



SonicOS 7.1

Device Settings

Administration Guide

SONICWALL®

Contents

| | |
|--|-----------|
| About SonicOS | 5 |
| Working with SonicOS | 5 |
| SonicOS Workflow | 7 |
| How to Use the SonicOS Administration Guides | 8 |
| Guide Conventions | 9 |
| About Device Settings | 10 |
| Managing SonicWall Licenses | 11 |
| Licenses | 11 |
| Managing Security Services | 12 |
| Services Summary | 12 |
| Managing Security Services Online | 13 |
| Manual Upgrade for Closed Environments | 14 |
| Registering Your SonicWall Appliance | 15 |
| Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License | 16 |
| Activating FREE TRIALS | 16 |
| System Administration | 17 |
| Configuring the Firewall Name | 17 |
| Enabling Wireless LAN and IPv6 | 18 |
| Changing the Administrator Name and Password | 18 |
| Configuring Login Security | 19 |
| Configuring Password Compliance | 20 |
| Configuring Login Constraints | 22 |
| Multiple Administrators Support | 23 |
| Working of Multiple Administrators Support | 24 |
| Configuring Multiple Administrator Access | 27 |
| Enabling Enhanced Audit Logging Support | 28 |
| Configuring the Wireless LAN Controller | 28 |
| Enabling SonicOS API and Configuring Authentication Methods | 29 |
| Enabling GMS Management | 30 |
| Configuring the Management Interface | 32 |
| Managing through HTTP/HTTPS | 33 |
| Selecting a Security Certificate | 33 |
| Controlling the Management Interface Tables | 34 |
| Enforcing TLS Version | 35 |

| | |
|--|-----------|
| Switching Configuration Modes | 35 |
| Deleting Browser Cookies | 36 |
| Configuring SSH Management | 36 |
| Client Certificate Verification | 37 |
| About Common Access Card | 37 |
| Configuring Client Certificate Verification | 38 |
| Using the Client Certificate Check | 39 |
| Checking Certificate Expiration | 40 |
| Troubleshooting User Lock Out | 40 |
| Selecting a Language | 41 |
| Configuring Time Settings | 42 |
| Setting System Time | 43 |
| Configuring NTP Settings | 44 |
| Using a Custom NTP Server for Updating the Firewall Clock | 45 |
| Adding an NTP Server | 45 |
| Editing an NTP Server Entry | 46 |
| Deleting NTP Server Entry | 46 |
| Managing Certificates | 48 |
| About Digital Certificates | 48 |
| About the Certificates Table | 49 |
| About Certificate Details | 50 |
| Importing Certificates | 50 |
| Importing a Local Certificate | 51 |
| Importing a Certificate Authority Certificate | 52 |
| Creating a PKCS-12 Formatted Certificate File (Linux Systems Only) | 52 |
| Deleting Certificates | 54 |
| Generating a Certificate Signing Request | 55 |
| Configuring Simple Certificate Enrollment Protocol | 60 |
| Administering SNMP | 62 |
| About SNMP | 62 |
| Setting Up SNMP Access | 63 |
| Enabling and Configuring SNMP Access | 63 |
| Setting Up SNMPv3 Groups and Access | 68 |
| Configuring SNMP as a Service and Adding Rules | 71 |
| Firmware Settings | 72 |
| Firmware Management and Backup | 72 |
| Firmware Management & Backup Tables | 73 |
| Searching the Table | 75 |
| Creating a Backup Firmware Image | 76 |
| Creating a Local Backup Firmware Image | 76 |

| | |
|---|------------|
| Creating a Cloud Backup Firmware Image | 77 |
| Scheduling Firmware Image Backups | 78 |
| Updating Firmware | 81 |
| Updating Firmware Manually | 81 |
| Firmware Auto Update | 82 |
| Using SafeMode to Upgrade Firmware | 83 |
| Importing and Exporting Settings | 84 |
| Importing Settings | 84 |
| Exporting Settings | 85 |
| Configuring Firmware and Backup Settings | 86 |
| Send Settings or Reports by FTP | 86 |
| Sending Diagnostic Reports to Technical Support | 88 |
| Boot Settings | 89 |
| One-Touch Configuration Overrides | 89 |
| Enabling FIPS Mode | 90 |
| Enabling NDPP mode | 92 |
| Storage | 94 |
| Storage Overview Tab | 95 |
| Diagnostics Data | 96 |
| Configuration Backup | 97 |
| System Logs | 98 |
| Threat Logs | 99 |
| Packet Captures | 100 |
| Logs (Legacy) | 102 |
| Restarting the System | 103 |
| SonicWall Support | 104 |
| About This Document | 105 |

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on

Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

| Firewall Type | Classic Mode | Policy Mode | Comments |
|------------------------------------|--------------|-------------|---|
| TZ Series | yes | no | The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support. |
| NSa Series | yes | no | NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management. |
| NSsp 10700, NSsp 11700, NSsp 13700 | yes | no | The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need. |
| NSsp 15700 | no | yes | The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability. |
| NSv Series | yes | yes | The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed. |

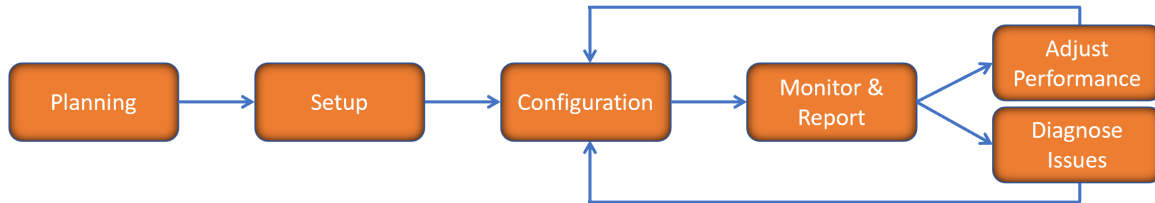
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- [SonicOS 7.1 API Reference Guide](#)

- [SonicOS Command Line Interface Reference Guide](#)

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

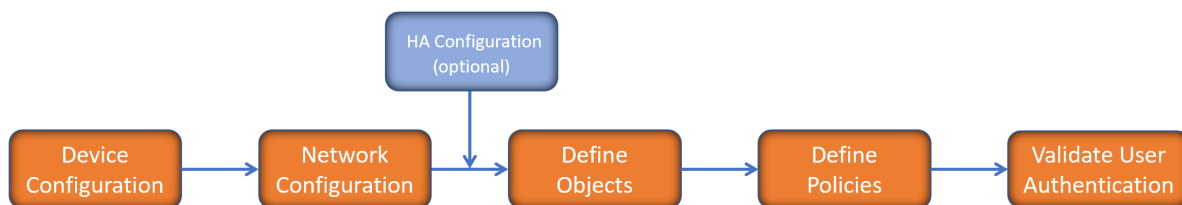


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

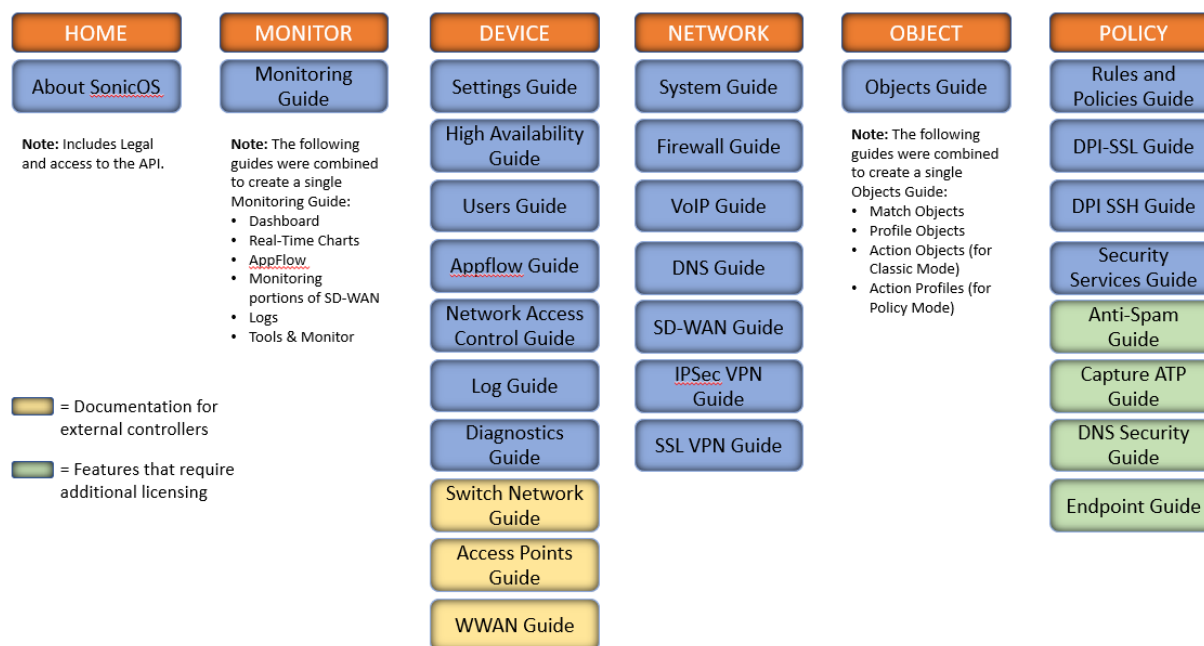


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the *SonicOS 7.1 Monitor Guide* and the *SonicOS 7.1 Objects Guide* which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the <https://www.sonicwall.com/support/technical-documentation/>.

Guide Conventions

These text conventions are used in this guide:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

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

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

| Convention | Description |
|---|---|
| Bold text | Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface. |
| Function Menu group > Menu item | Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page. |
| Code | Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface. |
| <Variable> | Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number> , replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004 . |
| Italics | Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept. |

About Device Settings

The web-based SonicOS Management Interface enables you to configure SonicWall network security appliances (firewalls).

This document provides information on:

- [Managing SonicWall Licenses](#)
- [System Administration](#)
- [Configuring Time Settings](#)
- [Managing Certificates](#)
- [Administering SNMP](#)
- [Firmware Settings](#)
- [Restarting the System](#)

Managing SonicWall Licenses

IMPORTANT: By design, the SonicWall License Manager cannot be configured to use a third-party proxy server. Networks that direct all HTTP and HTTPS traffic through a third-party proxy server may experience License Manager issues.

Topics:

- [Licenses](#)
- [Managing Security Services](#)
- [Registering Your SonicWall Appliance](#)
- [Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License](#)
- [Activating FREE TRIALS](#)

Licenses

Device | Settings > Licenses page in the SonicOS management interface provides links to activate, upgrade, or renew SonicWall Security Services licenses. From this page, you can manage all the licenses for your SonicWall security appliance. The information listed in the **Services** table is updated from your mysonicwall.com account. The **Licenses** page also includes links to FREE trials of SonicWall Security Services.

| SERVICES | STATUS | EXPIRY DATE | ACTIONS |
|---|--------------------------------------|-------------|------------------------|
| View: Licensed and Unlicensed Friendly Name: TZ570-157 MySonicWall Synchronize Manual License | | | |
| Service Bundles (0 licensed) | | | |
| Management & Analytics Services (1 licensed) | | | |
| Gateway Services (5 licensed) | | | |
| Gateway Anti-malware/Intrusion Prevention/App Control | Licensed | 28 Jan 2021 | Renew Start Trial |
| Content Filtering Service | Licensed | 28 Jan 2021 | Renew Start Trial |
| Comprehensive Anti-Spam Service | Licensed | 28 Jan 2021 | Renew Start Trial |
| Capture Advanced Threat Protection | Licensed | 28 Jan 2021 | Renew Start Trial |
| Stateful High Availability | Licensed | | |
| Endpoint & Remote Access Services (2 licensed) | | | |
| Capture Client | Unlicensed | | Manage License Sharing |
| Global VPN Client | Licensed Count: 2 MaxCount: 500 | | Upgrade Start Trial |
| SSL VPN | Licensed Count: 2 MaxCount: 200 | | Upgrade Start Trial |

Managing Security Services

When you have established your Internet connection, it is recommended you register your SonicWall security appliance, which provides the following benefits:

- Try a FREE 30-day trial of SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention, Content Filtering Service, and Client Anti-Virus
- Activate SonicWall Anti-Spam
- Activate SonicWall security services and upgrades
- Access SonicOS firmware updates
- Get SonicWall technical support

Topics:

- [Services Summary](#)
- [Managing Security Services Online](#)

Services Summary

The **Device | Settings > Licenses** page lists all the available and activated services on the SonicWall security appliance. The friendly name of the security appliance is displayed above the **SERVICES** table.

Select appropriate option in the **View** drop-down box to list the services based on their activation status. The available options are:

- **Licensed and Unlicensed**
- **Licensed**
- **Unlicensed**

| SERVICES | STATUS | EXPIRY DATE | ACTIONS |
|---|------------|-------------|---------------------------|
| Service Bundles (0 licensed) | | | |
| ▶ Essential Protection Services Suite | Unlicensed | | ⚙️ Activate ⌚ Start Trial |
| ▶ Advanced Protection Services Suite | Unlicensed | | |
| Management & Analytics Services (1 licensed) | | | |
| Gateway Services (5 licensed) | | | |
| Endpoint & Remote Access Services (2 licensed) | | | |
| Support & Consulting Services (3 licensed) | | | |
| Miscellaneous Services (1 licensed) | | | |

The table displays the following information:

- **SERVICES** - lists all the available SonicWall Security Services and upgrades available for the SonicWall security appliance.
- **STATUS** - indicates if the security service is activated (Licensed), available for activation (Not Licensed), or no longer active (Expired).
- **ACTION** - displays options to upgrade, renew, try, or activate the service, depending on its license status.

- **Count** - displays the number of nodes/users currently connected to your appliance. If your security appliance is licensed for unlimited nodes, the count is displayed as Unlimited.
- **Max. Count** - displays the maximum number of nodes/users allowed for the license.
- **EXPIRY DATE** - displays the expiration date for any Licensed Security Service.

The information listed in the **Services** table is updated from your mysonicwall.com account the next time the SonicWall security appliance automatically synchronizes with MySonicWall (once a day) or you can click the **SYNCHRONIZE** button on this page to update the table.

For more information on SonicWall Security Services, see *SonicOS 7.0 Security Services* document available at <https://www.sonicwall.com/support/technical-documentation/>.

Managing Security Services Online

You can activate, upgrade or renew services using one of the following methods:

- Performing service license updates in MySonicWall and synchronizing the changes in SonicOS management interface.
 1. Navigate to **Device | Settings > Licenses** page.
 2. Click **MySonicWall** above the **Services** table.
 3. Log into your MySonicWall account and upgrade the licenses. See MSW online help.
 4. Synchronize changes. See [Synchronizing Changes](#).
- Performing service license updates through SonicOS management interface. See [Managing Services from SonicOS Management Interface](#).

Topics:

- [Managing Services from SonicOS Management Interface](#)
- [Synchronizing Changes](#)

Managing Services from SonicOS Management Interface

You can activate, upgrade, or renew licenses for the Security Services on **Device | Settings > Licenses** page.

To activate, upgrade, or renew services:

1. **Navigate to Device | Settings > Licenses.**
2. Select the appropriate option in the **View** drop-down box above the **SERVICES** table.
3. Locate the service you want to activate / renew / upgrade.
4. Click any option listed in the **ACTIONS** column based on what you need to do with the service.

The options listed for a service in the **ACTIONS** column depend on the status of the service.

 - To activate a FREE trial, click **Try**.
 - To activate a Security Service, click the **Activate** link.
 - To renew a Security Service, click the **Renew** link.

- To upgrade a Security Service, click the **Upgrade**.
5. Follow the prompts to activate/renew/upgrade the service license. After completion, you are returned to the **Licenses** page.

Synchronizing Changes

When you make changes to your Security Services in MySonicWall, you can synchronize them instead of waiting for the system to do it automatically.

To synchronize your MySonicWall account with the Services table in SonicOS management interface:

1. Navigate to **Device | Settings > Licenses** .
2. Click **Synchronize** option above the **SERVICES** table.

Manual Upgrade for Closed Environments

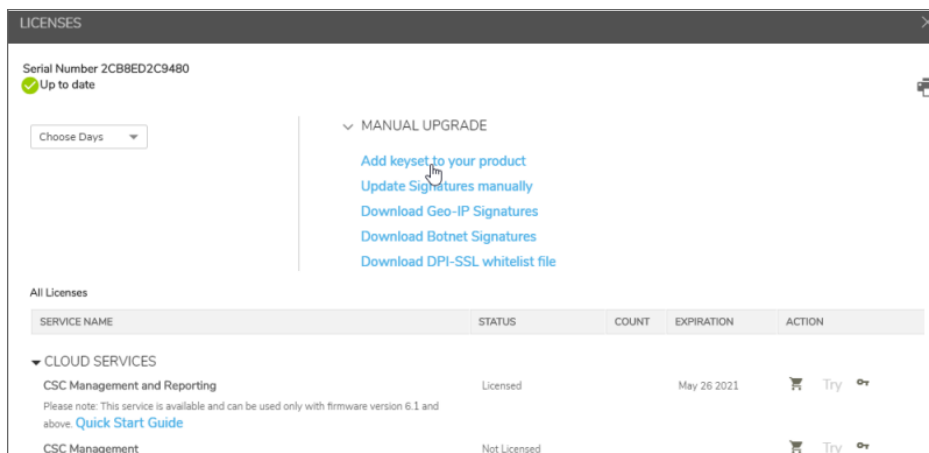
If your SonicWall security appliance is deployed in a high-security environment that does not allow direct Internet connectivity from the SonicWall security appliance, you can enter the encrypted license key information from <https://mysonicwall.com> manually on the **Device | Settings > Licenses** page in the SonicOS management interface.

① **NOTE:** Manual upgrade of the encrypted license keyset is only for closed environments. If your firewall is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.

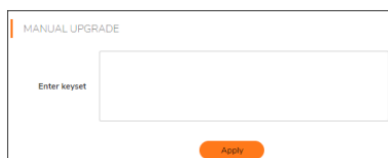
You need to perform steps 1 through 4 from a computer connected to the internet and then continue the procedure in the SonicOS Management Interface of the security appliance that does not have internet connectivity.

1. Make sure you have an account at <https://mysonicwall.com> and your SonicWall security appliance is registered to the account before proceeding.
2. After logging into MySonicWall, click on the serial number of your registered SonicWall security appliance listed in **Product Management > My Products**.

- Click **MANUAL UPGRADE** and select **Add keyset to your product**. The scrambled text displayed is the License Keyset for the selected SonicWall security appliance and activated Security Services.



- Click **Copy Code** to copy the Keyset text for pasting into the **Settings | Licenses** page.
- Make sure your SonicWall appliance is running the latest version of SonicOS.
- Navigate to **Device | Settings > Licenses**.
- Click **Manual License** at the upper-right corner of the page.
- Paste (or type) the Keyset (from the step 3) into the **Enter Keyset** field in the **Manual License Upgrade** dialog.



- Click **APPLY** to update your SonicWall security appliance. The status field at the bottom of the page displays `The configuration has been updated.`
 - You can generate the report from **Device | Diagnostics > Tech Support Report** to verify the upgrade details.
- ① | **NOTE:** After the manual upgrade, the **Settings | Licenses** page does not contain any registration and upgrade information.

Registering Your SonicWall Appliance

When you log in to your primary appliance for the first time, a Software Transaction Agreement (STA) form displays for your acceptance before you can proceed. If you are using a CLI, you must type (or select) **Yes** before proceeding. When you have accepted the STA, it is not shown for upgrades of either firmware or software.

- ① | **NOTE:** MySonicWall registration information is not sold or shared with any other company.

See the *Quick Start Guide* for your security appliance for additional information on applying licenses manually, synchronizing licenses manually, and upgrading firmware.

Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Your security appliance must be registered on MySonicWall to use these security services. See [Registering Your SonicWall Appliance](#) or the *Quick Start Guide* for your security appliance.

Because SonicWall Anti-Spyware is part of SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention, the Activation Key you receive is for all three services on your SonicWall security appliance.

If you do not have a SonicWall Gateway Anti-Virus , Anti-Spyware , and Intrusion Prevention license activated on your SonicWall security appliance, you must purchase it from a SonicWall reseller or through your [MySonicWall](#) account (limited to customers in the USA and Canada).

Activating FREE TRIALS

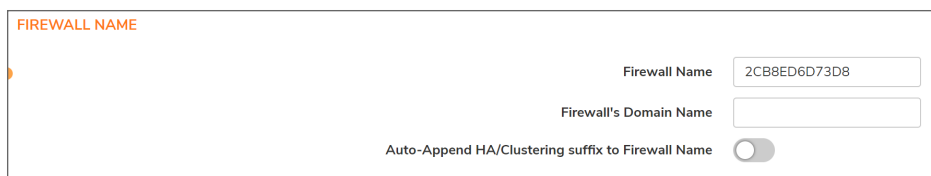
You can try FREE TRIAL versions of SonicWallGateway Anti-Virus, Anti-Spyware, and Intrusion Prevention. For information about activating a free trial of any or all of the Security Services, see the *Quick Start Guide* for your security appliance or [Managing Security Services Online](#).

System Administration

Configuring the Firewall Name

To configure the firewall name:

1. Navigate to **Device | Settings > Administration**.
2. Click **Firewall Administrator**.



The screenshot shows a configuration window titled "FIREWALL NAME". It contains three input fields and a toggle switch. The "Firewall Name" field contains the hexadecimal value "2CB8ED6D73D8". The "Firewall's Domain Name" field is empty. The "Auto-Append HA/Clustering suffix to Firewall Name" toggle switch is currently turned off.

3. Enter the hexadecimal serial number of the firewall in the **Firewall Name** field. This number uniquely identifies the SonicWall security appliance and defaults to the serial number of the firewall. The serial number is also the MAC address of the unit. To change the Firewall Name, enter a unique alphanumeric name in the Firewall Name field. It must be at least 8 characters in length and can be up to 63 characters long.
4. Enter a friendly name in the **Firewall's Domain Name** field. The name can be private, for internal users, or an externally registered domain name. This domain name is used in conjunction with User Web Login Settings.
5. To facilitate recognition of the primary/secondary firewalls in the Event Logs, enable **Auto-Append HA/Clustering suffix to Firewall Name**. When this option is enabled, an appropriate suffix is appended automatically to the firewall name in the **Monitor | Logs > System Logs** page.

This option is not selected by default. For more information about Event Logs, see the *SonicOS 7.0 Logs (Monitor)* document.

Enabling Wireless LAN and IPv6

To enable the visibility of a wireless LAN and/or IPv6:

1. Navigate to **Device | Settings > Administration > Firewall Administrator**.
2. Click **Enable Wireless LAN** and/or **Enable IPv6**. These options are selected by default. A confirmation message is displayed.
ⓘ | IMPORTANT: Enabling or disabling the Wireless LAN feature requires a restart of the firewall.



The screenshot shows a dialog box titled "FEATURE VISIBILITY". On the right side, there are two toggle switches. The first is labeled "Enable Wireless LAN" and is currently turned on. The second is labeled "Enable IPv6" and is also currently turned on.

When WLAN is disabled:

- All access point and wireless-related management interface pages do not display.
- WLAN is not displayed as a zone type.
- Any existing WLAN zones or objects become uneditable.

When IPv6 is disabled, all IPv6 packets are dropped by the firewall and the **Monitor | Tools and Monitor > Packet Monitor** page displays the log messages.

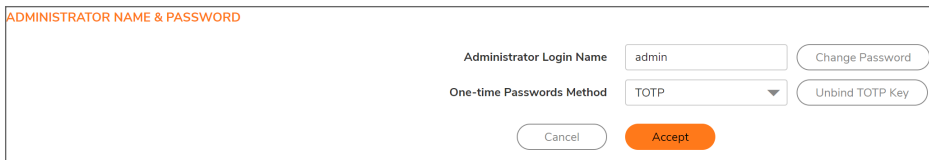
3. Click **OK**.

Changing the Administrator Name and Password

Each SonicWall security appliance has a default administrator name of admin and a password of password.

To change the administrator name and/or password:

1. Navigate to **Device | Settings > Administration**.
2. Click **Firewall Administrator**.



The screenshot shows a dialog box titled "ADMINISTRATOR NAME & PASSWORD". It contains the following fields and buttons:

- Administrator Login Name:** A text input field containing "admin". To its right is a "Change Password" button.
- One-time Passwords Method:** A dropdown menu currently set to "TOTP". To its right is an "Unbind TOTP Key" button.
- At the bottom center, there are two buttons: "Cancel" and "Accept".

3. Type the new name in the **Administrator Login Name** field.

The Administrator Name can be changed from the default setting of admin to any word using alphanumeric characters up to 32 characters in length.

4. Perform the following steps to change password, otherwise skip to step 4:
 - a. Click **Change Password**.
 - b. Type the old password in the **Old Password** field.
 - c. Type the new password in the **New Password** field. The new password can be up to 32 alphanumeric and special characters.
 - d. It is recommended you change the default password, password, to your own custom password. Enter a strong password that cannot be easily guessed by others. A strong password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, MyP@ssw0rd.
 - e. Type the new password again in the **Confirm Password** field.
 - f. Click **Accept**.
5. To enforce Two-factor Authentication, select **TOTP** from the One-time Passwords Method drop-down. You can now bind your mobile authentication application with your user account during the next login.
6. Click **Accept**.

Configuring Login Security

The internal SonicOS Web-server supports TLS 1.1 and above with strong ciphers (128 bits or greater) when negotiating HTTPS management sessions. SSL implementations are not supported. This heightened level of HTTPS security protects against potential SSLv2 rollback vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.

① TIP: SonicOS uses advanced browser technologies, such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari (does not operate on Windows platforms) browsers for administration of SonicOS. Mobile device browsers are not recommended for SonicWall system administration.

Configuring SonicOS password constraint enforcement ensures that administrators and users are using secure passwords. This password constraint enforcement can satisfy the confidentiality requirements as defined by current information security management systems or compliance requirements, such as Common Criteria and the Payment Card Industry (PCI) standard.

LOGIN SECURITY

Password must be changed every (days) 90

Change password after (hours) 1 ⓘ

Bar repeated passwords for this many changes 4

Apply password constraints ⓘ

Enforce a minimum password length of

Enforce password complexity

Complexity Requirement

Upper Case Characters

Lower Case Characters

Number Characters

Symbolic Characters

Max login attempts through CLI ⓘ

Apply these password constraints for

- Admin
- Other full admin
- Limited admin
- Guest admin
- Other local users
- System admin
- Crypto admin
- Audit admin

Log out the Admin after inactivity of (mins)

Admin/user logout

Local admin/user account lockout ⓘ

Log event only without lockout

Failed login attempts before lockout every mins

Lockout Period (mins) ⓘ

Topics:

- [Configuring Password Compliance](#)
- [Configuring Login Constraints](#)

Configuring Password Compliance

To configure password compliance:

1. Navigate to **Device | Settings > Administration**.
2. Click **Login / Multiple Administrators**.
Configure the following settings in the **LOGIN SECURITY** section.
3. To require users to change their passwords after a designated number of days has elapsed:
 - a. Select **Password must be changed every (days)**. The field becomes active. This option is not selected by default.
 - b. Enter the elapsed time in the field. The default number of days is 90, the minimum is 1 day, and the maximum is 9999.

When a user attempts to login with an expired password, a popup window prompts the user to enter a new password. The User Login Status window now includes a Change Password button so users can change their passwords at any time.

4. To specify the minimum length of time, in hours, allowed between password changes:
 - a. Select **Change password after (hours)**. The field becomes active.
 - b. Enter the number of hours. The minimum – and default – time is 1 hour; the maximum is 9999 hours.

5. To require users to use unique passwords for the specified number of password changes:
 - a. Select **Bar repeated passwords for this many changes**. The field becomes active.
 - b. Enter the number of changes. The default number is 4, the minimum number is 1, and the maximum number is 32.
6. To require users to change at least 8 alphanumeric/symbolic characters of their old password when creating a new one, select **Apply password constrains**. For how to specify what characters are allowed, see Step 7.
7. Specify the shortest allowed password, enter the minimum number of characters in the **Enforce a minimum password length of** field. The default number is **8**, the minimum is 1, and the maximum is 99.
8. Choose how complex a user's password must be to be accepted from the Enforce password complexity drop-down menu:
 - **None** (default)
 - **Alphanumeric characters**— Requires both alphabetic and numeric characters
 - **Alphanumeric and symbolic characters**— Requires alphabetic, numeric, and symbolic characters – for symbolic characters, only **!, @, #, \$, %, ^, &, *, (, and)** are allowed; all others are denied
9. When a password complexity option other than None is selected, the options under Complexity Requirement become active. Enter the minimum number of alphanumeric and symbolic characters required in a user's password. The default number for each is 0, but the total number of characters for all options cannot exceed 99.
 - **Upper Case Characters**
 - **Lower Case Characters**
 - **Number Characters**
 - **Symbolic Characters**

① **NOTE:** The Symbolic Characters field becomes active only if **Alphanumeric and symbolic characters** is selected.
10. Select to which classes of users the password constraints are applied under Apply the above password constraints for. By default, all options are selected:
 - **Admin** – Refers to the default administrator with the username admin.
 - **Other full admin**
 - **Limited admin**
 - **Guest admin**
 - **Other local users**

Configuring Login Constraints

To configure login constraints:

1. Navigate to **Device | Settings > Administration**.
2. Click **Login/Multiple Administrators**.

In the **LOGIN SECURITY** section, configure the following:

| | |
|--|--|
| Log out the Admin after inactivity of (mins) | <input type="text" value="60"/> |
| Admin/user lockout | <input type="checkbox"/> |
| Local admin/user account lockout | <input type="checkbox"/> ⓘ |
| Log event only without lockout | <input type="checkbox"/> |
| Failed login attempts before lockout | <input type="text" value="5"/> every <input type="text" value="1"/> mins |
| Lockout Period (mins) | <input type="text" value="5"/> ⓘ |

1. To specify the length of inactivity time that elapses before you are automatically logged out of the Management Interface, enter the time, in minutes, in the **Log out the Admin after inactivity of (mins)** field. By default, the SonicWall Security Appliance logs out the administrator after 5 minutes of inactivity. The inactivity timeout can range from 1 to 9999 minutes.

ⓘ **TIP:** If the Administrator Inactivity Timeout is extended beyond five minutes, you should end every management session by clicking Logout in the upper right corner of the view to prevent unauthorized access to the firewall's Management Interface.
2. To configure the SonicWall Security Appliance to lockout an administrator or a user if the login credentials are incorrect, enable **Admin/user lockout**. Both administrators and users are locked out of accessing the firewall after the specified number of incorrect login attempts. This option is disabled by default. When this option is enabled, the following fields become active.

⚠ **CAUTION:** If the administrator and a user are logging into the firewall using the same source IP address, the administrator is also locked out of the firewall. The lockout is based on the source IP address of the user or administrator.

 - a. Select Enable **local admin/user account lockout** (uncheck for login IP address lockout). This option locks out user accounts and IP addresses when they have surpassed a specified number of incorrect login attempts. This option is only available when **admin/user lockout** is enabled.
 - b. Select **Log event only without lockout** for SonicOS to log failed user login attempts that have reached the established threshold, but does not lock out the user or IP address. This option is only available when **Admin/user lockout** is enabled.

After a user or IP address is locked out, a “User login denied - User is locked out” message displays on the login screen and the login is rejected.

① **NOTE:** You can review and edit all locked out user accounts on the Active Users page when **local admin/user account lockout** is enabled.

- c. Enter the number of failed attempts within a specified time frame before the user is locked out in the **Failed login attempts per minute before lockout** field. The default number is 5, the minimum is 1, and the maximum is 99. Enter the maximum time in which failed attempts can be made. The default is 5 minutes, the minimum is 1 minute, and the maximum is 240 minutes (4 hours).
 - d. Enter the length of time that must elapse before the user is allowed to attempt to log into the firewall again in the **Lockout Period (mins)** field. The default is 5 minutes, the minimum is 0 (permanent lockout), and the maximum is 60 minutes.
3. Enter the number of incorrect login attempts from the command line interface (CLI) that triggers a lockout in the **Max login attempts through CLI** field. The default is 5, the minimum is 3, and the maximum is 15.
 4. Click **Accept**.

Multiple Administrators Support

SonicOS supports multiple concurrent administrators with full administrator privileges, read-only privileges, and limited privileges. The original version of SonicOS supported only a single administrator to log on to a firewall with full administrative privileges. Additional users can be granted “limited administrator” access, but only one administrator can have full access to modify all areas of the SonicOS GUI at one time.

SonicOS provides 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 user names 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 they cannot make configuration changes.

Multiple Administrators Support provides the following benefits:

- **Improved productivity:** Allowing multiple administrators to access a firewall 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 firewall without the risk of making unintentional changes to the configuration.

Working of Multiple Administrators Support

Topics:

- [Configuration Modes](#)
- [User Groups](#)
- [Priority for Preempting Administrators](#)
- [GMS and Multiple Administrator Support](#)

Configuration Modes

To allow multiple concurrent administrators, while also preventing potential conflicts caused by multiple administrators making configuration changes at the same time, these configuration modes have been defined:

| | |
|-------------------------------|--|
| Configuration mode | <p>Administrator has full privileges to edit the configuration. If no administrator is already logged into the appliance, this is the default behavior for administrators with full and limited administrator privileges (but not read-only administrators).</p> <p>NOTE: Administrators with full configuration privilege can also log in using the Command Line Interface (CLI; see the <i>SonicOS 7.0 CLI Reference Guide</i>).</p> |
| Read-only mode | <p>Administrator cannot make any changes to the configuration, but can view the entire management UI and perform monitoring actions.</p> <p>Only administrators who are members of the SonicWall Read-Only Admins user group are given read-only access, and it is the only configuration mode they can access.</p> |
| Non-configuration mode | <p>Administrator can view the same information as members of the read-only group and they can also initiate management actions that do not have the potential to cause configuration conflicts.</p> <p>Only administrators who are members of the SonicWall Administrators user group can access non-configuration mode. This mode can be entered when another administrator is already in configuration mode and the new administrator chooses not to preempt the existing administrator. By default, when an administrator is preempted out of configuration mode, he or she is converted to non-configuration mode. On the Device Settings > Administration page, this behavior can be modified so that the original administrator is logged out.</p> |

Access rights available to configuration modes table provides a summary of the access rights available to the configuration modes. Access rights for limited administrators are included also, but note that this table does not include all functions available to limited administrators.

ACCESS RIGHTS AVAILABLE TO CONFIGURATION MODES

| Function | Full admin in config mode | Full admin in non-config mode | Read-only administrator | Limited administrator |
|---------------------------------------|---------------------------|-------------------------------|-------------------------|-----------------------|
| Import certificates | X | | | |
| Generate certificate signing requests | X | | | |
| Export certificates | X | | | |
| Export appliance settings | X | X | X | |
| Download TSR | X | X | X | |
| Use other diagnostics | X | X | | X |
| Configure network | X | | | X |
| Flush ARP cache | X | X | | X |
| Setup DHCP Server | X | | | |
| Renegotiate VPN tunnels | X | X | | |
| Log users off | X | X | | guest users only |
| Unlock locked-out users | X | X | | |
| Clear log | X | X | | X |
| Filter logs | X | X | X | X |
| Export log | X | X | X | X |
| Email log | X | X | | X |
| Configure log categories | X | X | | X |
| Configure log settings | X | | | X |
| Generate log reports | X | X | | X |
| Browse the full UI | X | X | X | |
| Generate log reports | X | X | | X |

User Groups

The Multiple Administrators Support feature supports 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 read-only access to view the full 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 these user groups. If you do so, however, the following behavior applies:

| If members of this user group Are | |
|-----------------------------------|--|
| SonicWall Administrators | Also included in the Limited Administrators or SonicWall Read-Only Admins user groups, the members have full administrator rights. |
| Limited Administrators | Included in the SonicWall Read-Only Admins user group, the members have limited administrator rights. |
| Read-Only Admins | Later included in another administrative group, If this read-only admin group is used with other administrative groups option in the SonicWall Read-Only Admins group configuration determines whether the members are still restricted to read-only access or have the full administration capabilities set by their other group. |

Priority for Preempting Administrators

These rules govern the priority levels that the various classes of administrators have for preempting administrators that are already logged into the appliance:

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

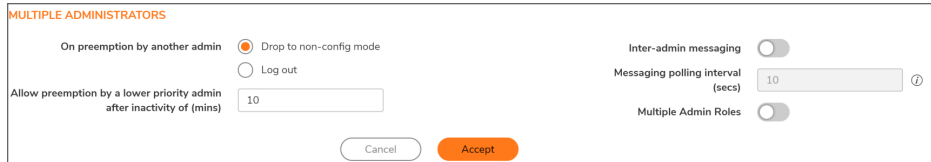
GMS and Multiple Administrator Support

When using SonicWall GMS to manage a firewall, 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.

Configuring Multiple Administrator Access

To configure multiple administrator access:

1. Navigate to **Device | Settings > Administration**.
Click **Login / Multiple Administrators**.



The screenshot shows a configuration dialog box titled "MULTIPLE ADMINISTRATORS". It contains the following options:

- On preemption by another admin:** Two radio buttons. "Drop to non-config mode" is selected (indicated by a red dot), and "Log out" is unselected.
- Allow preemption by a lower priority admin after inactivity of (mins):** A text input field containing the value "10".
- Inter-admin messaging:** A toggle switch that is currently turned off.
- Messaging polling interval (secs):** A text input field containing the value "10", with a help icon to its right.
- Multiple Admin Roles:** A toggle switch that is currently turned off.

At the bottom of the dialog are two buttons: "Cancel" and "Accept".

2. To configure what happens when one administrator preempts another administrator, from the **On preemption by another admin** option, select whether the preempted administrator can be converted to non-config mode or logged out:
 - **Drop to non-config mode:** More than one administrator to access the appliance in non-config mode without disrupting other administrators. This option is not selected by default.
 - **Log out:** The new administrator to preempt other sessions.
- ① **NOTE:** Selecting **Log Out** disables **Non-Config mode** and prevents entering **Non-Config mode** manually.
3. To allow a lower-priority administrator to preempt the current administrator after a specified time, enter the time, in minutes, in the **Allow preemption by a lower priority administrator after inactivity of (mins)** field. The default is 10 minutes, the minimum is 1 minute, and the maximum is 9999 minutes.
4. The SonicOS Management Interface allows administrators to send text messages through the Management Interface to other administrators logged into the appliance. The message appears in the browser's status bar. To enable this option:
 - a. Select **Inter-administrator messaging**. The **Messaging polling interval (seconds)** field becomes active.
 - b. Specify how often an administrator's browser checks for inter-administrator messages in the **Messaging polling interval (secs)** field. Specify a reasonably short interval to ensure timely delivery of messages, especially if there are likely to be multiple administrators who need to access the appliance. The default is **10 seconds**, the minimum is **1 second**, and the maximum is **99 seconds**.
5. To enable access by System Administrators, Cryptographic (Crypto) Administrators, and Audit Administrators, select **Multiple Admin Roles**. When this option is disabled, these administrators cannot access the system, and all related user groups and information about them are hidden. This option is not selected by default.

Enabling Enhanced Audit Logging Support

An enhanced log entry contains the parameter changed and user name in the **Monitor | Logs > System Events** page.

To enable logging of all configuration changes in the Monitor | Logs > System Logs page:

1. Navigate to **Device | Settings > Administration**.
2. Click **Audit / SonicOS API**.
3. In the **ENHANCED AUDIT LOGGING SUPPORT** section, enable **Enhanced Audit Logging**



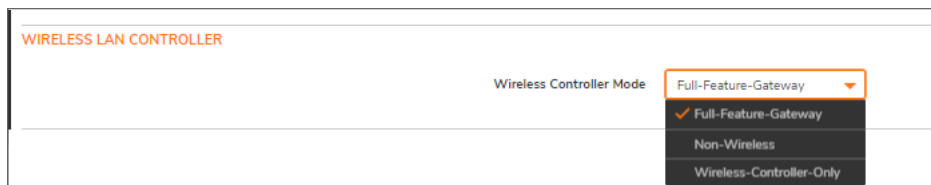
4. Click **ACCEPT**.

Configuring the Wireless LAN Controller

To enable wireless controller mode:

① | **IMPORTANT:** You must reboot the firewall after changing Wireless Controller modes.

1. Navigate to **Device | Settings > Administration**.
2. Click **Audit/SonicOS API**.
3. In the **Wireless LAN Controller** section, select any one of the options from the **Wireless Controller Mode** drop-down menu:
 - **Wireless-Controller-Only** (default)
This option enables wireless controller mode
 - **Non-Wireless**
This option enables non-wireless controller mode
 - **Full-Feature-Gateway**
This option enables normal firewall mode



4. After you select the appropriate wireless controller mode, click **OK** in the warning message displayed.
5. Click **Accept**.

Enabling SonicOS API and Configuring Authentication Methods

You can use SonicOS API as an alternative to the SonicOS Command Line Interface (CLI) for configuring selected functions. To do so, you must first enable SonicOS API. For more information about SonicOS API, see the *SonicOS 7.0 API document* available at <https://www.sonicwall.com/support/technical-documentation/>.

To enable SonicOS API and configure client authentication:

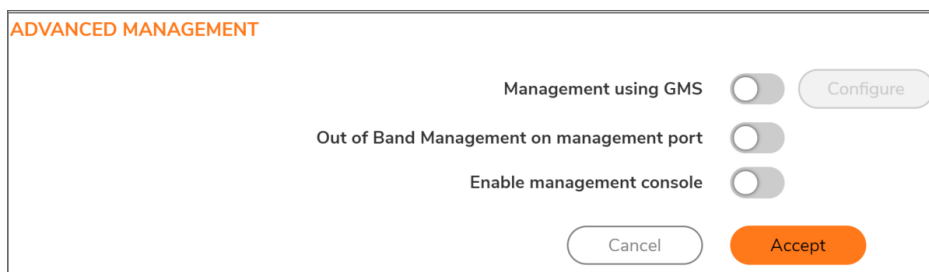
1. Navigate to **Device | Settings > Administration**.
2. Click **Audit / SonicOS API**.
3. In the **SONICOS API** section, enable **SonicOS API**.
4. Select any of the authentication methods for initial client authentication:
 - **RFC-7616 HTTP Digest Access authentication**
 - Select the appropriate digest algorithms: **SHA256** (default), MD5
 - Integrity protection: **Disabled** (default), Allowed, or Enforced.
 - Session variant (password hashes in place of passwords): **Disabled, Allowed** (default), or **Enforced**
 - **CHAP authentication**.
 - **RFC-2617 HTTP Basic Access authentication**
 - **Public Key Authentication**
 - **RSA modulus (key/cipher size in bits): 2014** is the default.
 - **RSA padding type:** PKCS#1 v1.5 or PKCS#1 v2.0 OAEP
 - OAEP hash method: SHA-1, SHA-256, or Other
 - OAEP mask (MGF1) method: SHA1, SHA-256, or Other
 - **Session security using RFC-7616 Digest Access Authentication**
 - Can hold user passwords received from the client.
 - Maximum nonce use: 10 by default
 - **Two-Factor and Bearer Token Authentication**
5. Click **Accept**.

Enabling GMS Management

① **NOTE:** For more information on SonicWall Global Management System, see the *SonicWall GMS* and *SonicWall Management Services* administration documentation, available at <https://www.sonicwall.com/support/technical-documentation/>.

To configure the Security Appliance for GMS management:

1. Navigate to **Device | Settings > Administration**.
2. Click **Audit / SonicOS API**.
3. Scroll to the **ADVANCED MANAGEMENT** section.



ADVANCED MANAGEMENT

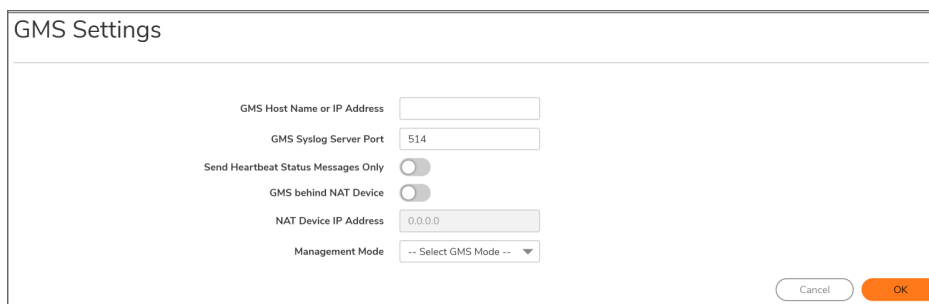
Management using GMS Configure

Out of Band Management on management port

Enable management console

Cancel Accept

4. Enable **Management using GMS**. The **Configure** button becomes available.
5. Click **Configure**. The **GMS Settings** screen is displayed.



GMS Settings

GMS Host Name or IP Address

GMS Syslog Server Port

Send Heartbeat Status Messages Only

GMS behind NAT Device

NAT Device IP Address

Management Mode

Cancel OK

6. Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
7. Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.
8. To send only heartbeat status instead of log messages, select **Send Heartbeat Status Messages Only**.
9. If the GMS Console is placed behind a device using NAT on the network, select **GMS behind NAT Device**. When you select **GMS behind NAT Device**, the **NAT Device IP Address** field becomes active.
10. Enter the IP address of the NAT device in the **NAT Device IP Address** field.

11. Select one of the following GMS modes from the **Management Mode** drop-down menu:
 - **IPSEC Management Tunnel** - Allows the firewall to be managed over an IPsec VPN tunnel to the GMS management console. If you selected this option, go to step 11.
 - **Existing Tunnel** - Uses an existing VPN tunnel over the connection between the GMS server and the firewall. If you selected this option, go to step 13.
 - **HTTPS** - Allows HTTPS management from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The SonicWall firewall also sends encrypted syslog packets and SNMP traps using 3DES and the firewall administrator's password. Options for configuring the GMS reporting server display. If you selected this option, go to step 12.
12. The default IPsec VPN settings are displayed with values populated by SonicOS. Verify the settings.

- a. From **Encryption Algorithms**, select the appropriate algorithm.
- b. Optionally, enter a new encryption key in the Encryption Key field:

| For | The key must be |
|-------------|---------------------------|
| DES | 16 hexadecimal characters |
| 3DES | 48 hexadecimal characters |

- c. Optionally, enter a new authentication key in the Authentication Key field:

| For | The key must be |
|-------------|---------------------------|
| MD5 | 32 hexadecimal characters |
| SHA1 | 40 hexadecimal characters |

- d. Go to Step 13.

13. SonicOS needs to know the GMS reporting server.

- a. Select **Send Syslog Messages to a Distributed GMS Reporting Server**. The **GMS Reporting Server IP Address** and **GMS Reporting Server Port** options become available.

- b. In the **GMS Reporting Server IP Address** field, enter the IP address of the GMS server.
 - c. In the **GMS Reporting Server Port** field, enter the port of the GMS server. The default port is **514**.
14. Click **OK**.
15. Click **Accept**.

Configuring the Management Interface

In this section, you configure:

- How the Management Interface tables display.
- Certificate usage.
- Whether you are operating in Configuration or Non-Config mode.
- Other management options.

WEB MANAGEMENT SETTINGS

| | |
|---|--|
| Allow management via HTTP | <input type="checkbox"/> |
| HTTP Port | <input type="text" value="80"/> |
| HTTPS Port | <input type="text" value="443"/> |
| Certificate Selection | <input type="text" value="Use Selfsigned Certifi..."/> ⓘ |
| Certificate Common Name | <input type="text" value="192.168.168.168"/> |
| Default Table Size (items per page) | <input type="text" value="50"/> ⓘ |
| Auto-updated Table Refresh Interval (secs) | <input type="text" value="10"/> ⓘ |
| Use Threat Protection View as starting page | <input type="checkbox"/> |
| Enable Tooltip | <input checked="" type="checkbox"/> |
| Form Tooltip Delay (msecs) | <input type="text" value="2000"/> |
| Button Tooltip Delay (msecs) | <input type="text" value="3000"/> |
| Text Tooltip Delay (msecs) | <input type="text" value="500"/> |
| Enforce TLS 1.1 and Above | <input type="checkbox"/> |

Topics:

- [Managing through HTTP/HTTPS](#)
- [Selecting a Security Certificate](#)
- [Controlling the Management Interface Tables](#)
- [Enforcing TLS Version](#)
- [Switching Configuration Modes](#)
- [Deleting Browser Cookies](#)
- [Configuring SSH Management](#)

Managing through HTTP/HTTPS

You can manage the SonicWall security appliance using HTTP or HTTPS and a Web browser. HTTP web-based management is disabled by default. Use HTTPS to log into the SonicOS Management Interface with factory default settings.

To manage through HTTP or HTTPS:

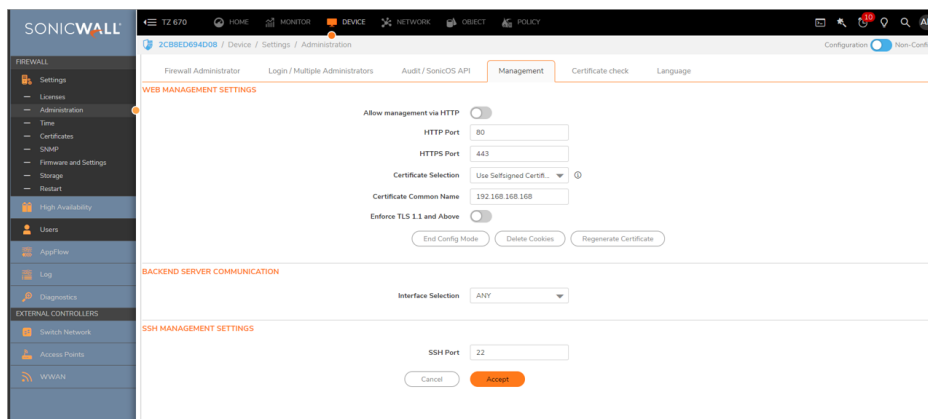
1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. To enable HTTP management globally, select **Allow management via HTTP** in the **WEB MANAGEMENT SETTINGS** section. This option is not selected by default.
4. The default port for HTTP is port **80**, but you can configure access through another port. Enter the number of the desired port in the **HTTP Port** field.
 - ① **IMPORTANT:** If you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWall Security Appliance. For example, if you configure the port to be 76, then you must type LAN IP Address:76 into the Web browser, for example, `http://192.18.16.1:76`.
5. The default port for HTTPS management is **443**. To add another layer of security for logging into the SonicWall Security Appliance by changing the default port, enter the preferred port number into the **HTTPS Port** field.
 - ① **IMPORTANT:** If you configure another port for HTTPS management Port, you must include the port number when you use the IP address to log into the SonicWall Security Appliance. For example, if you use 700 for the port, then you must log into the SonicWall using the port number as well as the IP address; for example, `https://192.18.16.1:700`.

Selecting a Security Certificate

Security certificates provide data encryption and a secure web site.

To specify the type of security certificate:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. From **Certificate Selection** drop-down box, select the type of certificate for your website:



- **Use Self-signed Certificate**, which allows you to continue using a certificate without downloading a new one each time you log into the SonicWall Security Appliance. This option is selected by default. Go to Step 3.
 - **Import Certificate** to select an imported certificate from the **Device | Settings > Certificates** page to use for authentication to the management interface. A confirmation message displays.
 - a. Click **OK**. The **Device | Settings > Certificates** page is displayed.
 - b. See [Managing Certificates](#) section.
4. In the **Certificate Common Name** field, enter the IP address or common name for the firewall. If you choose Use Selfsigned Certificate, SonicOS populates the field with the firewall's IP address.
 5. Click **Accept**.

To regenerate a Self-Signed Certificate:

1. Navigate to **Device | System > Administration > Management**.
2. In the **WEB MANAGEMENT SETTINGS** section, click **Regenerate Certificate**.
3. Click **OK** in the confirmation message that is displayed.

Controlling the Management Interface Tables



The SonicWall Management Interface allows you to control the display of large tables of information across all tables in the Management Interface by changing the:

- Number of table entries displayed on a page.
- Frequency of background automatic refresh of tables.

Some tables have individual settings for items per page that are initialized at login to the value configured here. After these pages are viewed, their individual settings are maintained. Subsequent changes made here affect these pages only following a new login.

To change the display and refresh of tables:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. In the **WEB MANAGEMENT SETTINGS** section:
 - a. Enter the desired number of items per page in the **Default Table Size (items per page)** field. The minimum is 1, the maximum is 5000, and the default is **50**.
 - b. Enter the desired refresh interval, in seconds, in the **Auto-updated Table Refresh Interval (secs)** field. The minimum is 1 second, the maximum is 300 seconds, and the default is 10 seconds.

| | | |
|---|---------------------------------|---|
| Default Table Size (items per page) | <input type="text" value="50"/> |  |
| Auto-updated Table Refresh Interval (secs) | <input type="text" value="10"/> |  |

4. Click **Accept**.

Enforcing TLS Version

SonicOS supports versions 1.0, 1.1, and 1.2 of the Transport Layer Security (TLS) protocol. You can ensure that the more secure version 1.1 and above are used.

To enforce use of TLS versions 1.1 and above:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. In the **WEB MANagements SETTINGS** section, enable **Enforce TLS 1.1 and Above**.

Enforce TLS 1.1 and Above

4. Click **Accept**.

Switching Configuration Modes

Each appliance includes a Mode option that toggles the configuration mode of the Management Interface. If you are in Configuration Mode, you can switch to Non-Config Mode at any time, or if you are in Non-Config Mode, you

can switch to Configuration Mode.

① **TIP:** This method is in addition to switching modes from the Mode setting on each view. For more information about modes, see the *SonicOS 7.1 About SonicOS* documentation.

To switch modes:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. In the **WEB MANAGEMENT SETTINGS** section, If you are in:
 - Configuration Mode, click **End Config Mode**, and click **OK**.
The Mode indicator in the top right of the page displays **Non-Config**.
 - Non-Config Mode, click **Configuration Mode**.
The Mode indicator in the top right of the page displays **Configuration**.

Deleting Browser Cookies

① **IMPORTANT:** Deleting cookies causes you to lose any unsaved changes made in the Management Interface.

To delete all browser cookies saved by the Security Appliance:

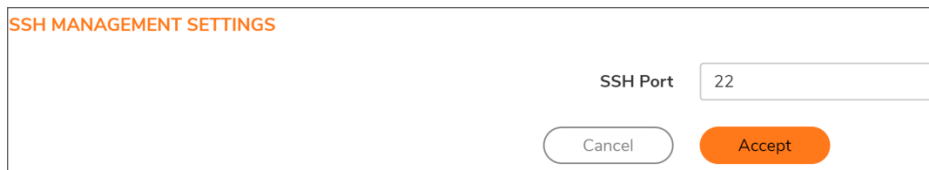
1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. Click **Delete Cookies**.
4. Click **OK**.

Configuring SSH Management

If you use SSH to manage the firewall, you can change the SSH port for additional security.

To change the SSH port:

1. Navigate to **Device | Settings > Administration**.
2. Click **Management**.
3. Scroll to **SSH MANAGEMENT SETTINGS**.



SSH MANAGEMENT SETTINGS

SSH Port

4. Enter the port in the **SSH Port** field. The default SSH port is **22**.
5. Click **Accept**.

Client Certificate Verification

You can configure certificate verification with or without a Common Access Card (CAC).

NOTE: None of the options is selected by default.

CLIENT CERTIFICATE CHECK

Enable Client Certificate Check

Enable Client Certificate Cache

User Name Field

Client Certificate Issuer

CAC user group memberships retrieve method

Enable OCSP Checking

OCSP Responder URL

Enable periodic OCSP Check

OCSP check interval: 1-72 (hours)

Topics:

- [About Common Access Card](#)
- [Configuring Client Certificate Verification](#)
- [Using the Client Certificate Check](#)
- [Troubleshooting User Lock Out](#)

About Common Access Card

A Common Access Card (CAC) is a United States Department of Defense (DoD) smart card used by military personnel and other government and non-government personnel who require highly secure access over the Internet. A CAC uses PKI authentication and encryption.

NOTE: Using a CAC requires an external card reader connected on a USB port.

The Client Certificate Check was developed for use with a CAC; however, it is useful in any scenario that requires a client certificate on an HTTPS/SSL connection. CAC support is available for client certification only on HTTPS connections.

NOTE: CACs might not work with browsers other than Microsoft Internet Explorer.

Configuring Client Certificate Verification

To configure Client Certificate Check:

1. Navigate to **Device | Settings > Administration**.
2. Click **Certificate Check**.

CLIENT CERTIFICATE CHECK

Enable Client Certificate Check

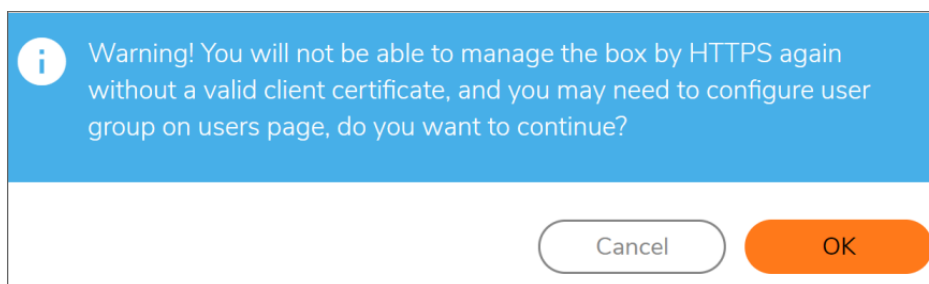
Enable Client Certificate Cache

User Name Field

Client Certificate Issuer

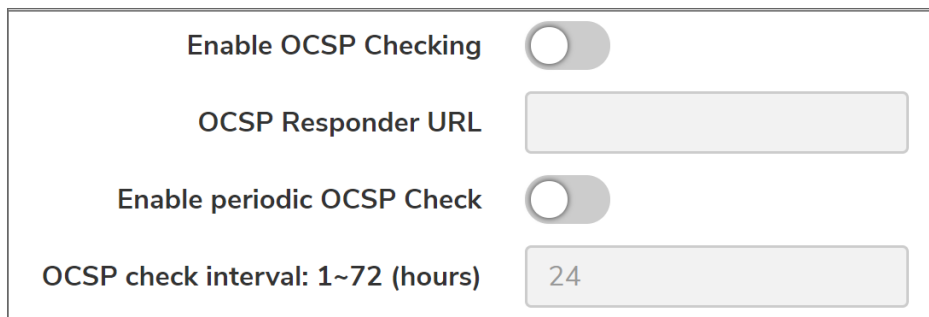
CAC user group memberships retrieve method

3. To enable client certificate checking and CAC support on the SonicWall Security Appliance, select **Enable Client Certificate Check**. If you enable this option, the other options become available. A warning confirmation message displays:



4. Click **OK**.
5. To activate the client certification cache, select **Enable Client Certificate Cache**.
i | **NOTE:** The cache expires 24 hours after being enabled.
6. To specify from which certificate field the user name is obtained, choose an option from User Name Field:
 - **Subject: Common Name** (default)
 - **Sub Alt: Email**
 - **Sub Alt: Microsoft Universal Principal Name**
7. To select a Certification Authority (CA) certificate issuer, choose one from the **Client Certificate Issuer** drop-down menu. The default is **thawte Primary Root CA - G3**.
i | **NOTE:** If the appropriate CA is not listed, you need to import that CA into the SonicWall Security Appliance. See [Managing Certificates](#) section.
8. To select how to obtain the CAC user group membership and, thus, determine the correct user privilege, choose from the CAC user group memberships retrieve method drop-down menu:

- **Local Configured** (default) – If selected, you should create local user groups with proper memberships.
 - **From LDAP** – If selected, you need to configure the LDAP server. (see *Configuring the SonicWall for LDAP* section in *SonicOS 7.0 Users* document available at <https://www.sonicwall.com/support/technical-documentation/>.)
9. To enable the Online Certificate Status Protocol (OCSP) check to verify the client certificate is still valid and has not been revoked, select **Enable OCSP Checking**. When this option is enabled, the OCSP Responder URL field displays and the Enable periodic OCSP Check option displays.



The screenshot shows a configuration panel with the following elements:

- Enable OCSP Checking**: A toggle switch that is currently turned off.
- OCSP Responder URL**: An empty text input field.
- Enable periodic OCSP Check**: A toggle switch that is currently turned off.
- OCSP check interval: 1~72 (hours)**: A text input field containing the number "24".

Enter the URL of the OSCP server that verifies the status of the client certificate in the **OCSP Responder URL** field.

The **OCSP Responder URL** is usually embedded inside the client certificate and does not need to be entered. If the client certificate does not have an OCSP link, you can enter the URL link. The link should point to the Common Gateway Interface (CGI) on the server side, which processes the OCSP checking. For example: `http://10.103.63.251/ocsp`.

10. To enable a periodic OCSP check for the client certificate for verifying that the certificate is still valid and has not been revoked:
- Select **Enable periodic OCSP Check**. The **OCSP check interval** field becomes available.
 - Enter the interval between OCSP checks, in hours, in the OCSP check interval 1~72 (in hours) field. The minimum interval is 1 hour, the maximum is 72 hours, and the default is **24** hours.
11. Click **Accept**.

Using the Client Certificate Check

If you use the client certificate check without a CAC, you must manually import the client certificate into the browser.

If you use the Client Certificate Check with a CAC, the client certificate is automatically installed on the browser by middleware. When you begin a management session through HTTPS, a certificate selection window asks you to confirm the certificate.

After you select the client certificate from the drop-down menu, the HTTPS/SSL connection is resumed, and the SonicWall Security Appliance checks the Client Certificate Issuer to verify that the client certificate is signed by the CA. If a match is found, the administrator login page displays. If no match is found, the browser displays a standard browser connection fail message, such as:

.....cannot display web page!

If OCSP is enabled, before the administrator login page is displayed, the browser performs an OCSP check and displays the following message while it is checking.

Client Certificate OCSP Checking.....

If a match is found, the administrator login page is displayed, and you can use your administrator credentials to continue managing the SonicWall Security Appliance.

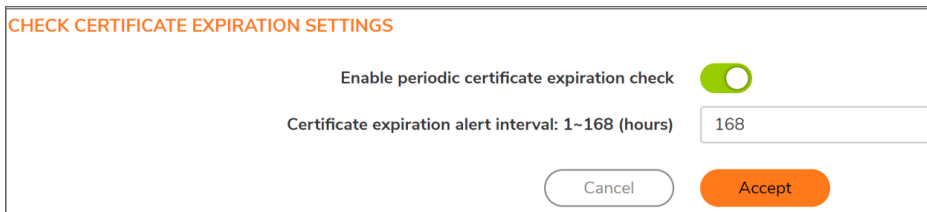
If no match is found, the browser displays:

OCSP Checking fail! Please contact system administrator!

Checking Certificate Expiration

To activate periodic checks of certificate's expiration:

1. Navigate to **Device | Settings > Administration > Certificate Check**.
2. In the **CHECK CERTIFICATE EXPIRATION SETTINGS** section, select **Enable periodic certificate expiration check**. This option is selected by default. When enabled, the Certificate expiration alert interval field becomes available.



3. To set the interval between certificate checks, in hours, enter the interval in the **Certificate expiration alert interval: 1 - 168 (in hours)** field. The minimum time is 1 hour, the maximum is 168 hours, and the default is **168**.
4. Click **Accept**.

Troubleshooting User Lock Out

When using the client certificate feature, these situations can lock the user out of the SonicWall Security Appliance:

- **Enable Client Certificate Check** is checked, but no client certificate is installed on the browser.
- **Enable Client Certificate Check** is checked and a client certificate is installed on the browser, but either no **Client Certificate Issuer** is selected or the wrong **Client Certificate Issuer** is selected.
- **Enable OSCP Checking** is enabled, but either the OSCP server is not available or a network problem is preventing the SonicWall Security Appliance from accessing the OSCP server.

To restore access to a user who is locked out, the following CLI commands are provided:

- `web-management client-cert disable`
- `web-management ocsp disable`

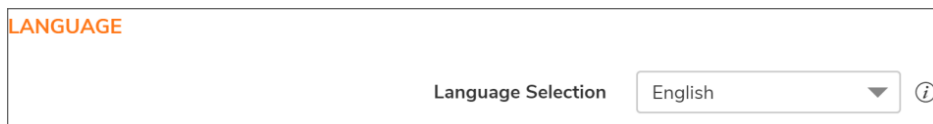
Selecting a Language

If your firmware contains other languages besides English, one can be selected from Language Selection.

① **NOTE:** Changing the language of the SonicOS Management Interface requires that the SonicWall Security Appliance be rebooted.

To select a language for the Management Interface:

1. Navigate to **Device | Settings > Administration**.
2. Click **Language**.



3. In the **LANGUAGE** section, select the appropriate language from the **Language Selection** drop-down box.
4. Click **Accept**.

Configuring Time Settings

The **Device | Settings > Time** page provides a way to define the time and date settings used to time stamp log events, to automatically update SonicWall Security Services, and for other internal purposes.

The screenshot shows the 'Settings' page for 'NTP Servers'. It is divided into two sections: 'SET TIME' and 'NTP SETTINGS'. In the 'SET TIME' section, there are several toggle switches and input fields: 'Set time automatically using NTP' (checked), 'Date / Time' (26/02/2020 03:37:37), 'Time Zone' (Pacific Time (US & Ca...)), 'Automatically adjust clock for daylight saving time' (checked), 'Display UTC in logs (instead of local time)' (unchecked), 'Display date in International format' (unchecked), and 'Only use custom NTP servers' (checked). The 'NTP SETTINGS' section has an 'Update Interval every' field set to 60 minutes. At the bottom, there are 'Cancel' and 'Accept' buttons.

By default, the SonicWall security appliance uses an internal list of public NTP servers to update the time automatically. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

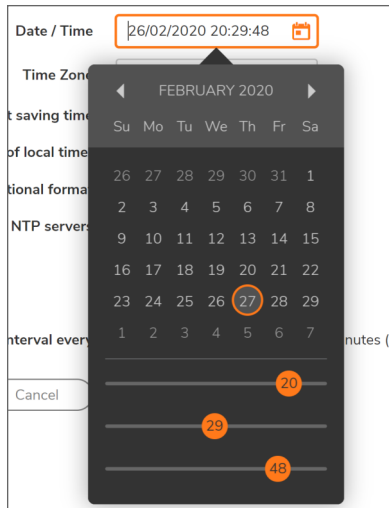
Setting System Time

You set the system time in the **Settings** screen of the **Device | Settings > Time** page.

The screenshot shows the 'Settings' screen for 'NTP Servers'. The page is divided into two sections: 'SET TIME' and 'NTP SETTINGS'. In the 'SET TIME' section, there are several toggle switches and input fields. The 'Set time automatically using NTP' toggle is turned on. The 'Date / Time' field shows '26/02/2020 03:37:37' with a calendar icon. The 'Time Zone' dropdown is set to 'Pacific Time (US & Ca...)'. Other toggles include 'Automatically adjust clock for daylight saving time' (on), 'Display UTC in logs (instead of local time)' (off), 'Display date in International format' (off), and 'Only use custom NTP servers' (on). The 'NTP SETTINGS' section has an 'Update Interval every' field set to '60' minutes, with a range of '5 - 99999'. At the bottom, there are 'Cancel' and 'Accept' buttons.

To set the system time:

1. Navigate to **Device | Settings > Time**.
2. On the **Settings** screen, select the time zone you are in from the **Time Zone** drop-down list.
3. To set the time automatically, select **Set time automatically using NTP** to use NTP (Network Time Protocol) servers from an internal list. This option is selected by default.
4. To set the time manually:
 - a. Clear **Set time automatically using NTP**. The **Date/Time** option becomes available.
 - b. Click the calendar icon in the **Date/Time** field to display the calendar.
 - c. Select the date, hour, minute, and seconds in the calendar.
 - d. Click away from the calendar to accept the settings.



5. To enable automatic adjustments for daylight savings time, select **Automatically adjust clock for daylight saving time**. For those areas that observe daylight savings time, this option is selected by default.
6. To use universal time (UTC) rather than local time for log events, select **Display UTC in logs (instead of local time)**. This option is not selected by default.
7. To display the date in International format, with the day preceding the month, select **Display date in International format**.
8. To use the manually entered list of NTP servers to set the firewall clock rather than the internal list of NTP servers, select **Only use custom NTP servers**.
 - ① **IMPORTANT:** Select this option only if you have configured one or more NTP servers. For more information about NTP servers, see [Configuring NTP Settings](#).
9. Click **Accept**.

Configuring NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.

- ① **TIP:** The SonicWall security appliance uses an internal list of NTP servers, so manually entering a NTP server is optional.

NTP SETTINGS

Update Interval every minutes (Range: 5 - 99999)

Using a Custom NTP Server for Updating the Firewall Clock

To use a local server to set the firewall clock:

1. Navigate to **Device | Settings > Time**.
2. Add one or more NTP servers as described in [Adding an NTP Server](#).
3. Select **Only use custom NTP servers** (see [Setting System Time](#)). This option is not selected by default.
4. To configure the frequency for the NTP server to update the firewall, enter the interval in **Update Interval every (minutes)**. The default value is **60** minutes. The range is 5 to 99,999 minutes.
5. Click **Accept**.

Adding an NTP Server

To add an NTP server to the firewall configuration:

1. Click **NTP Servers** tab on **Device | Settings > Time** page.
2. Click the **+Add** button.

The **Add NTP Server** dialog is displayed.

3. Type the IP address of the remote NTP server in the **NTP Server** field.

Add NTP Server

NTP Server

NTP Auth Type

Trust Key No ⓘ

Key Number ⓘ

Password

4. Select the authentication type from the **NTP Auth Type** drop-down list:
 - a. **No Auth** - Authentication is not required and the following three options are dimmed. Go to Step 8.
 - b. **MD5** - Authentication is required and the following three options are active.
5. Enter the Trust Key number in the **Trust Key No** field. The minimum is 1 and the maximum is 65535.
6. Enter the Key number in the **Key Number** field. The minimum is 1 and the maximum is 65535.
7. Enter the password in the **Password** field.
8. Click **Add**. A Success message is displayed.
9. Click **Close** to return to the **NTP Servers** screen. The **NTP Server** table shows the added server.

| Settings | | NTP Servers | |
|-------------------------------|--------------|---|--|
| <input type="text" value=""/> | | + Add 🗑 Delete 🔄 Refresh | |
| <input type="checkbox"/> | NTP SERVER | | |
| <input type="checkbox"/> | 10.203.28.57 | | |
| <input type="checkbox"/> | test | | |
| Total: 2 item(s) | | | |

Editing an NTP Server Entry

To edit an NTP server entry:

1. Navigate to the **NTP Servers** screen on **Device | Settings > Time** page.
2. In the **NTP Server** table, hover over the row with the NTP server and click the **Edit** icon. The **Add NTP Server** dialog opens, displaying the current settings for the server.
3. Make the changes. For more information, see [Adding an NTP Server](#).
4. Click **Edit**.

Deleting NTP Server Entry

To delete an NTP server entry:

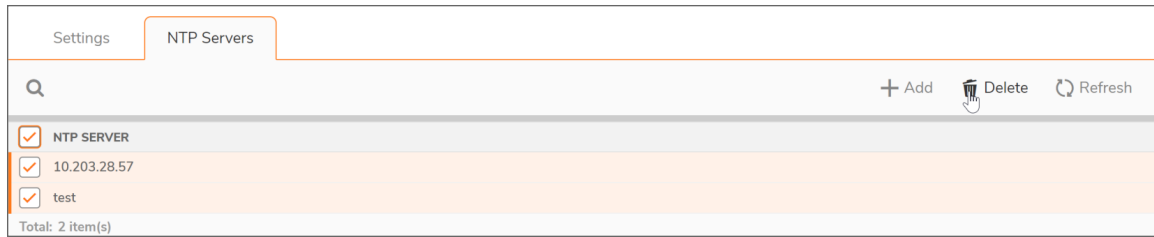
1. Navigate to the **NTP Servers** screen on **Device | Settings > Time**.
2. In the **NTP Server** table, hover over the row with the NTP server and click the **Delete** icon.
3. Click **OK**.

To delete multiple NTP servers:

1. Navigate to the **NTP Servers** screen on **Device | Settings > Time**.
2. Select the checkboxes next to the NTP servers that you want to delete.

① | **NOTE:** To delete all the NTP servers, select the checkbox next to **NTP Server** table title.

3. Click the **Delete** button at the top right of the table.



4. Click **OK**.

Managing Certificates

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third-party CA service. When you have a valid CA certificate, you can import it into the firewall to validate your Local Certificates. You import the valid CA certificate into the firewall using the **Device | Settings > Certificates** page. After you import the valid CA certificate, you can use it to validate your local certificates.

SonicOS provides a large number of certificates with the SonicWall network security appliance; these are built-in certificates and cannot be deleted or configured.

SonicOS supports a local Certificate Revocation List (CRL), which is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted. For further information about local CRL, contact [Technical Support](#).

About Digital Certificates

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). The X.509 v3 certificate standard is a specification used with cryptographic certificates and allows you to define extensions that you can include with your certificate. SonicWall has implemented this standard in its third-party certificate support.

You can use a certificate signed and verified by a third-party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up Security Associations (SAs). Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, and optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

SonicWall Security Appliances interoperate with any X.509v3-compliant provider of Certificates. SonicWall Security Appliance have been tested with the following vendors of Certificate Authority Certificates:

- Entrust
- Microsoft

- OpenCA
- OpenSSL and TLS
- VeriSign

Topics:

- [About the Certificates Table](#)
- [Importing Certificates](#)
- [Deleting Certificates](#)
- [Generating a Certificate Signing Request](#)
- [Configuring Simple Certificate Enrollment Protocol](#)

About the Certificates Table

| Q Search... | | | | New Signing Request | SCEP | Import | Delete | Refresh |
|--------------------------|---|-------------------|-------------|--------------------------|------|--------|--------|---------|
| <input type="checkbox"/> | CERTIFICATE | TYPE | VALIDATED | EXPIRES ON | | | | |
| <input type="checkbox"/> | ▶ Actalis Authentication Root CA | CA certificate | | Sep 22 11:22:02 2030 GMT | | | | |
| <input type="checkbox"/> | ▶ AffirmTrust Commercial | CA certificate | | Dec 31 14:06:06 2030 GMT | | | | |
| <input type="checkbox"/> | ▶ AffirmTrust Premium | CA certificate | | Dec 31 14:10:36 2040 GMT | | | | |
| <input type="checkbox"/> | ▶ Atos TrustedRoot 2011 | CA certificate | | Dec 31 23:59:59 2030 GMT | | | | |
| <input type="checkbox"/> | ▶ Bypass Class 2 Root CA | CA certificate | | Oct 26 08:38:03 2040 GMT | | | | |
| <input type="checkbox"/> | ▶ Bypass Class 3 Root CA | CA certificate | | Oct 26 08:28:58 2040 GMT | | | | |
| <input type="checkbox"/> | ▶ COMODO ECC Certification Authority | CA certificate | | Jan 18 23:59:59 2038 GMT | | | | |
| <input type="checkbox"/> | ▶ D-TRUST Root Class 3 CA 2 EV 2009 | CA certificate | | Nov 5 08:50:46 2029 GMT | | | | |
| <input type="checkbox"/> | ▶ Equifax Secure Global eBusiness CA-1 | CA certificate | | Jun 21 04:00:00 2020 GMT | | | | |
| <input type="checkbox"/> | ▶ Equifax Secure eBusiness CA-1 | CA certificate | | Jun 21 04:00:00 2020 GMT | | | | |
| <input type="checkbox"/> | ▶ GeoTrust Primary Certification Authority - G2 | CA certificate | | Jan 18 23:59:59 2038 GMT | | | | |
| <input type="checkbox"/> | ▶ GeoTrust Primary Certification Authority - G3 | CA certificate | | Dec 1 23:59:59 2037 GMT | | | | |
| <input type="checkbox"/> | ▶ GlobalSign | CA certificate | | Mar 18 10:00:00 2029 GMT | | | | |
| <input type="checkbox"/> | ▶ Go Daddy Root Certificate Authority - G2 | CA certificate | | Dec 31 23:59:59 2037 GMT | | | | |
| <input type="checkbox"/> | ▶ HTTPS Management Certificate | Local certificate | Self-signed | Jan 19 03:14:07 2038 GMT | | | | |
| <input type="checkbox"/> | ▶ Izenpe.com | CA certificate | | Dec 13 08:27:25 2037 GMT | | | | |
| <input type="checkbox"/> | ▶ Microsec e-Szigno Root CA 2009 | CA certificate | | Dec 30 11:30:18 2029 GMT | | | | |
| <input type="checkbox"/> | ▶ NetLock Arany (Class Gold) Főtanúsítvány | CA certificate | | Dec 6 15:08:21 2028 GMT | | | | |

Total: 245 item(s)

The Certificates page provides all the settings for managing CA and Local Certificates.

The table on the Certificates page displays this information about certificates:

| Column | Information displayed |
|-------------|---|
| CERTIFICATE | Name of the certificate. |
| TYPE | Type of certificate: <ul style="list-style-type: none"> • CA certificate • Local certificate • Pending request |

| Column | Information displayed |
|-----------|---|
| VALIDATED | Validation information: <ul style="list-style-type: none"> • Blank • Self-signed • Expire in n days • Expired |
| Expires | Date and time the certificate expires. |

About Certificate Details

Clicking on the certificate's row in the table displays information about the certificate, which might include the following, depending on the type of certificate:

| HTTPS MANAGEMENT CERTIFICATE | |
|------------------------------|--|
| Signature Algorithm | sha256WithRSAEncryption |
| Certificate Issuer | C = US, O = GeoTrust Inc., OU = (c) 2008 GeoTrust Inc. - For authorized use only, CN = GeoTrust Primary Certification Authority - G3 |
| Subject Distinguished Name | C = US, O = GeoTrust Inc., OU = (c) 2008 GeoTrust Inc. - For authorized use only, CN = GeoTrust Primary Certification Authority - G3 |
| Public Key Algorithm | RSA 2048 bits |
| Certificate Serial Number | 15AC6E9419B2794B41F627A9C3180F1F |
| Valid from | Apr 2 00:00:00 2008 GMT |
| Expires On | Dec 1 23:59:59 2037 GMT |
| CRL Status | CRL is required |

- **Signature Algorithm**
- **Certificate Issuer**
- **Subject Distinguished Name**
- **Public Key Algorithm**
- **Certificate Serial Number**
- **Valid from**
- **Expires On**
- **CRL Status (for Pending requests and local certificates)**

The details depend on the type of certificate. **Certificate Issuer**, **Certificate Serial Number**, **Valid from**, and **Expires On** are not shown for Pending requests as this information is generated by the Certificate provider.

Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates might also be imported to verify local Certificates and peer Certificates used in IKE negotiation.

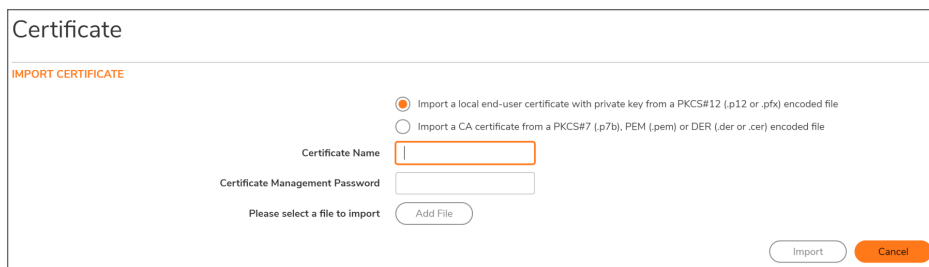
Topics:

- [Importing a Certificate Authority Certificate](#)
- [Importing a Local Certificate](#)
- [Creating a PKCS-12 Formatted Certificate File \(Linux Systems Only\)](#)

Importing a Local Certificate

To import a certificate from a certificate authority:

1. Navigate to **Device | Settings > Certificates**.
2. Click **Import**.
The **IMPORT CERTIFICATE** dialog is displayed.



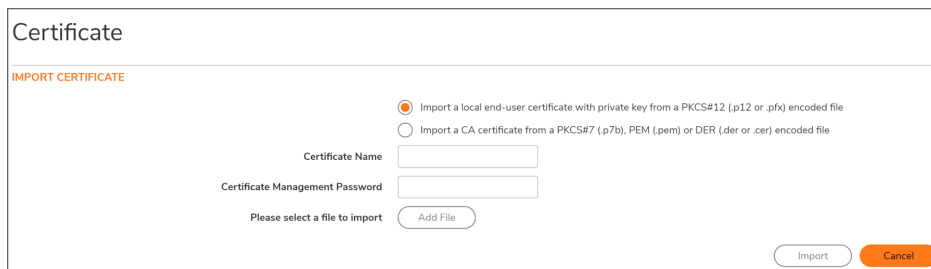
The screenshot shows a dialog box titled "Certificate" with a sub-header "IMPORT CERTIFICATE". It contains two radio button options: "Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file" (selected) and "Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file". Below these are two text input fields: "Certificate Name" and "Certificate Management Password". At the bottom left, there is a prompt "Please select a file to import" and an "Add File" button. At the bottom right, there are "Import" and "Cancel" buttons.

3. Enter a certificate name in the **Certificate Name** field.
4. Enter the password used by your Certificate Authority to encrypt the PKCS#12 file in the **Certificate Management Password** field.
5. Click **Add File** to locate the certificate file.
6. Select the certificate and click **Open**.
7. Click **Import** to import the certificate into the firewall. When it is imported, you can view the certificate entry in the Certificates table.
8. Click the certificate displayed on the **Certificates** page, to know the status and other details.

Importing a Certificate Authority Certificate

To import a local certificate:

1. Navigate to **Device | Settings > Certificates**.
2. Click **Import**.
The **IMPORT CERTIFICATE** dialog is displayed.



Certificate

IMPORT CERTIFICATE

Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file

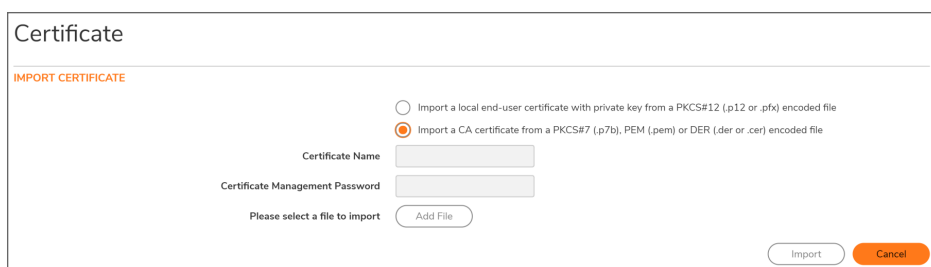
Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Certificate Name

Certificate Management Password

Please select a file to import

3. Choose **Import a CA certificate from a PKCS#7 (*.p7b) or DER (.der or .cer) encoded file**. The Import Certificate dialog settings change.



Certificate

IMPORT CERTIFICATE

Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file

Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file

Certificate Name

Certificate Management Password

Please select a file to import

4. Click **Add File** and locate the certificate file.
5. Click **Open**.
6. Click **Import** to import the certificate into the firewall. When it is imported, you can view the certificate entry in the **Certificates** table.
7. Click the certificate displayed on the **Certificates** page, to know the status and other details.

Creating a PKCS-12 Formatted Certificate File (Linux Systems Only)

A PKCS12-formatted certificate file can be created using Linux system with OpenSSL. To create a PKCS-12 formatted certificate file, one needs to have two main components of the certificate:

- Private key (typically a file with .key extension or the word key in the filename)
- Certificate with a public key (typically a file with .crt extension or the word cert as part of filename).

For example, the Apache HTTP server on Linux has its private key and certificate in these locations:

- `/etc/httpd/conf/ssl.key/server.key`
- `/etc/httpd/conf/ssl.crt/server.crt`

With these two files available, run the following command:

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

In this example **out.p12** become the PKCS-12 formatted certificate file and **server.key** and **server.crt** are the PEM-formatted private key and the certificate file respectively.

After running the **openssl** command, you are prompted for the password to protect/encrypted the file. After choosing the password, the creation of the PKCS-12-formatted certificate file is complete, and it can be imported into the appliance.

Deleting Certificates

① | **NOTE:** Built-in certificates cannot be deleted.

You can delete an imported certificate if it has expired or if you decide not to use third-party certificates for VPN authentication. You can always delete certificates you created.

To delete a certificate:

1. Navigate to **Device | Settings > Certificates**.
2. Hover over the certificate and click the **Delete** icon.

To delete multiple certificates:

1. Navigate to **Device | Settings > Certificates**.
2. Select the certificates that you want to delete by selecting the checkbox(es) next to the certificates.
① | **TIP:** To select all the certificates, select the checkbox next to the **Certificate** column in the header row.
3. Click the **Delete** icon at the top of the table.

Generating a Certificate Signing Request

You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.

To generate a certificate signing request:

1. Navigate to **Device | Settings > Certificates**.
2. Click **New Signing Request**. The **Certificate** dialog is displayed.

The screenshot shows the 'Certificate' dialog box with the following fields and options:

- GENERATE CERTIFICATE SIGNING REQUEST**
- Certificate Alias**: Text input field.
- Country**: Dropdown menu.
- State**: Text input field.
- Locality, City or County**: Text input field.
- Company or Organiza...**: Text input field.
- Department**: Text input field.
- Group**: Text input field.
- Team**: Text input field.
- Common Name**: Text input field.
- Subject Distinguished Name**: Text input field.
- SUBJECT ALTERNATIVE NAME (OPTIONAL)**
- Domain Name**: Text input field.
- Signature Algorithm**: Dropdown menu (SHA1).
- Subject Key Type**: Dropdown menu (RSA).
- Subject Key Size/Curve**: Dropdown menu (1024 bits).
- Buttons**: Cancel and Generate.

3. Enter an alias name for the certificate in the **Certificate Alias** field.
4. Create a Distinguished Name (DN) using the drop-down menus shown in table below, then enter information for the certificate in the associated fields.

① **NOTE:** For each DN, you can select your country from the associated drop-down menu; for all other components, enter the information in the associated field.

| Drop-down menu | Select appropriate information |
|----------------------------------|--|
| Country | Country (default) State Locality or County Company or Organization |
| State | Country State (default) Locality, City, or County Company or Organization Department |
| Locality, City, or County | Locality, City, or County (default) Company or Organization Department Group Team |
| Company or Organization | Company or Organization (default) Department Group Team Common Name Serial Number E-Mail Address |
| Department | Department (default) Group Team Common Name Serial Number E-Mail Address |
| Group | Group (default) Team Common Name Serial Number E-Mail Address |
| Team | Team (default) Common Name Serial Number E-Mail Address |
| Common Name | Common Name (default) Serial Number E-Mail Address |

As you enter information for the components, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

Certificate

GENERATE CERTIFICATE SIGNING REQUEST

| | |
|----------------------------|-----------------------------|
| Certificate Alias | <input type="text"/> |
| Country ▼ | INDIA (IN) ▼ |
| State ▼ | Karnataka |
| Locality, City or County ▼ | Bangalore |
| Company or Organiza... ▼ | SonicWall |
| Department ▼ | Engineering |
| Group ▼ | TechPubs |
| Team ▼ | <input type="text"/> |
| Common Name ▼ | <input type="text"/> |
| Subject Distinguished Name | C: ,ST: Karnataka,L: Bangal |

5. Optionally, you can also attach a SUBJECT ALTERNATIVE NAME to the certificate after selecting the type from the drop-down menu:

- **Domain Name**
- **Email Address**
- **IPv4 Address**

6. Select a signature algorithm from the Signature Algorithm drop-down menu:

- **SHA1** (default)
- **MD5**
- **SHA256**
- **SHA384**
- **SHA512**

7. Select a subject key type from the Subject Key Type drop-down menu:

| | |
|----------------------|---|
| RSA (default) | A public key cryptographic algorithm used for encrypting data, |
| ECDSA | Encrypts data using the Elliptic Curve Digital Signature Algorithm, which has a high strength-per-key-bit security. |

8. Select a subject key size or curve from the **Subject Key Size/Curve** drop-down menu.

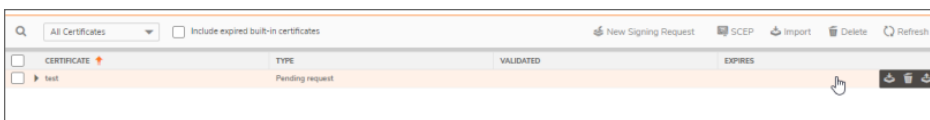
NOTE: Not all key sizes or curves are supported by a Certificate Authority, therefore, you should check with your CA for supported key sizes.

IF YOU SELECTED A KEY TYPE OF

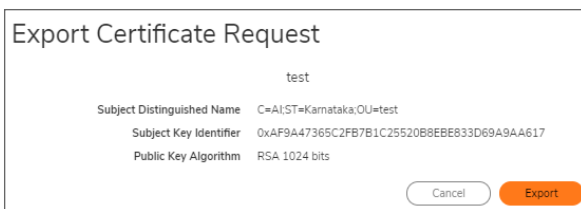
| RSA, select a key size | ECDSA, select a curve |
|----------------------------|---|
| 1024 bits (default) | prime256vi: X9.62.SECG curve over a 256 bit prime field (default) |
| 1536 bits | secp384r1: NIST/SECG curve over a 384 bit prime field |
| 2048 bits | secp521r1: NIST/SECG curve over a 521 bit prime field |
| 4096 bits | |

- Click **Generate** to create a certificate signing request file.

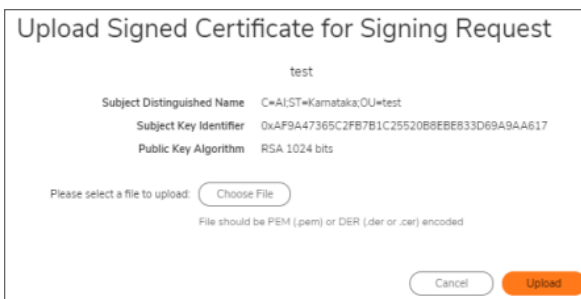
When the **Certificate Signing Request** is generated, a message describing the result is displayed and a new entry appears in the Certificates table with the type **Pending request**.



- Click the **Export** icon. The **Export Certificate Request** dialog is displayed.



- Click the **Export** icon to download the file to your computer. An **Opening <certificate>** dialog displays.
- Click **OK** to save the file to a directory on your computer.
You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.
- Click the **Upload** icon to upload the signed certificate for a signing request. The **Upload Certificate dialog** is displayed.



- Click **Choose File** to select a file.
- Select the file and click **Open**.
- Click **UPLOAD**.

Configuring Simple Certificate Enrollment Protocol

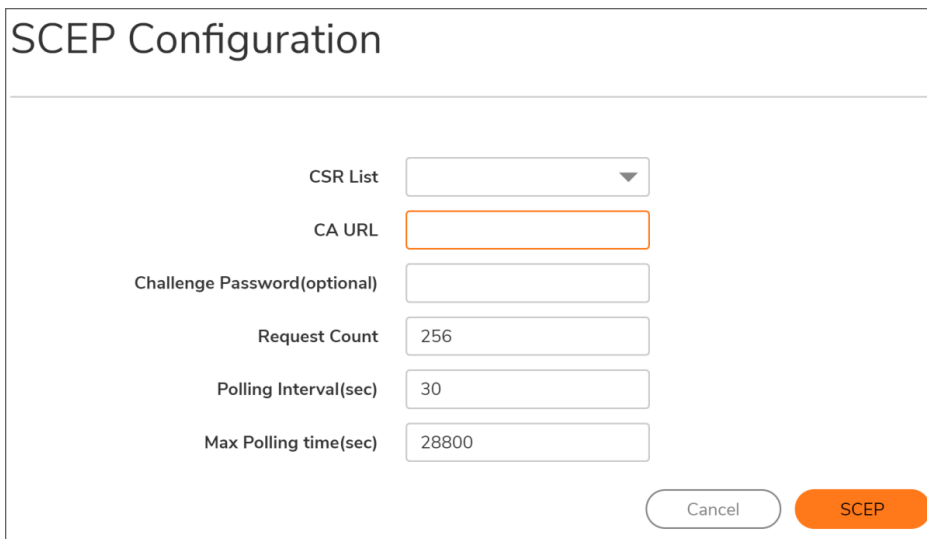
The Simple Certificate Enrollment Protocol (SCEP) is designed to support the secure issuance of certificates to network devices in a scalable manner. There are two enrollment scenarios for SCEP:

- SCEP server CA automatically issues certificates.
- SCEP request is set to PENDING and the CA administrator manually issues the certificate.

More information about SCEP can be found at: <http://tools.ietf.org/html/draft-nourse-scep-18> (Cisco Systems' Simple Certificate Enrollment Protocol draft-nourse-scep-18).

To use SCEP to issue certificates:

1. Generate a signing request as described in [Generating a Certificate Signing Request](#).
2. On the **Certificates** page, Click **SCEP**.
The **SCEP Configuration** dialog is displayed.



3. From **CSR List**, SonicOS selects a default CSR list automatically. If you have multiple CSR lists configured, you can modify this.
4. In the **CA URL** field, enter the URL for the Certificate authority.
5. If the **Challenge Password(optional)** field, enter the password for the CA if one is required.
6. In the **Request Count** field, enter the number of requests. The default value is **256**.
7. In the **Polling Interval(S)** field, you can modify the default value for duration of time, in seconds, between the sending of polling messages. the default value is 30 seconds.

8. In the **Max Polling Time(S)** field, you can modify the default value for the duration of time, in seconds, the firewall waits for a response to a polling message before timing out. The default value is 28800 seconds (8 hours).
9. Click **SCEP** to submit the SCEP enrollment.

The firewall contacts the CA to request the certificate. The time this takes depends on whether the CA issues certificates automatically or manually. After the certificate is issued, it is displayed in the list of available certificates on the **Device | Settings > Certificates** page, under the Imported certificates and requests or All certificates category.

Administering SNMP

You can manage the SonicWall security appliance using SNMP or SonicWall Global Management System (GMS). This section describes how to configure the SonicWall for management using SNMP. For information about managing the SonicWall appliance with GMS, see the *SonicWall GMS and SonicWall Management Services administration* documentation, available at <https://www.sonicwall.com/support/technical-documentation>.

Topics:

- [About SNMP](#)
- [Setting Up SNMP Access](#)
- [Configuring SNMP as a Service and Adding Rules](#)

About SNMP

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWall Security Appliance and receive notification of critical events as they occur on the network. The SonicWall Security Appliance supports SNMP v1/v2c/v3 and all relevant Management Information Base II (MIB-II) groups except **egp** and **at**.

SNMPv3 expands on earlier versions of SNMP and provides secure access to network devices by means of a combination of authenticating and encrypting packets.

Packet security is provided through:

- **Message Integrity:** ensures a packet has not been tampered with in transit
- **Authentication:** verifies a message comes from a valid source
- **Encryption:** encodes packet contents to prevent its being viewed by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up between a user and the group in which the user resides. The security level is the permitted level of security within a given security model. The security model and associated security level determine how an SNMP packet is handled. SNMPv3 provides extra levels of authentication and privacy, as well as additional authorization and access control.

Security Level, Authentication, and Encryption Based on SNMP Version shows how security levels, authentication, and encryption are handled by the different versions of SNMP.

SECURITY LEVEL, AUTHENTICATION, AND ENCRYPTION BASED ON SNMP VERSION

| Version | Level | Authentication Type | Encryption | Means of Authentication |
|---------|--------------|---------------------|------------|---|
| v1 | noAuthNoPriv | Community String | No | Community string match |
| v2c | noAuthNoPriv | Community String | No | Community string match |
| | noAuthNoPriv | Username | No | Username match |
| | authNoPriv | MD5 or SHA | No | Authentication is based on the HMAC-MD5 or HMSC-SRA algorithms. |
| v3 | authPriv | MD5 or SHA | DES or AES | Provides authentication is based on the HMAC-MD5 or HMSC-SRA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard, or AES 128-bit encryption, as well. |

The SonicWall Security Appliance replies to SNMP `Get` commands for MIB-II, using any interface, and supports a custom SonicWall MIB for generating trap messages. The custom SonicWall MIB is available for download from the SonicWall Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

You can view and configure SNMP settings. Settings cannot be viewed or modified by the user. SNMPv3 can be modified at the User or Group level. Access Views can be read, write, or both, and can be assigned to users or groups. A single View can have multiple Object IDs (OIDs) associated with it.

SNMPv3 settings for the SNMPv3 Engine ID are configurable under the **General** menu of the **Configure SNMP view** dialog. The **Engine ID** is used to authorize a received SNMP packet. Only matching packet EngineIDs are processed.

Setting Up SNMP Access

Setting up SNMP consists of:

- [Enabling and Configuring SNMP Access](#)
- [Setting Up SNMPv3 Groups and Access](#)

Enabling and Configuring SNMP Access

You can use either SNMPv1/v2 for basic functionality or configure the SonicWall security appliance to use the more extensive SNMPv3 options.

To use SNMP, you must first enable it.

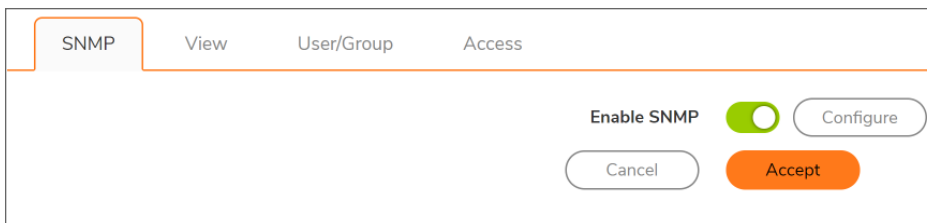
Topics:

- [Configuring Basic Functionality](#)
- [Configuring SNMPv3 Engine IDs](#)
- [Configuring Object IDs for SNMPv3 Views](#)
- [Creating Groups and Adding Users and Access](#)
- [Adding Access](#)

Configuring Basic Functionality

To enable SNMP:

1. Navigate to **Device | Settings > SNMP**.
2. Select **Enable SNMP**. By default, SNMP is disabled.



3. Click **Accept**. The SNMP information is populated on the SNMP page, and Configure becomes available.
4. To configure the SNMP interface, click **Configure**. The **Configure SNMP View** dialog is displayed.

The screenshot shows the 'Configure SNMP view' interface with the 'General' tab selected. The 'Advanced' tab is also visible. Under the 'GENERAL SETTINGS' section, there are the following fields:

- System Name
- System Contact
- System Location
- Asset Number
- Get Community Name
- Trap Community Name
- Host 1
- Host 2
- Host 3
- Host 4

At the bottom of the form, there are two buttons: 'Cancel' and 'Add'.

5. On the **General** page, enter the host name of the SonicWall security appliance in the **System Name** field.
6. Optionally, enter the network administrator's name in the **System Contact** field.
7. Optionally, enter an email address, telephone number, or pager number in the **System Location** field.
8. If the SNMPv3 configuration option is used, enter an asset number in the **Asset Number** field. Otherwise, this field is optional.
9. Enter a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.
10. Optionally, enter a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.
11. Enter the IP address(es) or host name(s) of the SNMP management system receiving SNMP traps in the **Host 1** through **Host n** fields. You must configure at least one IP address or host name, but up to the maximum number of addresses or host names for your system can be used.
12. If you:
 - Want to set up SNMPV3, go to [Configuring SNMPv3 Engine IDs](#) .
 - Finished setting up SNMP for now, click **Add**.

Configuring SNMPv3 Engine IDs

If SNMPv3 is used, you can configure the SNMPv3 Engine ID and SNMP priority. Configuring the SNMPv3 Engine ID provides maximum security for SNMP management.

To configure SNMPv3 engine IDs:

1. Navigate to **Device | Settings > SNMP**.
2. If you have not configured SNMP for your system, follow Step 1 through Step 11 in Configuring Basic Functionality.
3. Click **Advanced**.

Configure SNMP view

General Advanced

SNMP V3SETTINGS

Mandatory Require SNMPv3

Engine ID 80002225032CB8ED6946

SNMP OPTIONAL SETTINGS

Increase SNMP subsystem priority

Cancel Add

4. Select **Mandatory Require SNMPv3**. This disables SNMPv1/v2 and allows only SNMPv3 access, which provides maximum security for SNMP management.
 - ① | **IMPORTANT:** If you select this option, you must specify an asset number on the **General** page before clicking **OK**.
5. Enter the hexadecimal Engine ID number in the **Engine ID** field.

SonicOS automatically populates this field, but you can change it. This number is matched against received SNMP packets to authorize their processing; only packets whose Engine ID matches this number are processed.
6. Optionally, enable **Increase SNMP subsystem priority**.

For efficient system operation, certain operations might take priority over responses to SNMP queries. Enabling this option causes the SNMP subsystem to always respond and operate at a higher system priority.

 - ① | **IMPORTANT:** Enabling this option might affect the performance of the overall system.
7. Click **OK**. The SNMPv3 security options are now used in processing packets.

Configuring Object IDs for SNMPv3 Views

The SNMPv3 View shows access settings for Users and Groups. You create settings for users and groups, and these security settings are not user-modifiable. The SNMPv3 View defines the Object IDs (OID) and Object ID Groups, and is sometimes known as the SNMPv3 Access Object.

The SNMP View defines a collection of OIDs and OID groups. The initial set of default views cannot be changed or deleted. The default views reflect the most often used views, such as the root view, system view, IP, interfaces. The OIDs for these views are pre-assigned.

Additionally, you can create a custom view for specific users and groups.

You can modify any views that you create. You cannot modify the ones the system creates.

To configure OIDs for SNMPv3 views:

1. Navigate to **Device | Settings > SNMP**.
2. Click **View**.

| VIEW NAME | OID |
|-------------------------------------|----------------|
| <input type="checkbox"/> root | 1.3 |
| <input type="checkbox"/> system | 1.3.6.1.2.1.1 |
| <input type="checkbox"/> interfaces | 1.3.6.1.2.1.2 |
| <input type="checkbox"/> IP | 1.3.6.1.2.1.4 |
| <input type="checkbox"/> ICMP | 1.3.6.1.2.1.5 |
| <input type="checkbox"/> TCP | 1.3.6.1.2.1.6 |
| <input type="checkbox"/> UDP | 1.3.6.1.2.1.7 |
| <input type="checkbox"/> ifMIB | 1.3.6.1.2.1.31 |

3. In the View page, click **+ Add**. The **View Name** dialog box is displayed.

View Name

View Name

OID ASSOCIATED WITH THE VIEW

+ Add OID Refresh

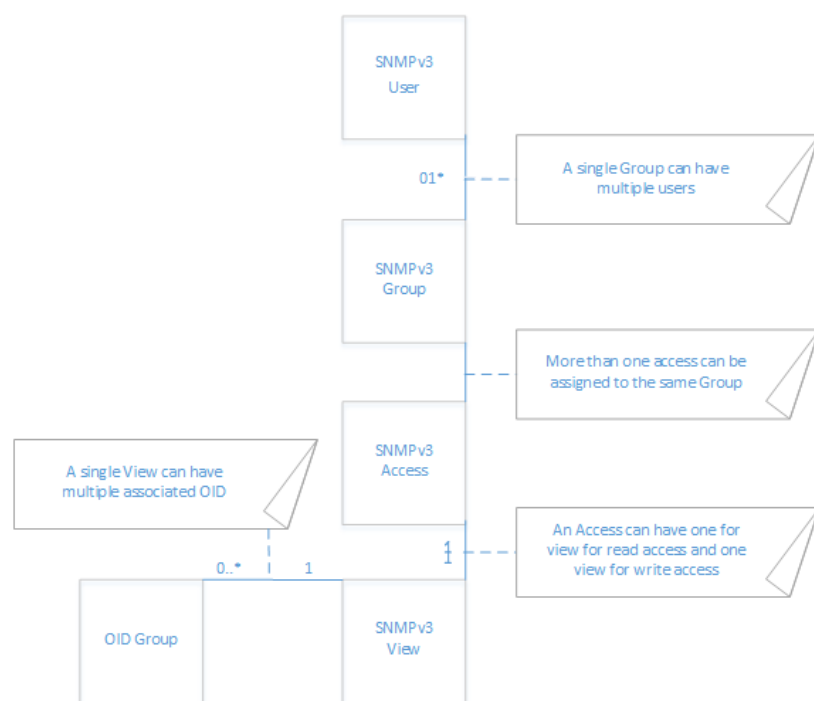
OID
No Data

Cancel OK

4. Enter a meaningful name in the **View Name** field.
5. Click **Add OID** to add OID to the View being created. The **Add SNMP OID** dialog is displayed.
6. Enter name in the **OID Name** field and click **OK**.
The OIDs associated with the View Name is listed in the OID table. To delete an OID from the OID List, hover over the OID and click **Delete**.
7. Add any more OIDs to associate with the View.
8. Click **OK**. The new view is displayed in the View page.

Setting Up SNMPv3 Groups and Access

SNMPv3 allows you to set up and assign groups and access with differing levels of security. Object IDs are associated with various levels of permissions, and a single view can be assigned to multiple objects. SNMPv3 group and user access shows how access for groups and users are associated with these different permission levels.



Creating Groups and Adding Users and Access

Topics:

- [Creating a Group](#)
- [Adding Users](#)
- [Adding Access](#)

Creating a Group

To create a group:

1. Navigate to **Device | Settings > SNMP**.
2. Click **User/Group**.
3. Click **Add Group**.

The image shows a dialog box titled "Add SNMP Group". It contains a text input field labeled "Group Name" with a cursor inside. Below the input field are two buttons: "Cancel" and "OK".

4. In the **Add SNMP Group** dialog, enter the name in the **Group Name** field.
The group name can contain up to 32 alphanumeric characters.
5. Click **OK**
The table in the **User/Group** page is updated to display the newly added group.

The image shows a screenshot of the "User/Group" page in the SNMP configuration interface. The page has tabs for "SNMP", "View", "User/Group", and "Access", with "User/Group" selected. Below the tabs is a search bar and several action buttons: "+ Add Group", "Add Name", "Delete", and "Refresh". A table below shows a list of groups with a checkbox and a name. The first row is a header with a checkbox and the text "NAME". The second row has a checkbox and the text "TechPubs".

Adding Access

SNMPv3 Access is an object that:

- Defines the read/write access rights of an SNMPv3 View.
- Can be assigned to an SNMPv3 Group.

Multiple groups can be assigned to the same Access object. An Access object can also have multiple views assigned to it.

To create an access object:

1. Navigate to **Device | Settings > SNMP**.
2. Click **Access**.
3. Click **+ Add**.

The **Access Name** dialog is displayed.

The image shows a dialog box titled "Access Name". It contains four fields: "Access Name" with a text input field containing "Enter View Name"; "Read View" with a dropdown menu showing "Select a View"; "Master SNMPv3 Group" with a dropdown menu showing "Select a Group"; and "Access Security Level" with a dropdown menu showing "None". Below the fields are two buttons: "Cancel" and "OK".

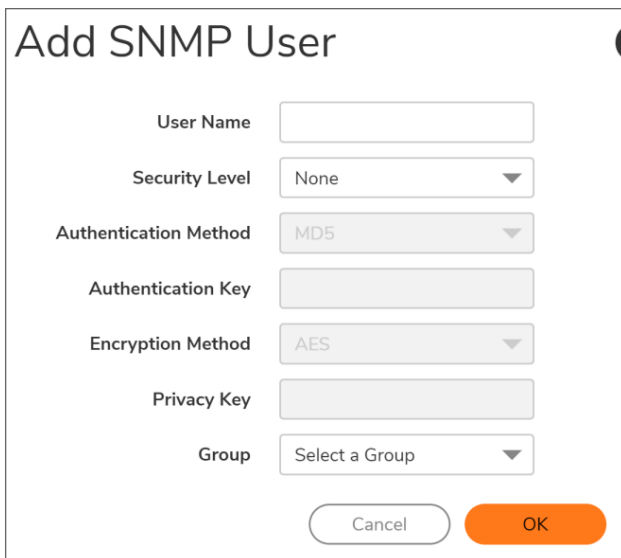
4. Enter a friendly name in the **Access Name** field.
5. From **Read View**, select a view from the list of available views.

6. From **Master SNMPv3 Group**, select a group from the list of available groups.
① **NOTE:** Access can be assigned to only one SNMPv3 group, but a group can be associated with multiple Access objects.
7. From Access Security Level, select a security level:
 - **None**
 - **Authentication Only**
 - **Authentication and Privacy**
8. Click **OK**. The Access object is added to the table in the Access page.

Adding Users

To add users:

1. Navigate to **Device | Settings > SNMP**.
2. Click **User/Group**.
3. Click **Add Name**.



The screenshot shows a dialog box titled "Add SNMP User". It contains the following fields and controls:

- User Name:** A text input field.
- Security Level:** A dropdown menu with "None" selected.
- Authentication Method:** A dropdown menu with "MD5" selected.
- Authentication Key:** A text input field.
- Encryption Method:** A dropdown menu with "AES" selected.
- Privacy Key:** A text input field.
- Group:** A dropdown menu with "Select a Group" selected.
- Buttons:** "Cancel" and "OK" buttons at the bottom.

4. Enter the user name in the **User Name** field.
5. Select a security level from Security Level:
 - **None** (default)
 - **Authentication only** – Two new options appear:
 - **Authentication Method** – Select one of these authentication methods: MD5 or SHA1.
 - **Authentication Key** – Enter an authentication key in the field. The key can be any string of 8 to 32 printable characters

- **Authentication and Privacy** – More options appear:
 - Select an encryption method from the Encryption Method drop-down menu: AES or DES.
 - Enter the encryption key in the **Privacy Key** field. The key can be any string of 8 to 32 printable characters.
6. Select a group from **Group** dropdown box.
 7. Click **OK**. The user is added to the User/Group table and added to the appropriate group.

Configuring SNMP as a Service and Adding Rules

By default, SNMP is disabled on the SonicWall Security Appliance. To enable SNMP, you must first enable SNMP on the **Device | Settings > SNMP** page, and then enable it for individual interfaces. To do this, go to the **NETWORK | System > Interfaces** page and edit the interface to enable SNMP. For more information about configuring SNMP as a service and adding rules, see *Configuring Interfaces* section in the *SonicOS 7.0 System* document.

If your SNMP management system supports discovery, the SonicWall Security Appliance agent automatically discovers the SonicWall Security Appliance on the network. Otherwise, you must add the SonicWall Security Appliance to the list of SNMP-managed devices on the SNMP management system.

Firmware Settings

Topics:

- [Firmware Management and Backup](#)
- [Creating a Backup Firmware Image](#)
- [Updating Firmware](#)
- [Importing and Exporting Settings](#)
- [Configuring Firmware and Backup Settings](#)

Firmware Management and Backup

The **Device | Settings > Firmware and Settings** page provides settings that allow for easy firmware upgrade and preferences management.

FIRMWARE MANAGEMENT AND BACKUP

Create Backup
 Import/Export Configuration
 Upload Firmware
 Settings

LOCAL

| # | CURRENT FIRMWARE VERSION | FIRMWARE LOAD DATE | FIRMWARE BUILD DATE | USERNAME | COMMENTS | BOOT |
|---|---|---------------------|---------------------|----------|-------------------------------|------|
| 1 | SonicOS Enhanced 7.0.0.0-60v-42-P171-59b1acaf ✓ | 03/18/2020 12:09:15 | 03/12/2020 04:05:39 | | This is the current firmware. | |

Total: 1 item(s)

CLOUD

| # | CURRENT FIRMWARE VERSION | FIRMWARE LOAD DATE | FIRMWARE BUILD DATE | USERNAME | COMMENTS | BOOT |
|---------|--------------------------|--------------------|---------------------|----------|----------|------|
| No Data | | | | | | |

Total: 0 item(s)

LOCAL PREF BACKUP

| # | CURRENT FIRMWARE VERSION | FIRMWARE LOAD DATE | FIRMWARE BUILD DATE | USERNAME | COMMENTS | BOOT |
|---------|--------------------------|--------------------|---------------------|----------|----------|------|
| No Data | | | | | | |

Total: 0 item(s)

The Firmware & Backups page allows you to:

- Create and schedule backups; see [Creating a Backup Firmware Image](#).
- View local, cloud backups; see [Creating a Backup Firmware Image](#)

- Search the listed backups; see [Searching the Table](#).
- Import and export configurations; see [Importing Settings](#) and [Exporting Settings](#).
- Upload firmware images and system settings; see [Updating Firmware](#).
- Configure settings; see [Configuring Firmware and Backup Settings](#).
- Boot to your choice of firmware and system settings; see [Updating Firmware](#).

Firmware Management & Backup Tables

Topics:

- [Local Table](#)
- [Cloud Table](#)
- [Show Configuration Files Table](#)

Local Table

The Local section of the Firmware Management & Backup table displays:

| LOCAL | | | | | | |
|------------------|--|---------------------|---------------------|----------|-------------------------------|------|
| # | CURRENT FIRMWARE VERSION | FIRMWARE LOAD DATE | FIRMWARE BUILD DATE | USERNAME | COMMENTS | BOOT |
| 1 | SonicOS Enhanced 7.0.0.0-60v-42-P171-59b1acaf✓ | 03/18/2020 12:09:15 | 03/12/2020 04:05:39 | | This is the current firmware. | ⏻ |
| Total: 1 item(s) | | | | | | |










- **FIRMWARE VERSION** - firmware currently loaded on the firewall
- **FIRMWARE LOAD DATE** - the date and time the firmware was installed on the appliance
- **FIRMWARE BUILD DATE** - the date and time the firmware was created
- **CONFIGURATION DATE** - the date and time when the configuration of the appliance was last updated
- **USERNAME**- the user who installed or updated the firmware
- **COMMENTS** - an Information icon that, when moused over, displays information about the firmware or backup file. If you did not specify a comment when creating a backup, a default comment is displayed:
 - This is the current firmware
 - This is the local backup
 - Custom comment
- **BOOT**- clicking the Boot icon displays whether to reboot the firewall with the current or factory default configuration:

⚠ **CAUTION:** Clicking Boot next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.

⚠ **CAUTION:** When uploading firmware to the firewall, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.

- **FIRMWARE ACTIONS** - displays the Download icon; clicking the icon saves the firmware to a new location on your computer or network. Only uploaded firmware can be saved to a different location

Cloud Table










| CLOUD | | | | | | |
|-----------------------|--|---------------------|--|----------|------------------------------------|---|
| # | FIRMWARE VERSION | FIRMWARE LOAD DATE | FIRMWARE BUILD DATE | USERNAME | COMMENTS | BOOT |
| 1 | 7.0.0.0-60v-42-P171-59b1acaf | 03/01/2010 08:00:00 | 03/18/2020 12:09:15 | System | This is the cloud backup firmware. | |
| CONFIGURATION VERSION | | | | | | |
| | CONFIGURATION VERSION | CONFIGURATION DATE | BACKUP TYPE | COMMENTS | USERNAME | BOOT |
| | sonicwall-2CB8ED69468C-20200326042131.exp.gz | 03/26/2020 04:20:24 | Manual   | | admin |  |
| | sonicwall-2CB8ED69468C-20200326042122.exp.gz | 03/26/2020 04:20:16 | Manual   | | admin |  |
| | sonicwall-2CB8ED69468C-20200326013751.exp.gz | 03/26/2020 01:36:44 | Manual   | | admin |  |

The **Cloud** table of the **Firmware and Settings** page displays the:

- **Firmware Version** - firmware backed up to the cloud. Up to 3 versions of each firmware are listed.
- **Firmware Load Date** - the date and time the firmware was installed on the appliance
- **Firmware Build Date** - the date and time the firmware was created
- **Username** - the user who installed or updated the firmware
- **Comment** - Displays information about the firmware or backup file. If you did not specify a comment when creating a backup, a default comment is displayed:
 - Automated backup
 - This is the cloud backup firmware
 - Custom comment

Show Configuration Files Table

Clicking the arrow mark next to firmware version displays information about the backup files on the cloud for that firmware version.

| CLOUD | | | | | | |
|-----------------------|--|---------------------|--|----------|------------------------------------|---|
| # | FIRMWARE VERSION | FIRMWARE LOAD DATE | FIRMWARE BUILD DATE | USERNAME | COMMENTS | BOOT |
| 1 | 7.0.0.0-60v-42-P171-59b1acaf | 03/01/2010 08:00:00 | 03/18/2020 12:09:15 | System | This is the cloud backup firmware. | |
| CONFIGURATION VERSION | | | | | | |
| | CONFIGURATION VERSION | CONFIGURATION DATE | BACKUP TYPE | COMMENTS | USERNAME | BOOT |
| | sonicwall-2CB8ED69468C-20200326042131.exp.gz | 03/26/2020 04:20:24 | Manual   | | admin |  |
| | sonicwall-2CB8ED69468C-20200326042122.exp.gz | 03/26/2020 04:20:16 | Manual   | | admin |  |
| | sonicwall-2CB8ED69468C-20200326013751.exp.gz | 03/26/2020 01:36:44 | Manual   | | admin |  |

CONFIGURATION VERSION Version number of the backup file.

CONFIGURATION DATE Date the backup file was created.

BACKUP TYPE Type of backup, **Auto** or **Manual**, as well as these icons:

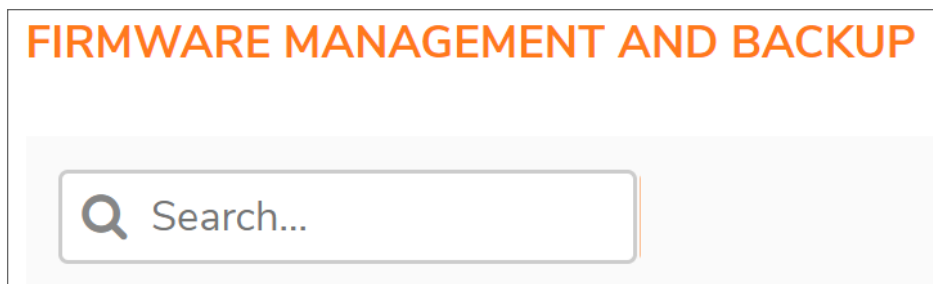
| | |
|------------------------------|---|
| | <ul style="list-style-type: none"> • Retain Configuration File – selecting this icon prevents the backup file from being overwritten during an auto or manual backup. • Gold Master – selecting this icon designates the backup file as the Gold Master backup file, that is, the combination prefs file and firmware image combination you can designate as the most stable configuration. When you designate an entry as a gold master, it cannot be deleted or unpinned until or unless you designate it as a non-gold, standard file. This protects your most stable version. Only one backup can be a gold standard. |
| COMMENTS | <p>Displays information about the firmware or backup file. If you did not specify a comment when creating a backup, a default comment is displayed:</p> <ul style="list-style-type: none"> • Automated backup • This is the cloud backup firmware • Custom comment |
| USERNAME | User who installed or updated the firmware. |
| BOOT | <p>Clicking the Boot icon displays whether to reboot the firewall with the current or factory default configuration:</p> <p>⚠ CAUTION: Clicking Boot next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.</p> <p>⚠ CAUTION: When uploading firmware to the firewall, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.</p> |
| Configuration Actions | <p>Displays icons:</p> <ul style="list-style-type: none"> • Download – Saves the firmware to a new location on your computer or network. Only uploaded firmware can be saved to a different location • Edit Comment – Allows you to edit the default or custom comment. • Delete – Deletes the backup file. |

Searching the Table

You can search the backup tables with the Search function. Although the Search function applies to all tables, results are displayed only for visible tables. For example, to see the results of the various Show Configuration Files tables, you must display them one by one.

To search the tables:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Enter the search criterion in the **Search** field.



The results are highlighted in the table.

Creating a Backup Firmware Image

When you click **Create Backup**, the SonicWall security appliance takes a snapshot of your current system state, firmware, and configuration preferences, and makes the snapshot the new System Backup firmware image. You can save backups locally or on the cloud. You can also schedule backups to occur automatically.

① | **IMPORTANT:** Creating backup overwrites the existing Backup firmware image as necessary.

Use the Backup file for saving good configurations and then booting them if upgrades or future configurations cause instability or other serious issues. The configuration file is conveniently saved onboard. The date and time the file was created as well as the firmware version in use at the time is displayed in the Firmware Management & Backup table. The dates for each item listed in the Firmware Management & Backup table are the build dates for the firmware images themselves.

You can create a backup of your current configuration settings on the appliance to be used with the current firmware version or with a newly uploaded firmware version.

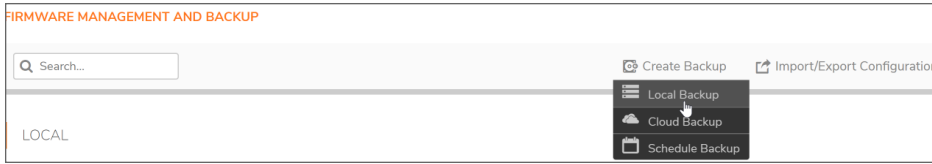
Topics:

- [Creating a Local Backup Firmware Image](#)
- [Creating a Cloud Backup Firmware Image](#)
- [Scheduling Firmware Image Backups](#)

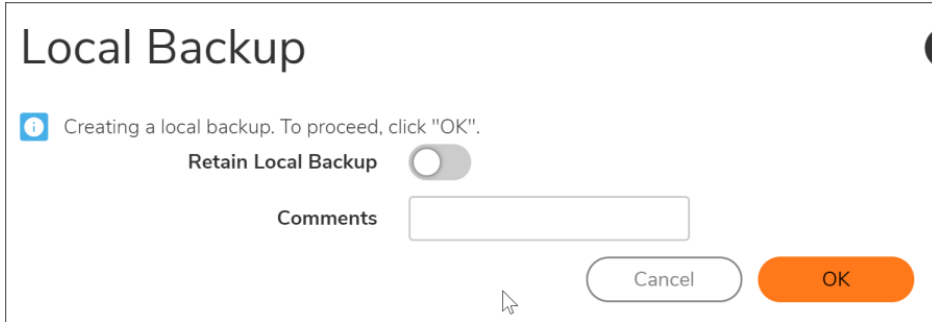
Creating a Local Backup Firmware Image

To create a local backup file:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Create Backup > Local Backup**.



3. In the **Local Backup** dialog, do the following to create a backup:



- a. Enabling **Retain Local Backup** option for local backup helps to retain configuration file so it is not overwritten during auto or local backup. To retain local backup, enable **Retain Local Backup**.
- b. Enter comments in the **Comments** field.
- c. Click **OK**.

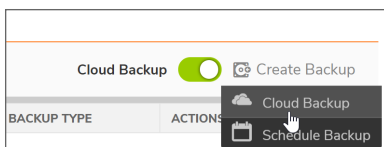
The backup image created on local storage is listed under LOCAL section.

① | **NOTE:** you must perform these steps each time for a local backup.

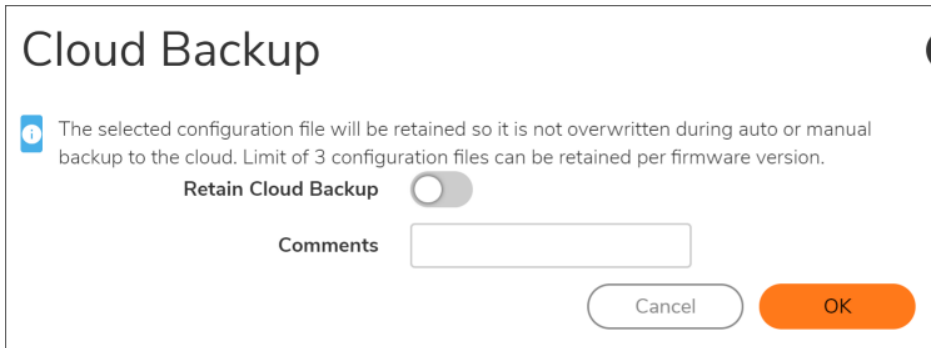
Creating a Cloud Backup Firmware Image

To create a cloud backup file:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Cloud Backups**.
3. If Cloud Backup has never been enabled, enable **Cloud Backup**.
4. Click **Create Backup > Cloud Backup**.



5. Select **Retain Cloud Backup** if you want this backup configuration file saved and not overwritten when you create additional backup configuration files on the cloud.



6. You can use the `Comment` field to optionally create a comment associated with the backup configuration file to make it easier to identify later.
7. Click **OK**. It may take a few minutes to create the backup file.

Scheduling Firmware Image Backups

① **NOTE:** Cloud Backup must be enabled before you can schedule backups of your firmware configuration file. This feature is not supported for Local Backup.

To schedule a backup:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Cloud Backups**.
3. If Cloud Backup has never been enabled, enable **Cloud Backup**.
4. Click **Create Backup > Schedule Backup**.
The **Schedule Backup** dialog is displayed.

5. Set the options for the backup you want to create:

- To schedule a one-time backup, see [Scheduling a One-Time Backup](#)
- To schedule a recurring backup, see [Scheduling Recurring Backups](#)
- To schedule a mixed backup schedule, select **Mixed** and configure the settings based on the procedure explained in [Scheduling a One-Time Backup](#) and [Scheduling Recurring Backups](#). This schedule occurs repeatedly during the same configured hours and days of the week, between the configured start and end dates.

Schedule Backup

Schedule Name: Cloud Backup Hours

Schedule Type: Once, Recurring, Mixed

RECURRING

| Select Day | |
|------------|-------------------------------------|
| Sunday | <input checked="" type="checkbox"/> |
| Monday | <input checked="" type="checkbox"/> |
| Tuesday | <input checked="" type="checkbox"/> |
| Wednesday | <input checked="" type="checkbox"/> |
| Thursday | <input checked="" type="checkbox"/> |
| Friday | <input checked="" type="checkbox"/> |
| Saturday | <input checked="" type="checkbox"/> |

Select All:

Start Time: 00:00:00

End Time: 00:00:00

Add

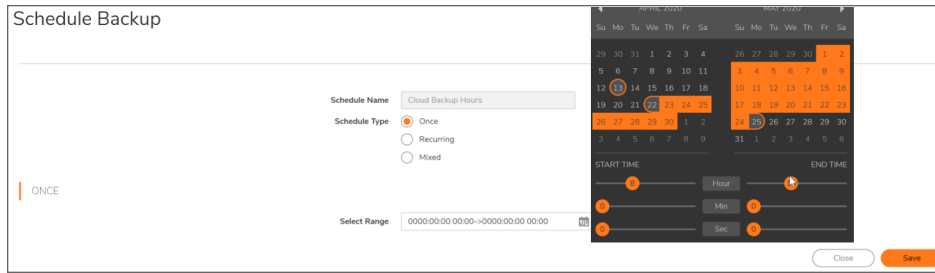
| Schedule List | |
|--|--------------------------|
| Mon-Tue-Wed-Thu-Fri-sat-Sun 02:00 to 03:00 | <input type="checkbox"/> |

Close Save

Scheduling a One-Time Backup

To schedule one-time backup:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Cloud Backups**.
3. If Cloud Backup has never been enabled, enable **Cloud Backup**.
4. Click **Create Backup > Schedule Backup**.
5. In the **Schedule Backup** page, do the following:
 - a. Select **Once** as **Schedule Type**.
 - b. In **ONCE** section, click calendar icon in **Select Range** field and set the schedule.
 - c. In the **Once** section, set the duration during which you want the backup to be created. Select the Year, Month, Day, Hour, and Minute from the drop-down menus to set the Start and End period for the backup.

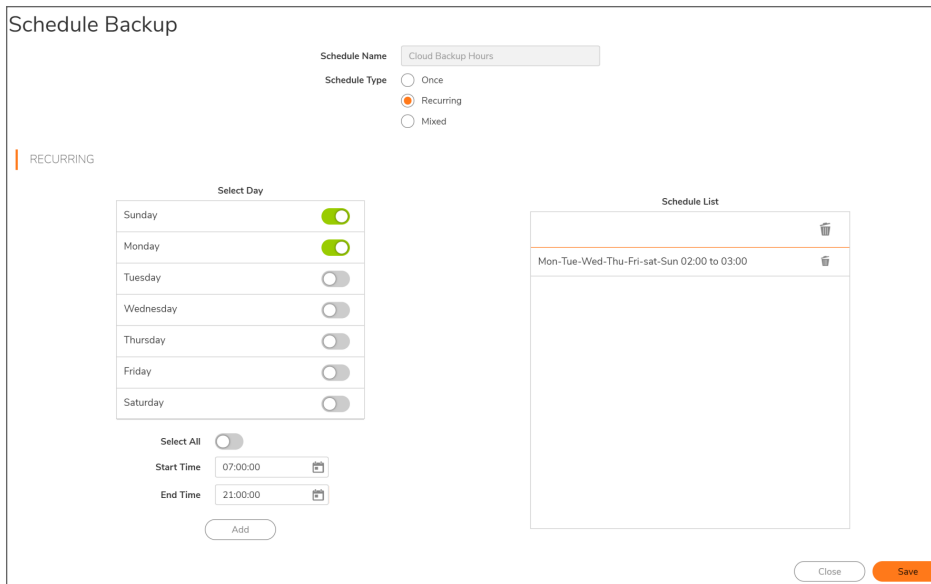


d. Click **Save**.

Scheduling Recurring Backups

To schedule recurring backups:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Cloud Backups**.
3. If Cloud Backup has never been enabled, enable **Cloud Backup**.
4. Click **Create Backup > Schedule Backup**.
5. Select **Recurring** as the **Schedule Type**.
6. Do the following in the **Recurring** section:



- a. Select the days on which you want the backup created. Click **Select All** to select all the days at once.
- b. Enter the Start Time and Stop Time for the report in 24-hour format (for example, 02:00 for 2:00am and 14:00 for 2:00pm).

- c. Click **Add** to add that report to the **Schedule List**.
 - d. Repeat these steps for each scheduled backup you want to create.
7. Click **Save**.

Deleting Scheduled Backups


To delete selected scheduled backups:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Cloud Backups**.
3. Click **Create Backup > Schedule Backup**.
The **Schedule Backup** dialog is displayed.
4. Click **Delete** icon on the scheduled backups listed in the **Schedule List** section.
5. To delete all the schedules at once, click **Delete** icon in the header row.

Updating Firmware

You can update firmware manually or use the Firmware Auto Update feature.

 **CAUTION:** Uploading new firmware will overwrite any existing uploaded firmware image.

 **NOTE:** Before uploading new firmware, it is recommended that you create a backup of your current settings. See [Creating a Backup Firmware Image](#) for more information on creating backups of your current configuration settings.

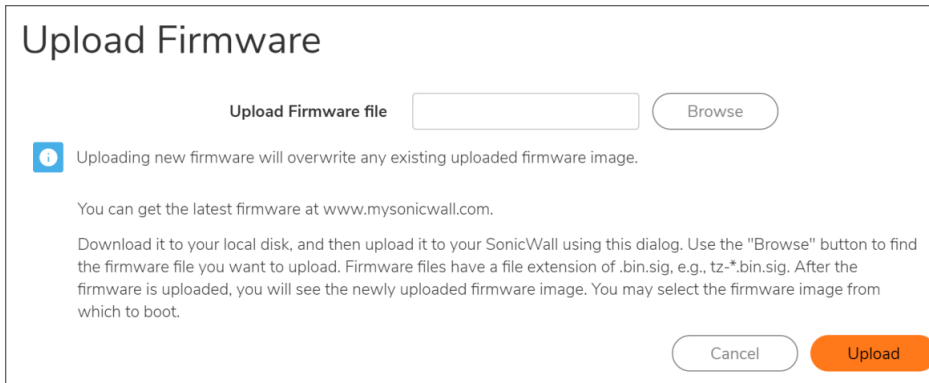
Topics:

- [Updating Firmware Manually](#)
- [Firmware Auto Update](#)
- [Using SafeMode to Upgrade Firmware](#)

Updating Firmware Manually

To update firmware manually:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Upload Firmware**.
3. Click **OK** to create a backup of your current settings before uploading new firmware.
The **Upload Firmware** dialog displays.



4. Click **Browse**. The File Upload dialog displays.
5. Browse to the firmware file located on your local drive.
6. Click **Open**.
7. Click **Upload** to upload the new firmware to the SonicWall security appliance. A success message displays in the Status bar, and the Firmware Management table displays the new firmware.
8. Click the **Boot** icon for the firmware you just downloaded.
9. Select whether you want to install the new firmware with your current configuration or a the default configuration.
10. Click **OK**. A message about the time to boot the firmware displays.
11. Click **OK**. A message about the boot status displays in the Status bar.
12. After the restart, when you log in again, the **Device | Settings > Firmware and Settings** page reflects the firmware update.

Firmware Auto Update

SonicOS supports the Firmware Auto Update feature, which helps ensure that your SonicWall security appliance has the latest firmware release.

To set the Firmware Auto Update options:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**. The Settings popup dialog displays
3. Click **Firmware Auto Update**.
4. Choose either:
 - **Enable Firmware Auto-Update** - Displays an **Alert** icon when a new firmware release is available. This option is selected by default.

- **Download new firmware automatically when available** - Downloads new firmware releases to the SonicWall security appliance when they become available. This option is not selected by default.

5. Click **OK**.

Using SafeMode to Upgrade Firmware

To Reviewers: Please verify this topic

If you are unable to connect to the SonicOS management interface, you can restart the security appliance in SafeMode. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface.

To use SafeMode to upgrade firmware:

1. Connect your computer to the X0 port on the appliance and configure your computer with an IP address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. To force the appliance into SafeMode, use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the **Reset** button on the front of the SonicWall appliance for at least twenty seconds, until the **Test** light begins blinking.
3. The **Test** light begins to blink when the SonicWall security appliance has rebooted into SafeMode.
4. Enter 192.168.1.254 into your computer's Web browser to access the SafeMode management interface.
5. Click **Upload New Firmware**.
6. Browse to the location where you saved the SonicOS firmware image.
7. Select the file and click **Upload**.
8. Select the Boot icon in the row for one of the following:
 - **Uploaded Firmware - New!** - Use this option to restart the appliance with your current configuration settings.
 - **Uploaded Firmware with Factory Default Settings- New!** - Use this option to restart the appliance with default configuration settings.
9. In the confirmation dialog, click **OK** to proceed.
10. To connect to SonicOS through the LAN or WAN interface of the firewall:
 - a. Disconnect your computer from the MGMT port.
 - b. Either:
 - Reconfigure it to automatically obtain an IP address and DNS server address.
 - Reset it to its normal static values.
11. Connect your computer to the local network.
12. Point your browser to the LAN or WAN IP address of the SonicWall appliance.

13. After successfully booting the firmware, the log-in screen displays. If you restarted with factory default settings, enter the default user name and password (**admin/password**) to access the SonicOS management interface.

Importing and Exporting Settings

You can choose to import and export firmware management configuration settings.

Topics:

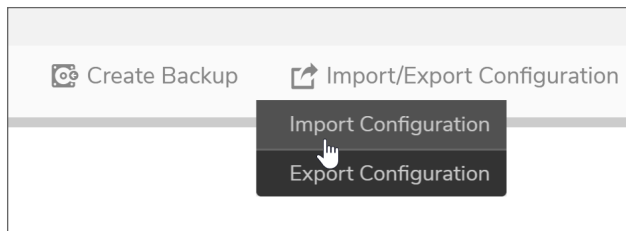
- [Importing Settings](#)
- [Exporting Settings](#)

Importing Settings

① **NOTE:** Before importing new configuration, it is recommended to export the current configuration or upload a copy to the cloud.

To import a previously saved preferences file into the firewall:

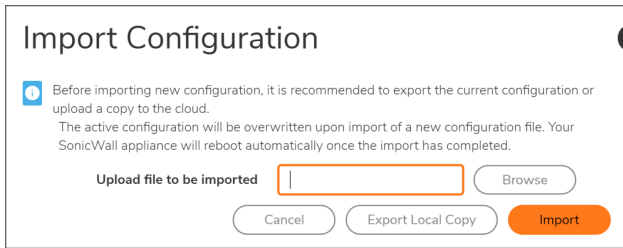
1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Import/Export Configuration > Import Configuration**.



① **IMPORTANT:** It is recommended that you create a backup, either locally or to the cloud, before proceeding. See [Creating a Local Backup Firmware Image](#) or [Creating a Cloud Backup Firmware Image](#) for instructions on creating a firmware configuration backup.

3. In the Import Configuration dialog, click **Browse** to select the previously saved preference file with the configuration settings into firewall.

① **NOTE:** The file you choose should have .exp file name extension.



4. Click **Import**.

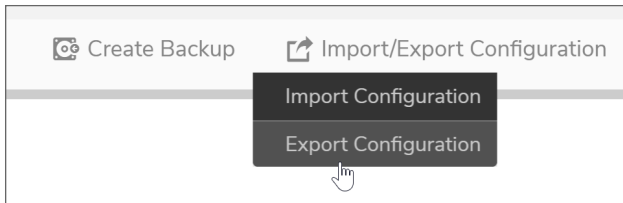
The active configuration will be overwritten upon import of a new configuration file. Your SonicWall appliance will reboot automatically once the import has completed.

Exporting Settings

The exported preferences file can be imported into the security appliance if it is necessary to reset the firmware.

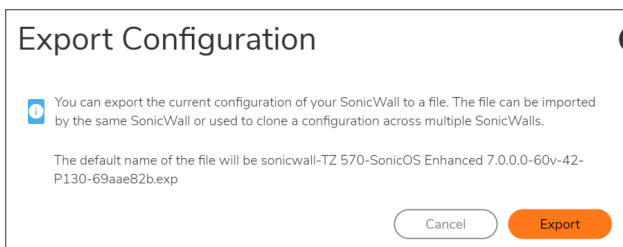
To export configuration settings from the firewall:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Import/Export Configuration > Export Configuration**.



3. In the Export Configuration window, click **Export**.

IMPORTANT: The current configuration of your SonicWall appliance is exported to a .exp file and is available in your local system. The file can be imported by the same SonicWall or used to clone a configuration across multiple SonicWall systems.



4. Click **Close**.

Configuring Firmware and Backup Settings

To configure firmware and backup settings:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**.
The **Settings** dialog is displayed.

The screenshot shows a settings dialog with the following elements:

- Navigation tabs: Firmware & Local Backups, Cloud Backups, **Settings**, One-Touch Configuration Overrides, FIPS / NDPP.
- Sub-tabs: **Scheduled Reports**, Diagnostics, Firmware Auto Update.
- Settings:
 - Send Tech Support Report by FTP:
 - Send Settings by FTP:
 - FTP Server:
 - User Name:
 - Password:
 - Directory:
- Buttons: Set Schedule, Cancel, OK.

Topics:

- [Send Settings or Reports by FTP](#)
- [Sending Diagnostic Reports to Technical Support](#)
- [Firmware Auto Update](#)
- [One-Touch Configuration Overrides](#)
- [Enabling FIPS Mode](#)
- [Enabling NDPP mode](#)

Send Settings or Reports by FTP

You can send configuration settings and/or tech support reports (TSRs, or detailed reports of security appliance configuration and status) to a specific FTP server on a one-time or scheduled basis. By scheduling when these reports are sent to the FTP server, you can create and manage schedule objects and enforce schedule times.

To send diagnostic reports to Technical Support:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**.

3. Click **Scheduled Reports**.

Settings

SCHEDULE REPORTS

Send Tech Support Report by FTP

Send Settings by FTP

FTP Server

User Name

Password

Directory

Set Schedule

4. To send TSRs by FTP, select the **Send Tech Support Report by FTP**. This option is not selected by default.
5. To send configuration settings by FTP, select **Send Settings by FTP**. This option is not selected by default.
6. When either or both of the Actions settings are selected, the server fields become available. Make changes as necessary.
 - a. Enter the server's IP address in the **FTP Server** field. The default is 0.0.0.0.
 - b. Enter the user name associated with the server in the **User Name** field.
 - c. Enter the password associated with the user name in the **Password** field.
 - d. Enter the directory where the reports are to be sent in the **Directory** field.
7. Click **Set Schedule**. The **Settings** dialog displays.

The Schedule Name is TSR Report Hours and cannot be changed.

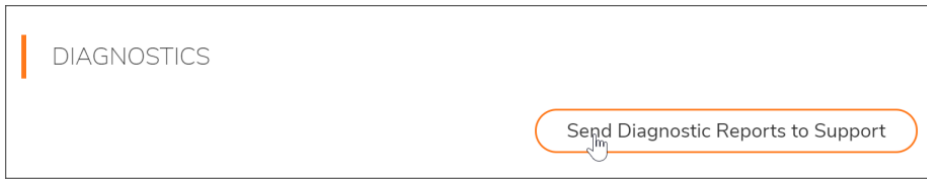
8. Configure the schedule. For how to configure a schedule, see [Scheduling Firmware Image Backups](#) section.
9. Click **Save**.

Sending Diagnostic Reports to Technical Support

To help determine system problems, you can send system diagnostics to SonicWall [Technical Support](#).

To send diagnostic reports to Technical Support:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**.
3. Click **DIAGNOSTICS**.
4. Click **Send Diagnostic Reports to Support**. This can take up to a minute. While sending the report, the status bar at the bottom of the screen displays:



5. Click **OK**.

Boot Settings

To Reviewers: Do we have this option? I don't see this option in Settings dialog..

To boot your SonicWall network security appliance with diagnostics enabled:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**. The Settings dialog displays.
3. Click **Boot with firmware diagnostics enabled** (if available). This option is not selected by default.
4. Click **Apply**.

One-Touch Configuration Overrides

① | **NOTE:** Be sure to export the configuration of your SonicWall security appliance before executing a configuration override, so the current configuration may be restored. Please refer to [Exporting Settings](#).

△ | **CAUTION:** Be aware that the **One-Touch Configuration Overrides** may change the behavior of your SonicWall security appliance. Review the list of configurations before applying **One-Touch Configuration Overrides**. In particular, these configurations may affect your experience:

- **Administrator password requirements on the Device | Settings page**
- **Requiring HTTPS management**
- **Disabling HTTP-to-HTTPS redirect**
- **Disabling Ping management**

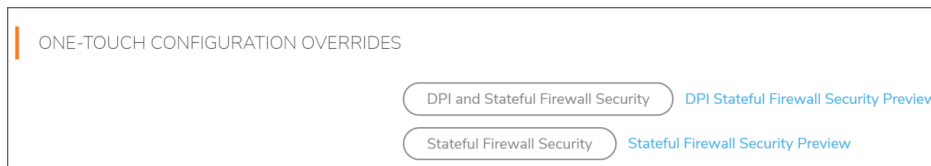
The One-Touch Configuration Overrides feature is configured on the Settings dialog available from the **Device | Settings > Firmware and Settings** page. It can be thought of as a quick tune-up for your SonicWall network security appliance's security settings. With a single click, One-Touch Configuration Overrides applies over sixty configuration settings to implement SonicWall's recommended best practices. These settings ensure that your appliance is taking advantage of SonicWall's security features.

To override the One-Touch Configuration settings:

① | **NOTE:** A system restart is required for the updates to take full effect.

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**. The Settings dialog is displayed.

3. Scroll to the ONE-TOUCH CONFIGURATION OVERRIDES section.



- **DPI and Stateful Firewall Security** - For network environments with Deep Packet Inspection (DPI) security services enabled, such as Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware, and App Rules.
- **Stateful Firewall Security** - For network environments that do not have DPI security services enabled, but still want to employ SonicWall's stateful firewall security best practices.

Both of the One-Touch Configuration Overrides deployments implement the following configurations:

- Configure Administrator security best practices
- Enforce HTTPS login and disables ping
- Configure DNS Rebinding
- Configure Access Rules best practices
- Configure Firewall Settings best practices
- Configure Firewall Flood Protection best practices
- Configure VPN Advanced settings best practices
- Configure Log levels
- Enable Flow Reporting and Visualization

The DPI and Stateful Firewall Security deployment also configures the following DPI-related configurations:

- Enable DPI services on all applicable zones
- Enable App Rules
- Configure Gateway Anti-Virus best practices
- Configure Intrusion Prevention best practices
- Configure Anti-Spyware best practices

To see exactly which settings are reconfigured, click on the Preview link next to each button. A page displays with a list of each setting and the value to which it will be set.

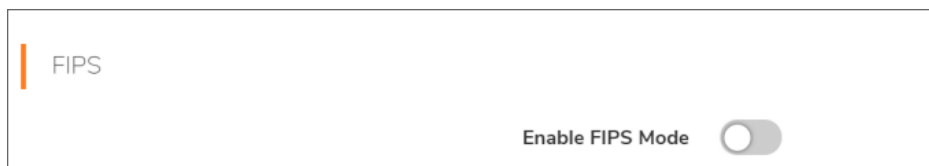
Enabling FIPS Mode

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWall security appliances support FIPS 140-2 Compliant security. Among the FIPS-compliant features of the son include PRNG-based on SHA-1 and support of only FIPS-approved algorithms (DES, 3DES, and AES with SHA-1).

To enable FIPs and see a list of which of your current configurations are not allowed or are not present:

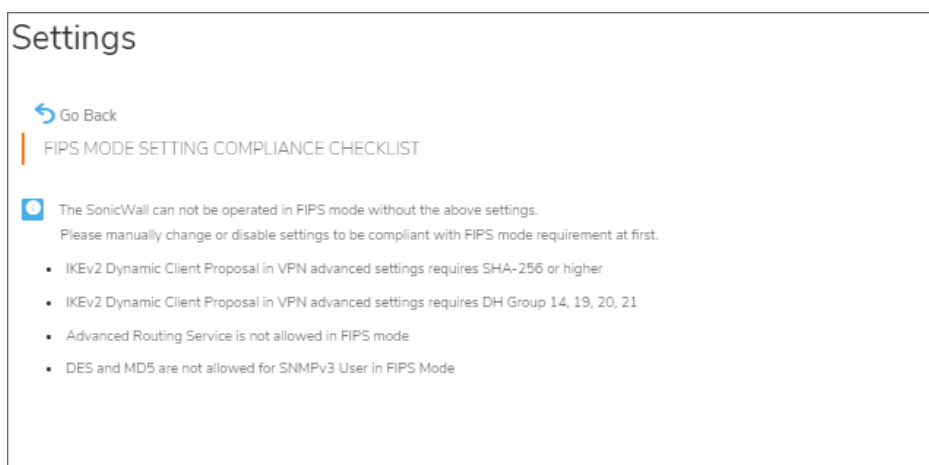
- ① **NOTE:** The Enable FIPS Mode option cannot be enabled at the same time as the Enable NDPP Mode option, which is also on the Firmware and Settings > Settings dialog.

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**.
3. Click **FIPS/NDPP**.
4. Enable the **Enable FIPS Mode** option.



5. Click **OK**.

The **FIPS Mode SETTING COMPLIANCE CHECKLIST** dialog appears with a list of your required and not allowed configurations.



6. If your SonicWall appliance:
 - Complies with the checklist, go to **Step 7**.
 - Does not comply with the checklist, manually change or disable settings to be compliant with FIPS mode setting compliance checklist.

① **TIP:** Leave the checklist dialog open while you make the configuration changes. If you click **OK** before all required changes are complete, the **Enable FIPS Mode checkbox** is cleared automatically upon closing the verification dialog. Select the checkbox again to see what configuration changes are still needed for FIPS compliance.

7. Click **OK** to reboot the security appliance in FIPS mode. A second warning displays.
8. Click **Yes** to continue rebooting. To return to normal operation, clear the **Enable FIPS Mode** checkbox and reboot the firewall in non-FIPS mode.

⚠ **CAUTION:** When using the SonicWall security appliance for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWall security appliance must remain in place and untouched.

Enabling NDPP mode

A SonicWall network security appliance can be enabled to be compliant with Network Device Protection Profile (NDPP), but certain security appliance configurations are either not allowed or are required.

① **NOTE:** NDPP is a part of Common Criteria (CC) certification. However, NDPP in SonicOS is not currently certified.

The security objectives for a device that claims compliance to a Protection Profile are defined as:

Compliant TOEs (Targets Of Evaluation) will provide security functionality that address threats to the TOE and implement policies that are imposed by law or regulation. The security functionality provided includes protected communications to and between elements of the TOE; administrative access to the TOE and its configuration capabilities; system monitoring for detection of security relevant events; control of resource availability; and the ability to verify the source of updates to the TOE.

When you enable NDPP, a popup message displays with the NDPP mode setting compliance checklist. The checklist displays every setting in your current SonicOS configuration that violates NDPP compliance so that you can change these settings. You need to navigate around the SonicOS management interface to make the changes. The checklist for an appliance with factory default settings is shown in the following procedure.

To enable NDPP and see a list of which of your current configurations are not allowed or are not present::

① **NOTE:** The Enable NDPP Mode option cannot be enabled at the same time as the Enable FIPS Mode option, which is also on the Firmware & Backups > Settings dialog.

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Settings**.
3. Click **FIPS / NDPP**.
4. Select **Enable NDPP Mode**.



The **NDPP MODE SETTING COMPLIANCE CHECKLIST** appears with a list of your required and not allowed configurations.

5. If your SonicWall appliance:
 - Complies with the checklist, go to **Step 6**.
 - Does not comply with the checklist, manually change or disable settings to be compliant with NDPP mode requirement.

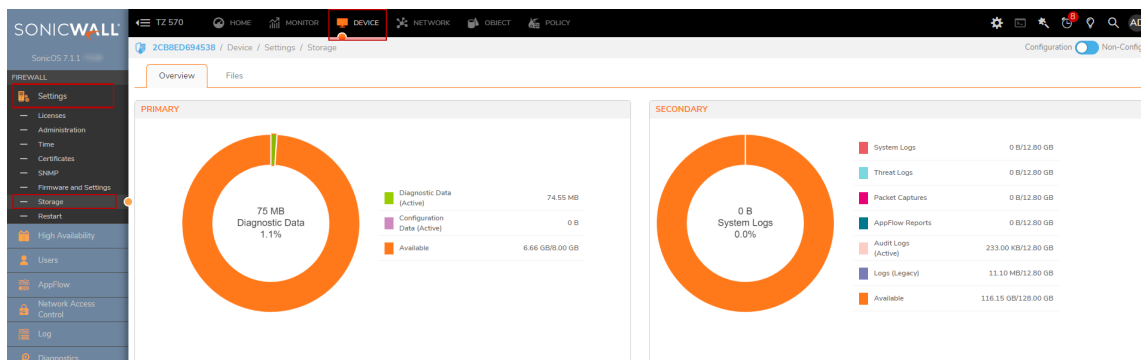
① **TIP:** Leave the checklist dialog open while you make the configuration changes. If you click **OK** before all required changes are complete, the **Enable NDPP Mode** option is cleared automatically upon closing the checklist dialog. Select the option again to see what configuration changes are still needed for NDPP compliance.

6. Click **OK**.

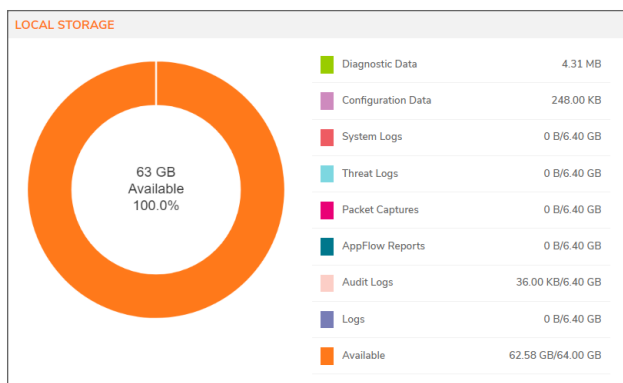
Storage

The **DEVICE | Settings > Storage > Overview** page displays information for your network security appliance about:

- Primary storage
- Secondary storage (if available for your network security appliance)
- Both Primary and Secondary storages are available in NSa 4700 series and higher, all NSsp and TZ series appliances.



- Local storage available only in NSv series appliances.



The advantages of Storage are:

- The Storage module stores diagnostic data, configuration backups, and logs from system logs, threat logs, Appflow Report data, and packet captures. Logs from 7.0.1 are preserved on the tab named **Logs (Legacy)**, but no new logs are added.
- Storage allows logs to persist when firewall is rebooted.
- The system logs, threat logs, and packet capture is allocated 10% of the total storage space each.
- The Appflow Report also gets 10% allocation.

Topics:

- [Storage Overview Tab](#)
- [Storage File Tab](#)

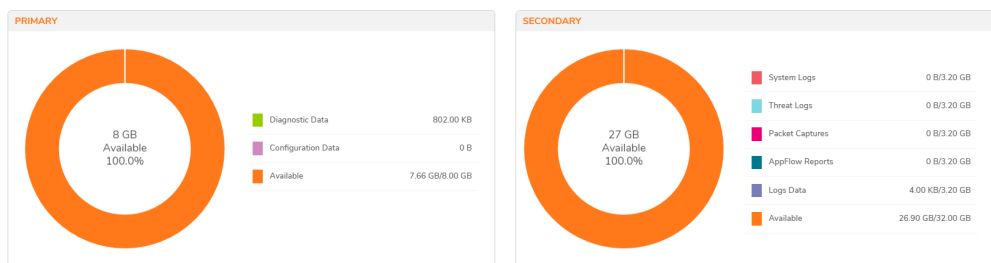
Storage Overview Tab

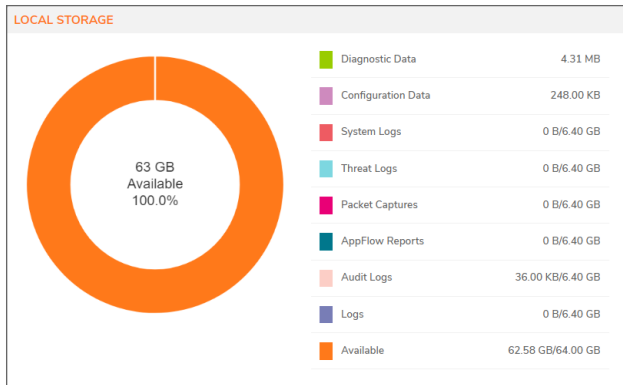
Only 4700 to 13700 modules allow selection of Primary or Secondary devices if the secondary device is available and valid. TZs, NSa 2700 and NSa 3700 only allows applications to write to secondary storage, primary storage is for System, diagnostic and configuration data only. For NSv, only one storage exists **Local Storage**, applications can write into this storage. You can change the storage option. It is required to reboot for the changing the storage device to take effect. Only **Packet capture** and **Logs (Legacy)** allows deletion of files. **System Logs**, **Threat Logs** and **Appflow Report** does not allow deletion of files.

Storage is disabled if your security appliance does not have any available storage modules.

Unlike Primary Storage, that is meant to be used by only one firewall, the Secondary Storage module is a shared device that can be used on multiple firewalls if successfully activated on each firewall. In the Secondary Storage module, a top-level directory is created with the firewall EPAID as the directory name. Applications create subdirectories inside this top-level directory and store their data there.

The **Overview** tab displays a pie chart representation of each storage module. It gives a high level representation of storage space used by each module and also the remaining available space. The log names in the chart are interactive-clicking on them redirects to specific storage tabs.







Each storage module is assigned with 10% of the total storage space.

Diagnostics Data

The **Diagnostic Data** tab displays diagnostics files stored on disk allowing users to download these files from this tab for further analysis.

To view and download diagnostics data:

1. Navigate to **Device | Settings > Storage > Files**.
2. Click on **Diagnostic Data** tab.
This page displays all the created files.
3. Hover on the file that you need to download and click on the **Download** icon .

| NAME | DATE LAST UPDATED | FILE SIZE | FILE LOCATION |
|-----------------|----------------------------|-----------|---|
| diagnostic_data | December 6, 2023 2:51 PM | 50.72 KB | Primary  |
| diagnostic_data | December 5, 2023 10:48 AM | 2.66 MB | Primary |
| diagnostic_data | September 25, 2023 7:41 PM | 3.15 MB | Primary |
| diagnostic_data | December 6, 2023 2:02 PM | 198 B | Primary |
| diagnostic_data | December 6, 2023 2:02 PM | 3.31 KB | Primary |
| diagnostic_data | December 6, 2023 2:01 PM | 354 B | Primary |
| diagnostic_data | December 6, 2023 2:02 PM | 475.54 KB | Primary |
| diagnostic_data | December 6, 2023 2:45 PM | 16.61 KB | Primary |
| diagnostic_data | December 6, 2023 2:45 PM | 4.65 MB | Primary |
| diagnostic_data | April 21, 2023 5:29 AM | 794.53 KB | Primary |
| diagnostic_data | December 5, 2023 12:56 PM | 783.45 KB | Primary |
| diagnostic_data | December 5, 2023 1:32 PM | 19.52 KB | Primary |
| diagnostic_data | December 5, 2023 1:32 PM | 217.97 KB | Primary |
| diagnostic_data | December 5, 2023 1:35 PM | 22.03 KB | Primary |
| diagnostic_data | December 6, 2023 2:02 PM | 172.60 KB | Primary |
| diagnostic_data | December 6, 2023 2:02 PM | 234.17 KB | Primary |



















 | **NOTE:** The file downloaded are encrypted so use **decryptor** to view the contents.

Configuration Backup







The **Configuration Backup** tab lists firewall configuration files. This tab allows the administrators the ability to perform various operations similar to those available on the **Device > Firmware > Settings** page.

To create backup:

1. Navigate to **Device | Settings > Storage > Files**
2. Click on **Configuration Backup** tab.

| # | FIRMWARE VERSION | CONFIGURATION DATE | FIRMWARE LOAD DATE | USERNAME | COMMENTS | BACKUP TYPE | ACTIONS |
|---|---|---------------------|--------------------|----------|------------------------------------|-------------|---|
| 1 | Backup created with version SonicOS 7.1.1-7019-DB676 (1 Configuration Files available) Local backup 7 | | | admin | This is a backup on Local Storage. | |       |
| 2 | Backup created with version SonicOS 7.1.1-7011-D6661 (1 Configuration Files available) Local backup 6 | 07/20/2023 14:54:53 | | admin | This is a backup on Local Storage. | |       |
| 3 | Backup created with version SonicOS 7.1.1-7006-D6314 (1 Configuration Files available) Local backup 5 | | | admin | This is a backup on Local Storage. | |       |

3. Expand the required firmware version and you can do the following:

| Icon | Definition |
|---|--|
|  | This icon helps to retain the selected configuration file so that it is not overwritten during auto or local backup. |
|  | This icon helps to make the selected configuration file as Gold Master. |
|  | This icon helps to boot the firmware with selected configuration file. |
|  | This icon helps to download the selected configuration file. |
|  | This icon helps to add/edit a comment to the selected configuration file. |
|  | This icon helps to delete the selected configuration file. |

4. Click on **Create Backup**.
5. Enable or disable the **Retain Local Backup** option as per your requirement.
6. Add comment to the **Comment** text box.
7. Click **OK**.

Local Backup

Creating a local backup. To proceed, click "OK".

Retain Local Backup

Comments

Cancel

OK

NOTE: The backup created is stored in Primary storage only and cannot be changed.

System Logs

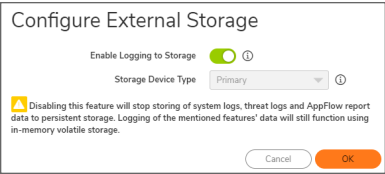
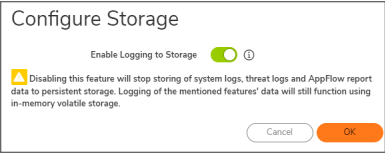
The **System Logs** tab displays the files containing system log events, allowing to export them in CSV format or download as an SQLite database file. To manage storage capacity, older files are rotated out when the disk is nearing full, ensuring space for new log entries. You can review system log events on the **Monitor > Logs > System Logs** page.

To store System Logs to External Storage:

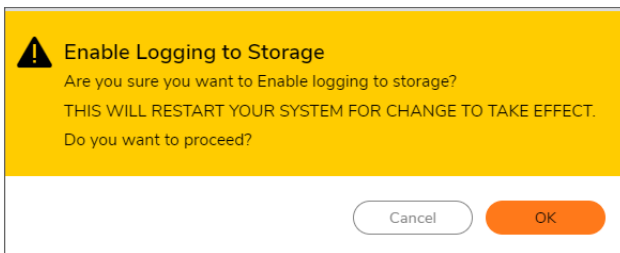
1. Navigate to **DEVICE | Settings > Storage > Files**.
2. Click on **System Logs** tab.

| NAME | START TIME | END TIME | NUMBER OF LOGS | FILE LOCATION | ACTION |
|----------------------------------|---------------------------|---------------------------|----------------|---------------|--------|
| systemlogs_1696979458_1696985228 | October 11, 2023 4:40 AM | October 11, 2023 6:17 AM | 12500 | Primary | ↓ |
| systemlogs_1696985230_1697002636 | October 11, 2023 6:17 AM | October 11, 2023 11:07 AM | 12500 | Primary | ↓ |
| systemlogs_1697002636_1697024677 | October 11, 2023 11:07 AM | October 11, 2023 5:14 PM | 12500 | Primary | ↓ |
| systemlogs_1697024677_1697034573 | October 11, 2023 5:14 PM | October 11, 2023 7:59 PM | 12500 | Primary | ↓ |
| systemlogs_1697034573_1697046294 | October 11, 2023 7:59 PM | October 11, 2023 11:14 PM | 12500 | Primary | ↓ |
| systemlogs_1697046294_1697067322 | October 11, 2023 11:14 PM | October 12, 2023 5:05 AM | 12500 | Primary | ↓ |
| systemlogs_1697067322_1697082229 | October 12, 2023 5:05 AM | October 12, 2023 9:13 AM | 12500 | Primary | ↓ |
| systemlogs_1697082229_1697091631 | October 12, 2023 9:13 AM | October 12, 2023 11:50 AM | 12500 | Primary | ↓ |
| systemlogs_1697091631_1697099706 | October 12, 2023 11:50 AM | October 12, 2023 2:05 PM | 12500 | Primary | ↓ |
| systemlogs_1697099706_1697108059 | October 12, 2023 2:05 PM | October 12, 2023 4:24 PM | 12500 | Primary | ↓ |
| systemlogs_1697108059_1697127117 | October 12, 2023 4:24 PM | October 12, 2023 9:41 PM | 12500 | Primary | ↓ |

3. Click on **Settings** tab.

| Screen | Description |
|---|--|
|  | <p>For NSa 4700 series and higher and all NSsp series appliances:</p> <ul style="list-style-type: none">• Enable the Enable Logging to Storage for storing system logs, threat logs, audit logs, and AppFlow report data.• Select Primary or Secondary from the Storage Device Type drop-down. <p>NOTE: Requires a reboot for the changing the storage device to take effect. The Firewall displays files and data only from the active storage.</p> |
|  | <p>For TZ and NSvseries appliances:</p> <ul style="list-style-type: none">• Enable the Enable Logging to Storage for storing system logs, threat logs, audit logs, and AppFlow report data. |

NOTE: Enabling **Enable Logging to Storage** requires a reboot for the changes to take effect.




4. Click **OK**.

Threat Logs

The **Threat Logs** tab displays files containing app flow sessions marked with threats, viruses, instructions, spyware, and botnet activities. You can export these files in CSV format or download them as SQLite database files. To manage storage capacity, older files are rotated out when the disk is nearing full, ensuring space for new log entries. You can review the threat logs in **Monitor > Logs > Threat Logs** page.

To export the threat logs:

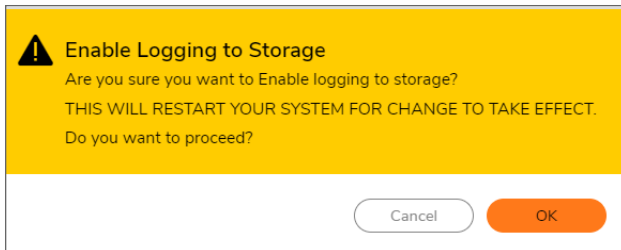
1. Navigate to **DEVICE | Settings > Storage > Files**.
2. Click the **Threat Logs** tab.
3. Click the **Download** icon  beside the selected threat log.
4. Select **Export to CSV** or **Download File**.

| NAME | START TIME | END TIME | NUMBER OF LOGS | FILE LOCATION | ACTION |
|----------------------------------|---------------------------|---------------------------|----------------|---------------|--------------------------------|
| threatlogs_1668111340_1668173486 | November 11, 2022 1:45 AM | November 11, 2022 7:01 PM | 12500 | Primary | Export to CSV Download File |
| threatlogs_1668173507_1668263482 | November 11, 2022 7:01 PM | November 12, 2022 8:01 PM | 12500 | Primary | |
| threatlogs_1668263468_1668349686 | November 12, 2022 8:01 PM | November 13, 2022 7:58 PM | 12500 | Primary | |
| threatlogs_1668349689_1668415625 | November 13, 2022 7:58 PM | November 14, 2022 2:17 PM | 12500 | Primary | |
| threatlogs_1668415628_1668462739 | November 14, 2022 2:17 PM | November 15, 2022 3:22 AM | 12500 | Primary | |
| threatlogs_1668462739_1668545292 | November 15, 2022 3:22 AM | November 16, 2022 2:18 AM | 12500 | Primary | |
| threatlogs_1668545301_1668584107 | November 16, 2022 2:18 AM | November 16, 2022 1:05 PM | 12500 | Primary | |

5. Click on **Settings** tab.

| Screen | Description |
|--------|---|
| | <p>For NSA 4700 series and higher and all NSsp series appliances:</p> <ul style="list-style-type: none"> Enable the Enable Logging to Storage for storing system logs, threat logs, audit logs, and AppFlow report data. Select Primary or Secondary from the Storage Device Type drop-down. <p>NOTE: Requires a reboot for the changing the storage device to take effect. The Firewall displays files and data only from the active storage.</p> |
| | <p>For TZ and NSvseries appliances:</p> <ul style="list-style-type: none"> Enable the Enable Logging to Storage for storing system logs, threat logs, audit logs, and AppFlow report data. |

NOTE: Enabling **Enable Logging to Storage** requires a reboot for the changes to take effect.



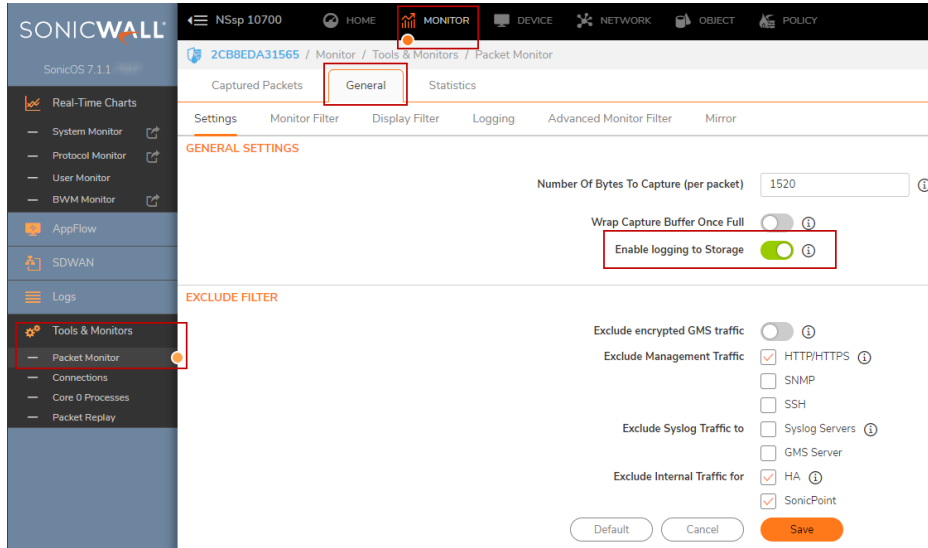
6. Click **OK**.

Packet Captures

The **Packet Capture** tab displays recorded packet files, exportable in PCAPNG format. As storage nears capacity, older files are rotated to accommodate new files. These files become available when packet capturing is activated, that is when the **Enable logging to Storage** option is enabled in **Monitor > Packet Monitor** settings page. The setting ensures the capture buffer is being utilized, triggering availability once it is full.

To enable packet capturing:

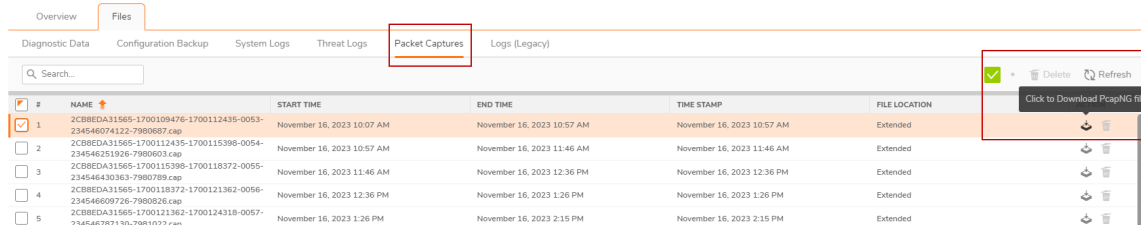
1. Navigate to **Monitor | Tools & Monitors > Packet Monitor > General**.
2. Enable the **Enable logging to Storage**.



3. Click **Save**.

To download, export and/or delete packet capture files from Storage:

1. Navigate to **DEVICE | Settings > Storage > Files**.
2. Click the **Packet Captures** tab.



3. Hover on the file to view the options.

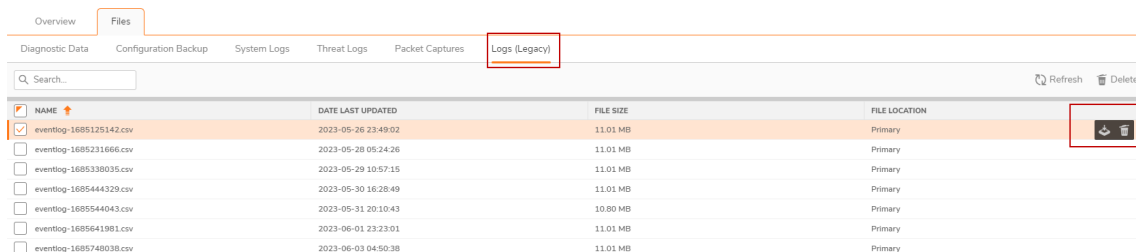
| Icon | Definition |
|------|--|
| | This icon helps to download the selected file. |
| | This icon helps to delete the selected file. |

Logs (Legacy)

The **Logs (Legacy)** displays a list of stored event log files collected from a previous SonicOS version, retained for historical purposes. You can export or delete each file as needed.

To export or delete the logs:

1. Navigate to **Device | Settings > Storage > Files**
2. Click on **Logs (Legacy)** tab.



| <input checked="" type="checkbox"/> | NAME | DATE LAST UPDATED | FILE SIZE | FILE LOCATION |
|-------------------------------------|-------------------------|---------------------|-----------|---------------|
| <input checked="" type="checkbox"/> | eventlog-1685125142.csv | 2023-05-26 23:49:02 | 11.01 MB | Primary |
| <input type="checkbox"/> | eventlog-1685231666.csv | 2023-05-28 05:24:26 | 11.01 MB | Primary |
| <input type="checkbox"/> | eventlog-1685330035.csv | 2023-05-29 10:57:15 | 11.01 MB | Primary |
| <input type="checkbox"/> | eventlog-1685444329.csv | 2023-05-30 16:28:49 | 11.01 MB | Primary |
| <input type="checkbox"/> | eventlog-1685544043.csv | 2023-05-31 20:10:43 | 10.80 MB | Primary |
| <input type="checkbox"/> | eventlog-1685641981.csv | 2023-06-01 23:23:01 | 11.01 MB | Primary |
| <input type="checkbox"/> | eventlog-1685748038.csv | 2023-06-03 04:50:38 | 11.01 MB | Primary |

3. Hover on the log file to view the options.

Icon Definition



This icon helps to download (export) the selected file.



This icon helps to delete the selected file.

Restarting the System

To restart the firewall:

 **CAUTION:** The restarting process takes few minutes. During the restart time, all users are disconnected. If you made any changes to the settings, apply them before you restart.

1. Navigate to **Device | Settings > Restart**.
2. Click the **Restart SonicOS** button.

SonicWall Support

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

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 and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services at <https://sonicwall.com/pes>.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

About This Document

SonicOS Device Settings Administration Guide
Updated - December 2023
Software Version - 7.1
232-005346-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall 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 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. 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/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. 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
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035