
Gateway                  10.0.0.254
Network                  NAT Enabled
Down@                    Nov 08, 2006 11:32:01

===========================

DGW_235_SPW [0006B1124E58]
Model                    TZ 170 SP Wireless Enhanced
Firmware                 SonicOS Enhanced 3.2.0.6-d_58e - English
WAN IP                   10.0.89.235
Gateway                  10.0.0.2
Network                  NAT Enabled
Down@                    Apr 13, 2007 09:37:28

===========================

DGW_240_TZ170 [0006B104006C]
Model                    TZ 170 Standard
Firmware                 SonicOS Standard 3.1.0.15-95s - English
WAN IP                   10.0.89.240
Gateway                  10.0.0.254
Network                  NAT Enabled
Down@                    Feb 16, 2007 14:07:11
```

Plain Text (Simple)



```
Units Down:

DGW_220_T3SP [004010115184]
===========================
DGW_235_SPW [0006B1124E58]
===========================
DGW_240_TZ170 [0006B104006C]
===========================
DGW_5060 [0006B112450C]
User: Ajit Nair
Phone: 408 962 7091
===========================
Prasads 190 3G [0017C5081870]
===========================
josephs 2040 STD [0006B1110766]
===========================


Powered by SonicWALL GMS
```

10

Managing Licenses

This chapter provides information about GMS licensing, registration, upgrading to new versions, and applying software patches.

Topics:

- GMS License on page 107
- SonicWall Upgrades on page 110

GMS License

The following sections describe how to manage GMS licenses.

Topics:

- Upgrading a Demo License to a Retail License on page 107
- Product Licenses on page 108

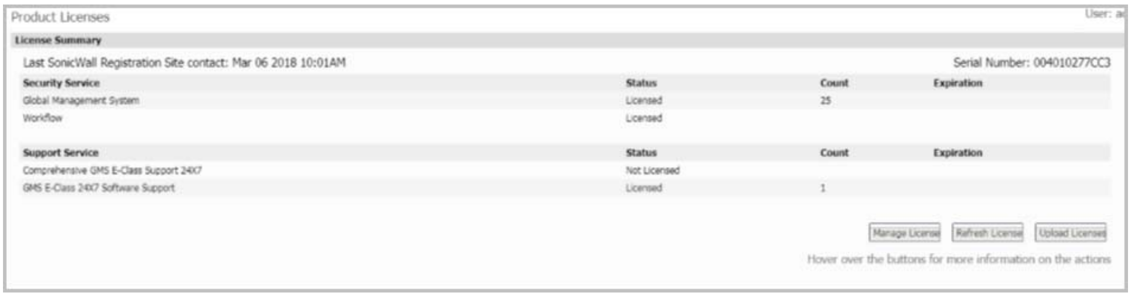
Upgrading a Demo License to a Retail License

The following sections describe how to upgrade a GMS demo license to a retail license.

Upgrading within the Demo Period

To upgrade a GMS demo license to a retail license within the demo period, complete the following steps:

1 Navigate to **CONSOLE | Licenses > Product Licenses**. The Product License summary page displays. If prompted to login, enter your MySonicWall.com **User name** and **password** before continuing.



Product Licenses

User: a

License Summary

Last SonicWall Registration Site contact: Mar 06 2018 10:01AM

Serial Number: 004010277CC3

Security Service	Status	Count	Expiration
Global Management System	Licensed	25	
Workflow	Licensed		

Support Service	Status	Count	Expiration
Comprehensive GMS E-Class Support 24X7	Not Licensed		
GMS E-Class 24X7 Software Support	Licensed	1	

Hover over the buttons for more information on the actions

2 Enter the activation code in the **Activation Code** field and click **Upgrade.**

The License Type changes to Retail License and the Current Nodes Allowed changes from 10 to 25.

Upgrading Outside the Demo Period

To upgrade a GMS demo license to a retail license after the demo period expires, complete the following steps:

1 Start GMS. The Registration page displays.

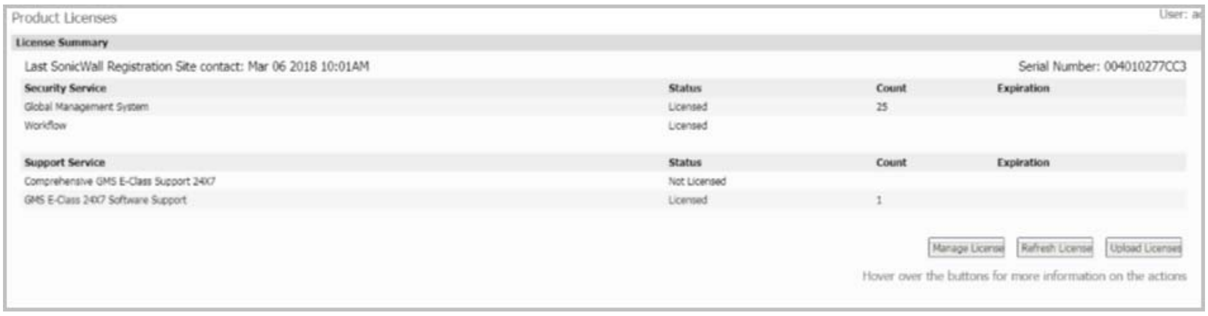
2 Enter the demo upgrade activation code and click **Update**. The Login displays and the license is upgraded.

Product Licenses

The Product Licences page allows the user to view, upload, and manage licenses and subscriptions for this GMS installation.

License Summary

View license details on the **CONSOLE | Licenses > Product Licences** page, under the License Summary section.



License Summary

Last SonicWall Registration Site contact: Mar 06 2018 10:01AM

Serial Number: 004010277CC3

Security Service	Status	Count	Expiration
Global Management System	Licensed	25	
Workflow	Licensed		

Support Service	Status	Count	Expiration
Comprehensive GMS E-Class Support 24X7	Not Licensed		
GMS E-Class 24X7 Software Support	Licensed	1	

This section allows you to view the following information about security services and support services:

Status—Displays whether the product is licensed or not licensed

Count—Displays the remaining number of licenses for this service.

Expiration—Displays the expiration date of the service (if applicable).

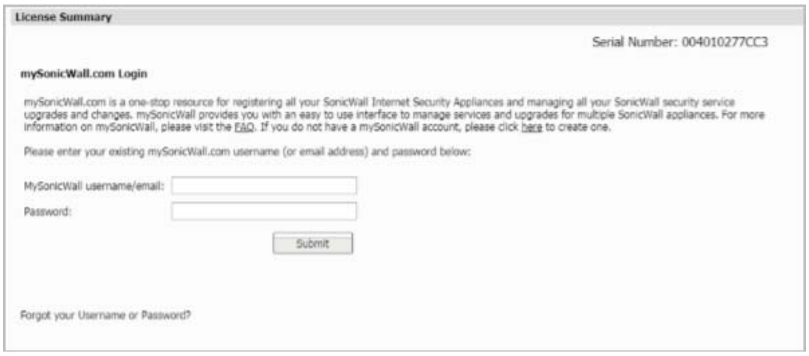
Managing Licenses

This feature allows licenses to be managed through your MySonicWall.com account.

To manage licenses:

1 Navigate to **CONSOLE | Licenses > Product Licenses**. The Product Licenses page appears.

2 Click **Manage Licenses**. The MySonicWall login page displays.



Serial Number: 004010277CC3

mySonicWall.com Login

mySonicWall.com is a one-stop resource for registering all your SonicWall Internet Security Appliances and managing all your SonicWall security service upgrades and changes. mySonicWall provides you with an easy to use interface to manage services and upgrades for multiple SonicWall appliances. For more information on mySonicWall, please visit the FAQ. If you do not have a mySonicWall account, please click here to create one.

Please enter your existing mySonicWall.com username (or email address) and password below:

MySonicWall username/email:

Password:

Forgot your Username or Password?

3 Log in with your MySonicWall credentials to manage your licenses.

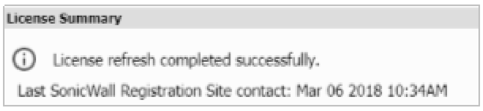
Refreshing Licenses

This feature allows the administrator to synchronize GMS with the MySonicWall license server. Synchronization is useful if you have recently purchased new licenses, and these licenses are not yet appearing in the summary page.

To refresh licenses:

1 Navigate to **CONSOLE | Licenses > Product Licenses**. The Product Licenses page appears.

2 Click **Refresh Licenses**. The License Summary page displays a message, and the date of last contact changes to reflect this.



License refresh completed successfully.

Last SonicWall Registration Site contact: Mar 06 2018 10:34AM

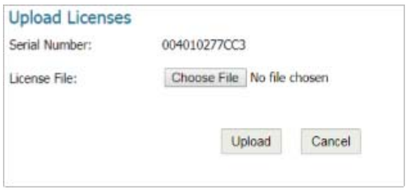
Manually Uploading a License

Normally, MySonicWall communicates with your GMS installation to synchronize licenses automatically. The manual upload feature is useful if for some reason your GMS node is without Internet connectivity.

To manually upload a license:

1 Navigate to **CONSOLE | Licenses > Product Licenses**. The Product Licenses page appears.

2 Click **Upload Licenses**. The Upload Licenses page displays.



Serial Number: 004010277CC3

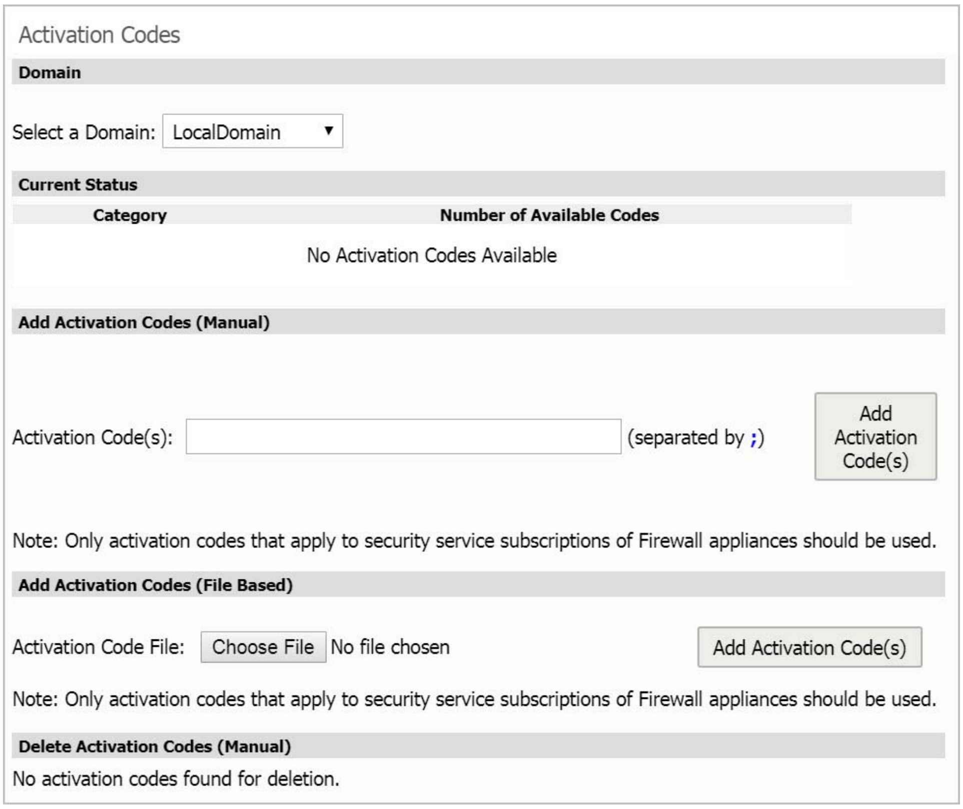
License File: No file chosen

3 Click **Choose File** to search for your locally stored license file.

> **NOTE:** License files for manual updates are available for download through your MySonicWall account.

4 Click **Upload** to complete the license transfer.

Activation Codes



Activation Codes

Domain

Select a Domain: LocalDomain ▾

Current Status

Category	Number of Available Codes
No Activation Codes Available	

Add Activation Codes (Manual)

Activation Code(s): (separated by ;) [Add Activation Code(s)]

Note: Only activation codes that apply to security service subscriptions of Firewall appliances should be used.

Add Activation Codes (File Based)

Activation Code File: [Choose File] No file chosen [Add Activation Code(s)]

Note: Only activation codes that apply to security service subscriptions of Firewall appliances should be used.

Delete Activation Codes (Manual)

No activation codes found for deletion.

SonicWall Upgrades

This section describes the procedures for upgrading SonicWall appliances. This functionality includes adding nodes, content filter subscriptions, VPN functionality, VPN clients, anti-virus licenses, and more.

When a GMS subscription service (such as warranty support, anti-virus, or content filtering) is about to expire, the GMS administrator receives expiration notifications through email prior to the expiration. The email notification is sent once a day (if applicable) and lists all managed SonicWall appliances with expiring subscription services.

To upgrade SonicWall appliances, complete the procedures listed in the following sections.

Topics:

- Upgrading the Node License on page 110
- Purchasing Upgrades on page 111
- Activating the Upgrades on page 111
- Viewing Deployments on page 112

Upgrading the Node License

Depending on the number of licenses you have ordered, you might need to add GMS licenses to configure and support additional SonicWall appliances. This section describes how to perform a node license upgrade. To view the current node license, navigate to **CONSOLE | Licenses > Product License**. The current license is displayed under the **License Summary** section.

SonicWall offers unified support packages called Comprehensive GMS Support (CGS). CGS is an annual agreement that includes:

- Technical support for the GMS application
- Software updates and upgrades for GMS
- Technical support, advanced-exchange hardware replacement and firmware updates for all of the units under GMS management

Comprehensive GMS Support is sold in increments of 25, 100, and 1,000 nodes and is available in both 8X5 and 24X7 versions. The nodes can be any combination of SonicWall firewall appliances or SMA nodes. Currently SonicWall Email Security is not included in CGS packets.

Purchasing Upgrades

To purchase upgrades, complete the following steps:

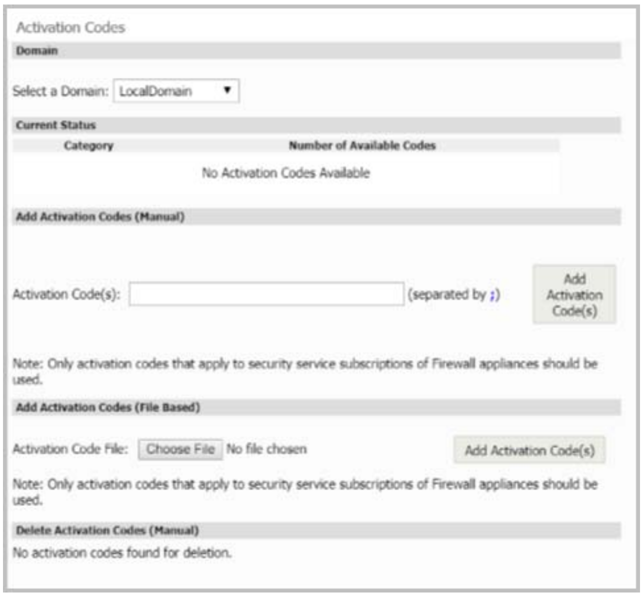
1 Contact your SonicWall sales representative through https://support.sonicwall.com/. You will receive an activation code for each upgrade that you purchase.

2 After receiving the activation codes for the SonicWall upgrades, continue to the next section.

Activating the Upgrades

To license upgrades, complete the following steps:

1 Navigate to **CONSOLE | Licenses > Activation Codes**. The SonicWall Activation Codes page displays.



Activation Codes

Domain

Select a Domain: LocalDomain

Current Status

Category	Number of Available Codes
No Activation Codes Available	

Add Activation Codes (Manual)

Activation Code(s): (separated by ;)

Note: Only activation codes that apply to security service subscriptions of Firewall appliances should be used.

Add Activation Codes (File Based)

Activation Code File: No file chosen

Note: Only activation codes that apply to security service subscriptions of Firewall appliances should be used.

Delete Activation Codes (Manual)

No activation codes found for deletion.

2 To manually add one or more activation codes, in the **Add Activation Code (manual)** field, enter a list of activation codes separated by semi-colons.

3 Click **Add Activation Code(s)**.
GMS validates the codes with the backend server and then adds them to the GMS license pool database

if they are valid. The **CONSOLE | Log > View Log** screen provides more information on success/failure of individual activation codes.

4 To delete activation codes, select one or more codes under the **Delete Activation Codes (Manual)** section and click **Delete Activation Code(s)**.

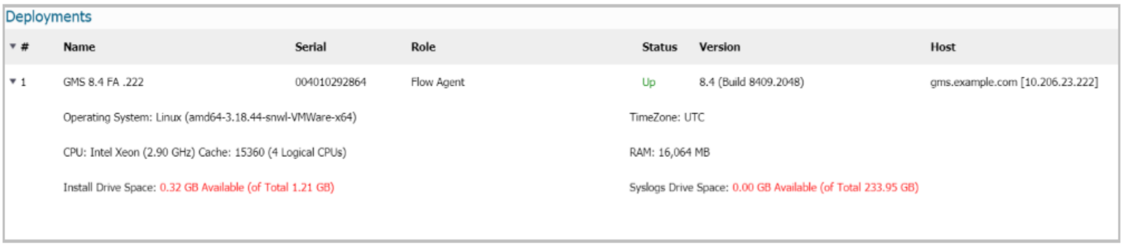
5 To add a large number of activation codes from a file, click **Choose File** under **Add Activation Codes (File Based)** to select the file. Then, click **Add Activation Code(s)** and follow the on-screen prompts.
The file can contain multiple activation codes - each line in the file has a single activation code. After the operation is completed, the **CONSOLE | Log > View Log** screen has more detailed information on the success/failure of individual activation codes that were provided in the file. A sample file is as follows, which includes for activation codes (one per line):

- SBRG4827
- AGTRUY56
- GFKJASLJ

Viewing Deployments

The **CONSOLE | Licenses > Deployments** page displays the following information about your GMS deployments:

- **Name**
- **Serial**
- **Role**
- **Status**
- **Version**
- **Host**—This field accepts/displays IPv4 and IPv6 addresses.



Deployments

▾ #	Name	Serial	Role	Status	Version	Host
▾ 1	GMS 8.4 FA .222	004010292864	Flow Agent	Up	8.4 (Build 8409.2048)	gms.example.com [10.206.23.222]

Operating System: Linux (amd64-3.18.44-snwl-VMWare-x64)
TimeZone: UTC
CPU: Intel Xeon (2.90 GHz) Cache: 15360 (4 Logical CPUs)
RAM: 16,064 MB
Install Drive Space: 0.32 GB Available (of Total 1.21 GB)
Syslogs Drive Space: 0.00 GB Available (of Total 233.95 GB)

11

Web Services

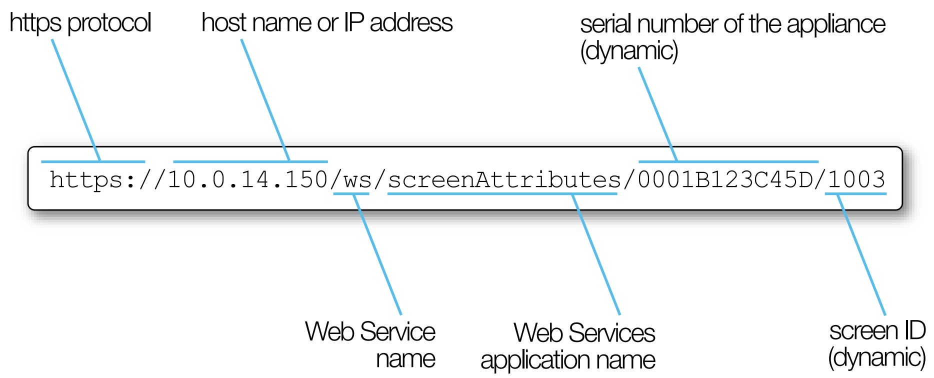
This chapter provides information about the GMS Web Services feature. Web Services is a software function designed to support interoperability between GMS and other network appliances, servers, and devices through an application programming interface (API).

Topics:

URI Basics

The URI is a SSL string which is used to identify Web Services resources. Each URI is composed of both static and dynamic parts that differ based on each particular deployment.

The following provides a typical, though not comprehensive, URI example:



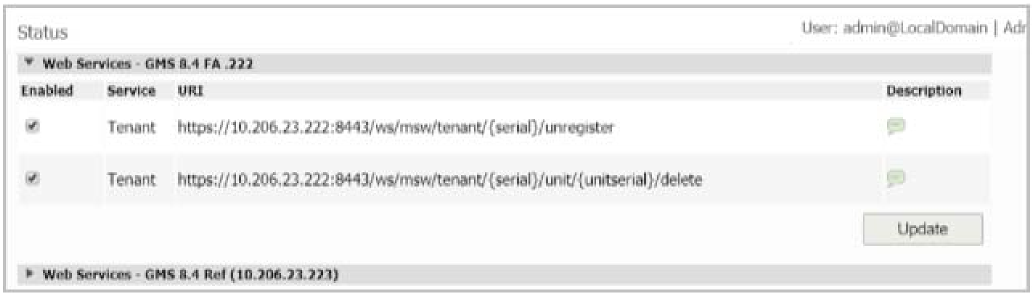
```
https://10.0.14.150/ws/screenAttributes/0001B123C45D/1003
```

Status

The status screen allows the administrator to view, enable, and disable individual Web Services across one or more GMS deployments.

To view and configure Web Services status:

1 Navigate to the **CONSOLE | Web Services > Status**. The Status page appears.



Status

User: admin@LocalDomain | Adr

▼ Web Services - GMS 8.4 FA .222

Enabled	Service	URI	Description
☑	Tenant	https://10.206.23.222:8443/ws/msw/tenant/{serial}/unregister	💬
☑	Tenant	https://10.206.23.222:8443/ws/msw/tenant/{serial}/unit/{unitserial}/delete	💬

▶ Web Services - GMS 8.4 Ref (10.206.23.223)

2 Select or deselect **Enabled** for the following service(s):

- **Appliance Status—**Provides a list of appliances currently under management by the SGMS deployment. It also includes unit statuses in the for of missed heartbeat messages (0 missed heartbeats means the unit is UP).
- **Appliance Detail—**Retrieve detailed information about the specified appliances.
- **Appliance Licenses—**Information about service licenses that apply to the specified appliance.
- **Scheduled Report List—**Provides a list of XML Scheduled Reports available for download through Web Services.
- **Scheduled Report Retrieval—**Retrieves the specified XML Scheduled Report.
- **License Alert List—**Provides a list of appliance license alerts.
- **Console Logs—**Provides the most recent log entries (up to 200) from the GMS console.
- **Appliance Alerts—**Provides a list of appliance specific alerts.
- **System Alerts—**Provides a list of alerts that apply to the GMS system.
- **All Appliance Licenses—**Provides license information for all of the appliances.

3 Click **Update** to save your changes.

4 The Web Services table, in the **CONSOLE | Web Services > Status** screen gives the following information about each Web Service:

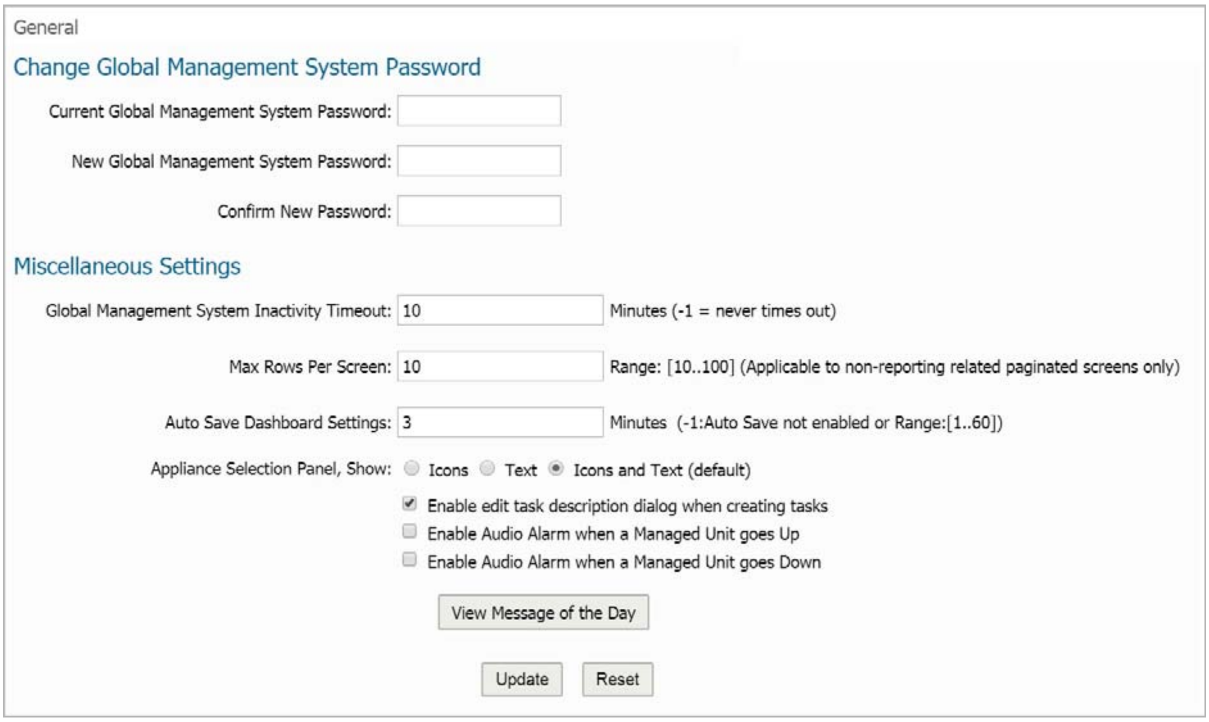
Web Services Information

Feature	Description
Enabled	If selected, this feature is currently enabled
Service	Indicates the name of the Web Service
URI	Indicates the full URI used to access this Web Service. This field can accept/display IPv4 and IPv6 addresses.
Description	Provides a description of the Web Service

12

Configuring User Settings

This chapter describes how to configure the user settings on the **CONSOLE | User Settings > General User** page that provides a way to change the GMS administrator password, the GMS inactivity Timeout, and pagination settings.



General

Change Global Management System Password

Current Global Management System Password:

New Global Management System Password:

Confirm New Password:

Miscellaneous Settings

Global Management System Inactivity Timeout: 10 Minutes (-1 = never times out)

Max Rows Per Screen: 10 Range: [10..100] (Applicable to non-reporting related paginated screens only)

Auto Save Dashboard Settings: 3 Minutes (-1:Auto Save not enabled or Range:[1..60])

Appliance Selection Panel, Show: ○ Icons ○ Text ● Icons and Text (default)

☑ Enable edit task description dialog when creating tasks

□ Enable Audio Alarm when a Managed Unit goes Up

□ Enable Audio Alarm when a Managed Unit goes Down

To configure the user settings navigate to CONSOLE | User Settings > General page and complete the following steps:

1 Enter the existing GMS password in the **Current GMS Password** field.

2 Enter the new GMS password in the **New GMS Password** field.

3 Reenter the new password in the **Confirm New Password** field.

> **NOTE:** Password fields are grayed out for users on a Remote Domain.

4 The GMS Inactivity Timeout period specifies how long GMS waits before logging out an inactive user. To prevent someone from accessing the GMS UI when GMS users are away from their desks, enter an appropriate value in the **GMS Inactivity Timeout** field. You can disable automatic logout completely by entering a “-1” in this field. The minimum is five minutes and the maximum is 120 minutes.

5 Select a value between 10 and 100 in the **Max Rows Per Screen** field. This value applies only to non-reporting related paginated screens.

6 The **Appliance Selection Panel** options determine how devices are displayed in the far left panel. You can display only icons (the **Icons** option), only the name of the appliance (**Text**), or both icons and names

(**Icons and text**), or use the default GMS display settings for this user (**Use default**). The default is **Icons and Text**.

7 To configure GMS to display an editable task description each time a task is generated, select **Enable edit task description dialog when creating tasks**.

8 To have GMS play an audio alert when an appliance goes up, check **Enable Audio Alarm when a Managed Unit goes Up**.

9 To have GMS play an audio alert when an appliance goes down, check **Enable Audio Alarm when a Managed Unit goes Down**.

To customize the audio alerts, place .WAV files in the following directory:

[SGMS2]\Tomcat\webapps\sgms\com\sonicwall\sgms\applets\common

The file names for an appliance going up and down must be *up_custom.wav* and *down_custom.wav* respectively.

10 To view the message of the day now, click **View Message of the Day**.

11 When you are finished, click **Update**. The settings are changed. To clear all screen settings and start over, click **Reset**.

ⓘ **NOTE:** The maximum size of the SonicWall GMS User ID is 24 alphanumeric characters. The password is one-way hashed and any password of any length can be hashed into a fixed 32 character long internal password.

13

Using GMS Help

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

The GMS online help provides context-sensitive conceptual overviews, configuration examples, and trouble shooting tips.

Topics:

- About GMS on page 117
- Tips and Tutorials on page 117

About GMS

The **CONSOLE | Help > About** page displays the version of GMS being run, who the GMS is licensed to, database information, and the serial number of the GMS.

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

Tips and Tutorials

To access tips and tutorials:

1. Navigate to **CONSOLE | Help > Tips and Tutorials**. The Tips and Tutorials page appears.
2. Click on a Knowledge Base article for more information.

14

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.