



# Migration Tool 4.35.3

Migration Tool User Guide

SONICWALL®

# Contents

<b>About the Guide</b> .....	<b>3</b>
Guide Conventions .....	3
<b>Supported Platforms</b> .....	<b>4</b>
<b>Knowledge Base Articles for Migrating</b> .....	<b>5</b>
<b>Using Migration Tool</b> .....	<b>6</b>
Exporting a Copy of your Current Configuration Settings .....	6
Starting your Firewall Migration .....	6
Uploading Configuration .....	7
Choosing Target Product .....	9
Assigning Interfaces .....	10
Downloading New Configuration Settings .....	11
<b>Importing Configuration Settings</b> .....	<b>13</b>
<b>SonicWall Support</b> .....	<b>14</b>
About This Document .....	15

# About the Guide

This User Guide provides instructions for users to use Migration Tool to migrate settings from an existing configuration of your SonicWall Product Series systems, enabling the creation of a new settings file that can be imported onto the target SonicWall Product Series systems.

This User Guide also provides information about importing new configuration settings to an appliance running latest versions. See [Supported Platforms](#) and [Knowledge Base Articles for Migrating](#) for details about the supporting models, firmware versions supported, and [Importing Configuration Settings](#) for steps to import the setting file.

## Topics:

- [Supported Platforms](#)
- [Knowledge Base Articles for Migrating](#)
- [Using Migration Tool](#)
- [Importing Configuration Settings](#)
- [SonicWall Support](#)

## Guide Conventions

The conventions used in this guide are as follows:

### GUIDE CONVENTIONS

Convention	Use
<b>Bold</b>	Highlights dialog box, window, and screen names. Also highlights buttons. Also used for file names and text or values you are being instructed to type into the interface.
<i>Italic</i>	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence. Sometimes indicates the first instance of a significant term or concept.

# Supported Platforms

The following are the supported platforms and versions.

PLATFORM	VERSIONS
SonicWall	GEN5: SOHO, SOHOW
	GEN6: TZ, NSA, SuperMassive, NSsp, NSv Series

① **NOTE:**

1. When migrating from SonicWall Gen6 Firewall to Gen7 Firewall, use the latest release of SonicOS 7 available on the MySonicWall Portal.
2. All physical-to-physical SonicWall product Series device migration supports according to the support matrix, refer to [Export/Import Support Matrix](#), excepts NSsp 15700 device since it runs on Policy Mode.
3. SonicWall Gen5 Firewall to Gen7 Firewall migration is only supported for SOHO devices.
4. Certificates and Licenses migration is not supported.
5. Migration Tool doesn't support SonicOS 7.1.1 release. Choose SonicOS 7.0.1-5145 firmware version as the target version of the migrated file in the Migration Tool and then upgrade to 7.1.1. For more information refer to KB article, [Migration Tool doesn't support target firmware of SonicOS 7.1.1](#).

# Knowledge Base Articles for Migrating

① **IMPORTANT:** Be sure to review the following Knowledge Base articles before upgrading your devices.

1. [Can Settings be Exported/Imported from one SonicWall to Another? \(Support Matrix\)](#)
2. [How to Create Gen 7 Settings File by Using the Online Migration Tool](#)
3. [Migration Tool doesn't support target firmware of SonicOS 7.1.1](#)

# Using Migration Tool

SonicWall created the Migration Tool version 4.35.3 to help users migrate configuration settings from an existing firewall, enabling the creation of a new settings file that can easily be imported into a new firewall.

## Topics:

- [Exporting a Copy of your Current Configuration Settings](#)
- [Starting your Firewall Migration](#)
- [Uploading Configuration](#)
- [Choosing Target Product](#)
- [Assigning Interfaces](#)
- [Downloading New Configuration Settings](#)

## Exporting a Copy of your Current Configuration Settings

Before beginning the migration process, export a copy of your SonicWall Product Series systems configuration settings to your local machine. The export configuration option saves a copy of the current configuration settings, protecting all your existing settings if it becomes necessary to return to a previous configuration state.

For example: The default settings file is named sonicwall-TZ 570--xxxx-xx-xxxxx\_xx\_xx.xxxZ.exp (where TZ 570--xxxx-xx-xxxxx\_xx\_xx.xxx is the time of the export from the appliance).

## Starting your Firewall Migration

Ensure the supported platforms and versions before starting your firewall migration via SonicWall Migration Tool.

**SONICWALL** Migration Tool v4.3.3

1 START 2 UPLOAD 3 TARGET 4 INTERFACES 5 EXPORT

**Start**  
**Start Your Firewall Migration**  
 Welcome to the SonicWall Settings Converter site.

**Supported Platforms**

PLATFORM	VERSIONS
Check Point	Smart Center, Provider-1 (excluding VPN-1 Edge, Safe@Office, SMP) with OS NG FP1 (4.0)
Cisco PIX/ASA	PIX 4.x, PIX 5.x, PIX 6.x, PIX 7.x, PIX 8.x
Fortinet	FortiGate Firewall Platform
Juniper	NetScreen Series, SRX Series, SSG Series
Palo Alto	PA-200, PA-500, PA-2000, PA-3000, PA-4000, PA-5000 Series
SonicWall	TZ, NSA, SuperMassive, NSsp, NSv
Sophos	SG, XG Series
Watchguard	FireBox, XTM Series

Previous Next

Settings can be exported from one firewall to another, but not every SonicWall model is compatible with all others. Similarly, some firmware versions are not compatible with subsequent versions as new features were added or changes were made to existing features. Refer to [Supported Platforms](#) and [Importing Configuration Settings](#) sections to help avoid possible settings corruption from unsupported settings imports.

## Uploading Configuration

The following are the steps to identify and upload your current Firewall configuration.

1. Based on your firewall, select the product as **SonicWall** or any of your source product to migrating from the **Select Product** drop-down menu.
2. On **Select Configuration**, click **Browse...** and select your settings file from your local machine. Refer to [Exporting a Copy of your Current Configuration Settings](#).
3. On **Select Configuration**, click **Upload** for uploading your settings file and ensure the file is found by the tool.

4. Click **Next**.

START 2 UPLOAD 3 TARGET 4 INTERFACES 5 EXPORT

### Upload Configuration

**Identify and Upload your Current Firewall Configuration**

Based on your firewall vendor, select the product you are migrating from the drop-down menu and upload the configuration file.

Demo Mode

Select Product SonicWall

Select Configuration Browse... Upload

1 firewall(s) found.  
sonicwall-TZ 570-...Z.exp

**NOTE**

1. Use the latest release of SonicOS7 which is available on MySonicWall portal when migrating from Gen6.
2. All physical to physical migrations are supported except from NSsp15/700 since that runs Policy Mode.
3. All physical to NSv Global/Classic Mode is supported.
4. NSv global model to physical models is supported
5. Support for Policy Mode migration is not supported now.
6. NSv Global mode to Policy Mode migration is not supported via migration tool. User can switch from global mode to policy mode from the firewall UI itself and some settings will be migrated like Address Objects/Groups, Service Objects/Groups, NAT policy, Route policy.
7. Certificates and Licenses will not be migrated

Previous Next



- For Demo Mode, select the check box **Demo Mode** and follow steps 1 to 4 again.

**Upload Configuration [Demo Mode]**

**Identify and Upload your Current Firewall Configuration**

Based on your firewall vendor, select the product you are migrating from the drop-down menu and upload the configuration file.

Demo Mode

Select Product -- Select Source Product --

Select Configuration

Source Product  
Configuration File  
Target Product

**NOTE**

1. Use the latest release of SonicOS7 which is available on MySonicWall portal when migrating from Gen6.
2. All physical to physical migrations are supported except from NSsp15700 since that runs Policy Mode.
3. All physical to NSv Global/Classic Mode is supported.
4. NSv global model to physical models is supported
5. Support for Policy Mode migration is not supported now.
6. NSv Global mode to Policy Mode migration is not supported via migration tool. User can switch from global mode to policy mode from the firewall UI itself and some settings will be migrated like Address Objects/Groups, Service Objects/Groups, NAT policy, Route policy.
7. Certificates and Licenses will not be migrated

## Choosing Target Product

Select a SonicWall firewall model you want to configure and apply the existing policies and rules. The following are the steps to identify which target firewall product or SonicWall firewall for deploying.

- Choose the target product from the **Select Target Product** list.
  - NOTE:** select the check box **Show All devices** will show you all the list of target product.
- The following warnings helps you to select the product based on your requirement.
  - FULL** - – selected product can be migrated fully.
  - PARTIAL** - – The partial migration represents that there are limitations, some of the settings may get dropped/ignored due to the interface limitation.
  - NOT** - – selected product not supported for migration.
- Make sure the summary of Source Product, Configuration File, Target Product and click **More info** to get information on the uploaded configuration supported devices list.

4. Make sure the Selected Product, Product description, and Specification, click **More specs** for more information on the specification and about selected product.
5. Click **Next**.

**Choose Target**

Identify Which SonicWall Firewall You Are Deploying

Select a SonicWall firewall model you want to configure and apply existing policies and rules.

The uploaded configuration can only be migrated to some of the devices listed below [\[More info\]](#)

**SELECT TARGET PRODUCT**

SEARCH

Show All devices

- TZ 400 Wireless
- TZ 470
- TZ 470W
- TZ 500
- TZ 500 Wireless
- TZ 570**
- TZ 570W
- TZ 570P
- TZ 600
- TZ 600P
- TZ 670

FULL -  PARTIAL -  NOT -

**SELECTED PRODUCT**

**TZ 570**

The SonicWall Network Security Appliance TZ 570 Series high-performance Next-Generation Firewalls offer branch offices and distributed enterprises in-depth frontline security, application and user control, network productivity and optional 802.11 dual-band wireless. The TZ 570 integrates dual-core hardware, SonicWall Reassembly-Free Deep Packet Inspection, application control, intrusion prevention, and SSL VPN for real-time protection without compromising performance.

**Interfaces**

10/100 Ethernet:	-
10/100/1000 Ethernet:	10
Console Interface:	1
USB Port:	2

[More Specs](#)

Home Previous Next

## Assigning Interfaces

Assigning current interfaces to the target firewall. The following are the steps to map your existing interfaces to the preferred interfaces.

1. Select the interfaces from **Interface** drop-down menu to map the interfaces to target device.
  - ① | **NOTE:** For multiple firewalls, select the firewall you are migrating from drop-down menu.
2. Click **1 To 1 Mapping**, if user want to use same interfaces to the target firewall.
  - ① | **NOTE:** It is recommended to use **1 To 1 Mapping** under assigned interfaces.

3. Click **Next**.

**Assign Interfaces**

**Assign Current Interfaces to Your New Firewall**

1. For multiple firewalls, select the firewall you are migrating from drop-down menu  
2. To map an interface to a target device, select a value in the dropdown under interface column

Source Product: SonicWall  
Configuration File: sonicwall-TZ 570-Soi  
Target Product: TZ 570

ZONE	NAME	IP	NETMASK	VLANS	INTERFACE
LAN	X0	192.168.168.168	255.255.255.0		X0
WAN	X1	10.203.28.159	255.255.255.0		Select
	X2	0.0.0.0	0.0.0.0		X0
	X3	0.0.0.0	0.0.0.0		X2
	X4	0.0.0.0	0.0.0.0		X3
	X5	0.0.0.0	0.0.0.0		X4
	X6	0.0.0.0	0.0.0.0		X5

Total interfaces found: 11

Clear All 1 To 1 Mapping

Home Previous Next

① | **NOTE:** Any unmapped interfaces will be dropped.

## Downloading New Configuration Settings

Select configuration to download by choosing the target version. The following are the steps to select the target version.

1. Select the target version for the new settings file from **Version** drop-down menu, under **Target** section.  
① | **NOTE:** Settings from a higher firmware version cannot be imported into a lower version of firmware.
2. Under **Advanced** section, select the following features.
  - a. By default **HA** feature will be selected.
  - b. Select the **Drop default access rules from source device** to only migrate custom access rule from source exp file.
  - c. Select the **Drop Certificate related configuration** to only migrate certificate related configuration from source exp file
  - d. Select the **Drop default Nat policy from source device** to only migrate Nat policy from source exp file.

3. Click **Finish**. The migrated new settings file will be downloaded to your local machine.
- ① **NOTE:** A pop-up notification appears if the configuration file successfully converted and ready to be imported into your target firewall.

START    UPLOAD    TARGET    INTERFACES    EXPORT

### Export The Settings [Demo Mode]

**Select Configuration to Export**

Select the target version, then click on **Finish** to download the migrated settings file.

<b>Source Product</b>	SonicWall
<b>Configuration File</b>	Demo Config 1
<b>Target Product</b>	TZ 270W

**Note:** Settings migrated to target firmware.

**Successfully converted**  
The config file is now ready to be imported into your SonicWall Firewall using the chosen format

**TARGET**

Version: 7.0.1-5145

---

**ADVANCED**

Feature

- HA
- Drop Certificate related config
- Drop default access rules from source device
- Drop default NAT policy from source device

Home    Previous    Finish

# Importing Configuration Settings

You can import configuration settings from one firewall to another firewall, which can save a lot of time when replacing an older firewall with a newer model. This feature is also useful when you need multiple appliances with similar configuration settings. The following are the steps to import your new configuration settings

1. Register the Target Firewall, download the latest firmware version and upgrade the firmware to the latest firmware version.  
① **NOTE:** It is recommended to factory default the Target Firewall before importing the configuration file (not required if the device is out of the box).
2. Upload the newly created settings file into your Target Firewall.  
For example: For SonicOS devices, navigate to **Device > Settings > Firmware and settings**, select **Import Configuration** to import configuration.
3. Click **Import**.

# 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

Migration Tool Migration Tool User Guide

Updated - January 2024

Software Version - 4.35.3

232-006033-00 Rev E

Copyright © 2024 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