Multiple Administrators Support

Document Scope

This solutions document describes how to use the Multiple Administrators Support feature. This document contains the following sections:

Feature Overview

This section provides an introduction to the Multiple Administrators Support feature. This section contains the following subsections:

What is Multiple Administrators Support?

The original version of SonicOS Enhanced supported only a single administrator to log on to a SonicWALL security appliance with full administrative privileges. Additional users can be granted "limited administrator" access, but only one administrator could have full access to all areas of the SonicOS GUI at one time.

SonicOS Enhanced release 4.0 introduces support for multiple concurrent administrators. This feature allows for multiple users to log-in with full administrator privileges. In addition to using the default "admin" user name, additional administrator usernames can be created.

Because of the potential for conflicts caused by multiple administrators making configuration changes at the same time, only one administrator is allowed to make configuration changes. The additional administrators are given full access to the GUI, but it is read-only access.

Benefits

Multiple Administrators Support provides the following benefits:

- **Improved productivity** - Allowing multiple administrators to access a SonicWALL security appliance simultaneously eliminates "auto logout," a situation that occurs when two administrators require access to the appliance at the same time and one is automatically forced out of the system.
- **Reduced configuration risk** – The new read-only mode allows users to view the current configuration and status of a SonicWALL security appliance without the risk of making unintentional changes to the configuration.

How Does Multiple Administrators Support Work?

The following sections describe how the Multiple Administrators Support feature works:

Configuration Modes

In order to allow multiple concurrent administrators, while also preventing potential conflicts caused by multiple administrators making configuration changes at the same time, the following configuration modes have been created:

- **Configuration mode** - Administrator has full privileges to edit the configuration. If no administrator is already logged into the appliance, this is the default behavior.
- **Read-only mode** - Administrator cannot make any changes to the configuration, but can view the following information:
  - Browse the entire management UI.
  - Export preferences and firmware.
  - Export certificates.
  - Export the log.
  - Download the TSR.
  - Display VPN tunnel statistics.
- **Non-configuration mode** - In addition to the read-only privileges, administrators in non-configuration mode can initiate the following types of management actions that do not have the potential to cause configuration conflicts:
  - Clear and email the log, set log categories and apply log filters.
  - Generate and reset log reports.
  - Use all of the diagnostics, including the packet trace.
  - Log out logged in users and unlock locked out users.
  - Initiate LDAP/RADIUS/CIA tests (so long as no LDAP/RADIUS/CIA configuration is changed).
  - Initiate DHCP lease renewal or release on interfaces using DHCP.

- Flush the ARP cache.
- Import certificates and generate certificate signing requests.
- Initiate VPN tunnel re-negotiation
- Clear dial-up reports.

User Groups

The Multiple Administrators Support feature introduces two new default user groups:

- **SonicWALL Administrators** - Members of this group have full administrator access to edit the configuration.
- **SonicWALL Read-Only Admins** - Members of this group have full read-only access to view the management interface, but they cannot edit the configuration, and they cannot switch to full configuration mode.

It is not recommended to include users in more than one of the user groups. However, if you do so, the following behavior applies:

- If members of the **SonicWALL Administrators** user group are also included in the **Limited Administrators** or **SonicWALL Read-Only Admins** user groups, the members will have full administrator rights.
- If members of the **Limited Administrators** user group are included in the **SonicWALL Read-Only Admins** user group, the members will have limited administrator rights.

Priority for Preempting Administrators

The various classes of administrators

1. The **admin** user and SonicWALL Global Management System (GMS) both have the highest priority and can preempt any users.
2. A user that is a member of the **SonicWALL Administrators** user group can preempt any users except for the **admin** and SonicWALL GMS.
3. A user that is a member of the **Limited Administrators** user group can only preempt other members of the **Limited Administrators** group.

GMS and Multiple Administrator Support

When using SonicWALL GMS to manage a SonicWALL security appliance, GMS frequently logs in to the appliance (for such activities as ensuring that GMS management IPSec tunnels have been created correctly). These frequent GMS log-ins can make local administration of the appliance difficult because the local administrator can be preempted by GMS.


Tip

In deployments where a SonicWALL security appliance will be managed both locally and by GMS, SonicWALL recommends configuring GMS to log in as a read-only admin.

??? I need clarification on this section. Do we want to describe all three methods, or only the "login-mode" CGI tag method???

There are three methods for configuring GMS to log in as a read-only admin:

- Configure the SonicWALL security appliance automatically create a user account with read-only administrator privileges for GMS. Optionally, a full administrator account can be created for situations when GMS needs to modify the configuration.
- Configure GMS to create a user account with read-only administrator privileges.
- Implement a new “login-mode” CGI tag that can be included with the name/password etc. in a login HTML or XML post, and can be set to request read-only mode on login. GMS can then optionally log in as admin (or some other user with full administration privilege) in read-only mode, and can then later post a "change to configuration mode" request before making configuration changes.

Tip When using RADIUS or LDAP authentication, SonicWALL recommends using the **RADIUS + Local Users** or **LDAP + Local Users** options and configuring the administrator accounts locally. This ensures that administrators will be able to log in to the appliance even if the RADIUS or LDAP server becomes unreachable.

Hardware Failover and Multiple Administrators

!!! To be written !!!

Platforms

Multiple Administrators Support is available on all SonicWALL security appliances running SonicOS Enhanced 4.0.

Using Multiple Administrators Support

This section contains the following subsections:

Configuring Multiple Administrators

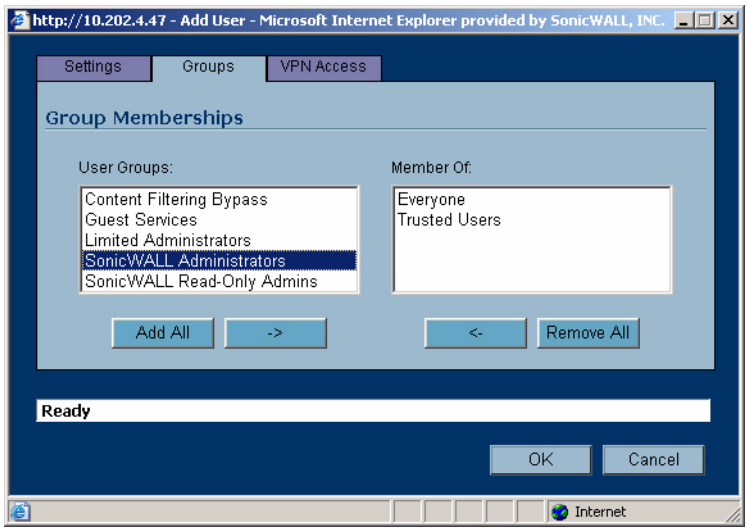
To configure multiple administrator, perform the following steps:

Step 1 While logged in as **admin**, navigate to the **Users > Local Users** page.

Step 2 Click the **Add User** button.

Step 3 Enter a **Name** and **Password** for the user.

Step 4 Click on the **Group Membership** tab.



Step 5 Select the appropriate group to give the user Administrator privileges:

- **Limited Administrators** - The user has limited administrator configuration privileges.

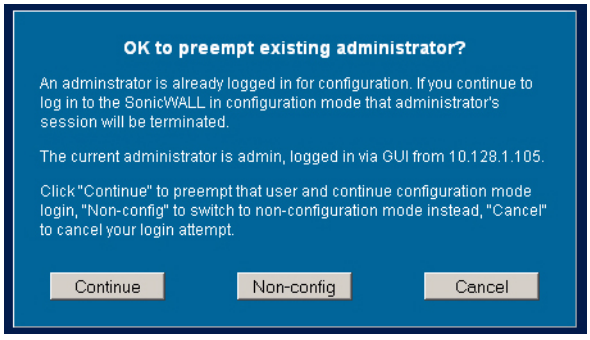
??? What does limited admin allow and disallow ???

- **SonicWALL Administrators** - The user has full administrator configuration privileges.
- **SonicWALL Read-Only Admins** - The user can view the entire management interface, but cannot make any changes to the configuration.

Step 6 Click the right arrow button and click **OK**.

Preempting Administrators

When an administrator attempts to logs in while another administrator is logged on, the following message is displayed. The message displays the current administrator's user name, IP address, and whether the administrator is logged in using the GUI or CLI.



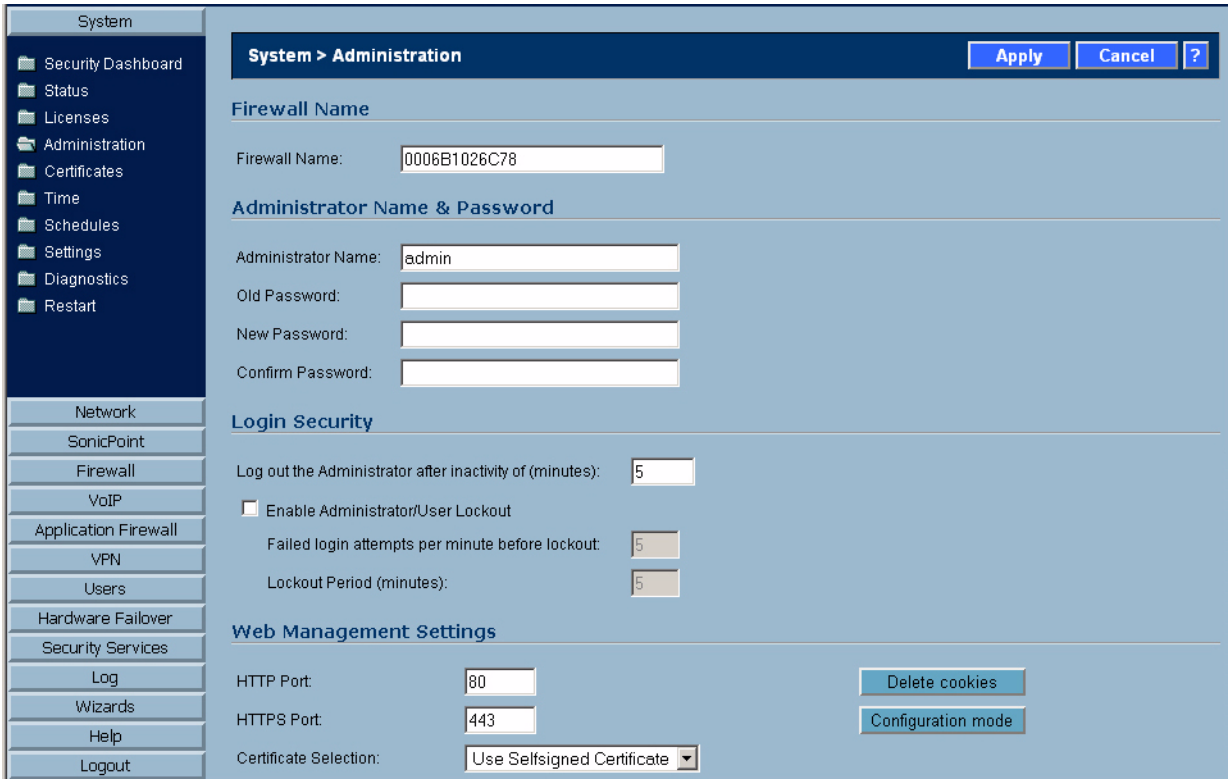
This window gives you three options:

- **Continue** - Preempts the current administrator. The current administrator is converted to read-only mode and you are given full administrator access.
- **Non-config** - You are logged into the appliance in non-config mode. The current administrator's session is not disturbed.
- **Cancel** - Returns to the authentication screen.

Activating Configuration Mode

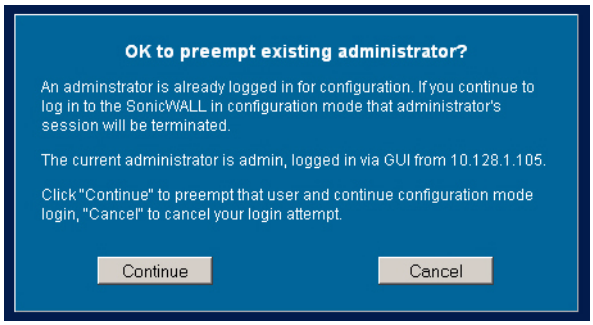
To switch from non-config mode to full configuration mode, perform the following steps:

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



Step 2 In the **Web Management Settings** section, click on the **Configuration mode** button. If there is not currently an administrator in configuration mode, you will automatically be entered into configuration mode.

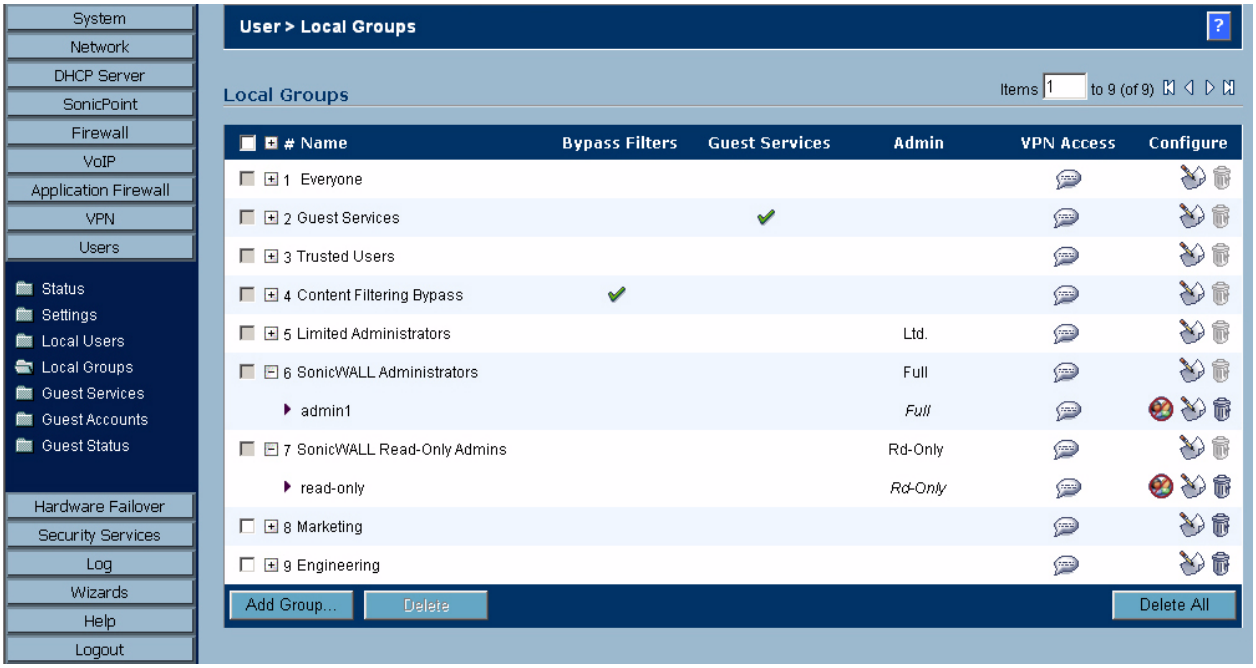
Step 3 If another administrator is in configuration mode, the following message displays.



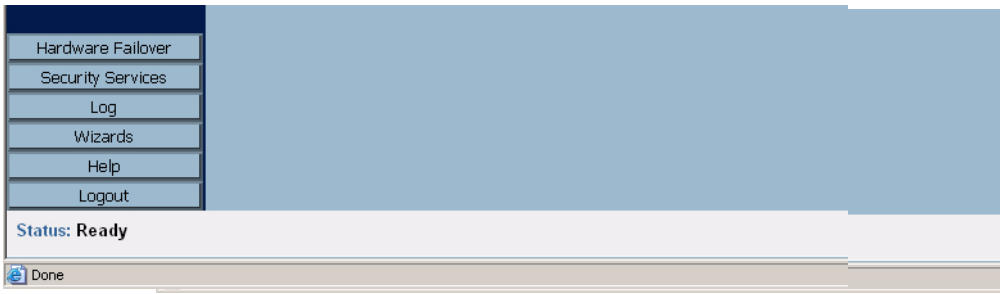
Step 4 Click the **Continue** button to enter configuration mode. The current administrator is converted to read-only mode and you are given full administrator access.

Verifying Multiple Administrators Support Configuration

User accounts with administrator and read-only administrators can be viewed on the **Users > Local Groups** page.



Administrators can determine which configuration mode they are in by looking at the status bar of their browser. To display the status bar in Firefox and Internet Explorer, click on the **View** menu and enable **status bar**. When the administrator is in full configuration mode, the status bar displays **Done**.



When the administrator is in read-only mode, the status bar displays **Read-only mode - no changes can be made**.

When the administrator is in non-config mode, the status bar displays.

!!! Need a screenshot of non-config mode status bar !!!

Viewing Multiple Administrator Related Log Messages

!!! Need to capture log messages !!!

- A GUI or CLI user begins configuration mode (including on admin login).
- A GUI or CLI user ends configuration mode (including on admin logout).
- A GUI user begins management in non-config mode (including on admin login and when a user in onfiguration mode is preempted and dropped back to read-only mode).
- A GUI user begins management in read-only mode.
- A GUI user terminates either of the above management sessions (including on admin logout).

Related Features

Solution Document Version History

Version Number	Date	Notes
1	3/22/2007	This document was created.