SonicWall® Web Application
Firewall 2.0
MS Azure Deployment Guide
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>4</td>
</tr>
<tr>
<td>Supported Azure Platforms</td>
<td>4</td>
</tr>
<tr>
<td>WAF Virtual Appliance Requirements</td>
<td>4</td>
</tr>
<tr>
<td>Internet Access Requirements</td>
<td>5</td>
</tr>
<tr>
<td>Creating a MySonicWall Account</td>
<td>5</td>
</tr>
<tr>
<td>Installing the WAF Virtual Appliance</td>
<td>7</td>
</tr>
<tr>
<td>Installing SonicWall WAF</td>
<td>7</td>
</tr>
<tr>
<td>Configuring the WAF Virtual Appliance</td>
<td>15</td>
</tr>
<tr>
<td>Viewing the WAF Virtual Appliance Settings</td>
<td>15</td>
</tr>
<tr>
<td>Powering the Virtual Appliance On or Off</td>
<td>16</td>
</tr>
<tr>
<td>Connecting to the Web Interface</td>
<td>17</td>
</tr>
<tr>
<td>Connecting to the Command Line Interface</td>
<td>18</td>
</tr>
<tr>
<td>Using the Command Line Interface</td>
<td>19</td>
</tr>
<tr>
<td>Show Network Info</td>
<td>19</td>
</tr>
<tr>
<td>Reboot</td>
<td>19</td>
</tr>
<tr>
<td>Restart WAF Services</td>
<td>20</td>
</tr>
<tr>
<td>Save TSR to Disk</td>
<td>20</td>
</tr>
<tr>
<td>Display EUPA</td>
<td>20</td>
</tr>
<tr>
<td>Logout</td>
<td>20</td>
</tr>
<tr>
<td>Registering Your WAF Virtual Appliance</td>
<td>21</td>
</tr>
<tr>
<td>About WAF Licensing</td>
<td>21</td>
</tr>
<tr>
<td>Registering WAF</td>
<td>21</td>
</tr>
<tr>
<td>Using the 30-day Trial Version</td>
<td>22</td>
</tr>
<tr>
<td>Deployment Considerations</td>
<td>22</td>
</tr>
<tr>
<td>Registering the 30-day Trial Virtual Appliance</td>
<td>22</td>
</tr>
<tr>
<td>Upgrading Your WAF Virtual Appliance</td>
<td>24</td>
</tr>
<tr>
<td>Exporting a Copy of Your Configuration Settings</td>
<td>24</td>
</tr>
<tr>
<td>Backing up Settings Automatically</td>
<td>24</td>
</tr>
<tr>
<td>Automatic Software Downloads</td>
<td>25</td>
</tr>
<tr>
<td>Uploading a New WAF Image Manually</td>
<td>26</td>
</tr>
<tr>
<td>SonicWall Support</td>
<td>27</td>
</tr>
<tr>
<td>About This Document</td>
<td>28</td>
</tr>
</tbody>
</table>
Welcome to the SonicWall® Web Application Firewall MS Azure Deployment Guide. This Deployment Guide contains installation procedures and configuration guidelines for deploying the SonicWall Web Application Firewall (WAF) in your MS Azure cloud network.

SonicWall WAF provides the following benefits:

- **Security**
  - WAF enforces a defense-in-depth strategy to protect a suite of backend web applications, thereby significantly reducing the development cost and effort involved in protecting individual web applications.
  - WAF provides an optimized, non-tamperable architecture.
- **Scalability and Redundancy**
  - Multiple virtual machines can be deployed as a single system, enabling specialization, scalability, and redundancy.
- **Operational Ease**
  - You can virtualize your entire environment and deploy multiple machines within a single server or across multiple servers.
- **Product Versatility**
  - WAF is compatible with other SonicWall platforms as a stand-alone (All-in-One) unit.

The award-winning SonicWall Web Application Firewall service enforces defense-in-depth strategy to protect your web applications running in Azure from most common threats using a high performance real-time intrusion scanning engine. It offers businesses a complete, affordable, out-of-box compliance solution for web applications that is easy to manage and deploy.

WAF supports OWASP Top Ten and PCI DSS compliance, providing protection against malicious injection and cross-site scripting attacks, credit card and Social Security Number theft, cookie tampering and cross-site request forgery. Dynamic signature updates and Application Profiling that leverages an active learning algorithm protect against known and zero-day vulnerabilities. Virtual Patching using Custom Rules allows customers to instantly address a vulnerability and avoid attacks that happen while waiting for a security hotfix. SonicWall WAF supports IP Reputation services and Rate Limiting features to block automated and brute-force attacks. Stacked authentication including 2-factor authentication, one-time passwords and SSL client certificate authentication combined with access policies provides granular access control to the web applications.

**Highlights:**

- Secures web applications against advanced web attacks including OWASP Top Ten
- Layer 7 Load Balancing and Health Monitoring features provides accelerated application delivery and high availability of your applications
- Geo-IP based visualization and policies help block potential attacks from high risk locations or countries
- Denial of service (DoS) protection, Rate Limiting and Botnet protection with Remediation blocks automated brute-force attacks
- Includes advanced statistics and reporting options for compliance
Before You Begin

This section specifies the supported MS Azure instances, computing requirements for the installation, and information about MySonicWall.

Topics:
- Supported Azure Platforms on page 4
- WAF Virtual Appliance Requirements on page 4
- Internet Access Requirements on page 5
- Creating a MySonicWall Account on page 5

Supported Azure Platforms

The elements of basic MS Azure infrastructure must be implemented prior to deploying SonicWall WAF.

WAF Virtual Appliance Requirements

Based on the WAF model you have purchased and the appropriate WAF tier license key that you have received, use the WAF Sizing Information table to size your WAF deployment.

WAF Sizing Information

<table>
<thead>
<tr>
<th>Component</th>
<th>WAF 200</th>
<th>WAF 400</th>
<th>WAF 800</th>
<th>WAF 1600</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAF Tier</td>
<td>Tier 1</td>
<td>Tier 2</td>
<td>Tier 3</td>
<td>Tier 4</td>
</tr>
<tr>
<td>Required Compute Units</td>
<td>2-6</td>
<td>7-12</td>
<td>13-24</td>
<td>25-48</td>
</tr>
<tr>
<td>Recommended vCPUs</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Recommended Memory</td>
<td>4 GB</td>
<td>8 GB</td>
<td>16 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Recommended Storage</td>
<td>8 GB</td>
<td>8 GB</td>
<td>8 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Recommended AWS Instance</td>
<td>c5.large</td>
<td>c5.xlarge</td>
<td>c5.2xlarge</td>
<td>c5.4xlarge</td>
</tr>
<tr>
<td>Requires Access to Internet</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

NOTE: The number of vCPUs is an estimation based on the required Compute Units delivered by each vCPU in a typical enterprise-grade server system. This might differ based on the underlying hardware processor on the server – e.g. a vCPU derived from a server with a 4-core processor would deliver a different compute unit than if it were derived from a server with an 8-core processor. There are a number of different factors that impact the compute units and deriving it from a processor specification is not trivial.
To help you determine if you have the right sizing for your WAF virtual appliance, SonicWall WAF automatically calculates the minimum WAF Tier that has to be licensed on the virtual appliance based on allocated resources every time it is booted up.

**License Requirements on System > Licenses Page**

If the WAF Tier does not match the Tier associated with the WAF model purchased, you should either scale up or scale down the number of vCPUs allocated to meet the compute unit requirements. If this is not done, when the license key for the WAF service is applied during initial setup, it will be deemed invalid.

**Internet Access Requirements**

Internet access is required for communication between the SonicWall WAF appliance and the SonicWall License Manager. An outbound rule of the WAF’s Security Group should allow HTTPS access to the SonicWall License Manager.

SonicWall WAF should be able to reach the following hosts for proper functioning:

- `licensemanager.sonicwall.com`
- `lm2.sonicwall.com`
- `soniclicense.global.sonicwall.com`
- `smagbdata.global.sonicwall.com`
- `geoipdata.global.sonicwall.com`

**Creating a MySonicWall Account**

A MySonicWall account is required for product registration. If you already have an account, product registration is described in **Registering Your WAF Virtual Appliance** on page 21.
To create a MySonicWall account:

1. In your browser, navigate to https://www.mysonicwall.com.
2. In the login screen, click SIGN UP.
3. Enter your email address and create a password, then click CONTINUE.
4. In the next screens, enter information about your company and yourself.
5. Click Submit to create your account.

NOTE: MySonicWall registration information is not sold or shared with any other company.
Installing the WAF Virtual Appliance

This section explains how to install the SonicWall WAF virtual appliance in your Microsoft Azure environment.

Topics:
- Installing SonicWall WAF on page 7

Installing SonicWall WAF

The WAF Virtual Appliance is installed by launching the SonicWall Web Application Firewall (WAF) - BYOL instance from the Microsoft Azure website.

To install SonicWall WAF:
2. In a browser, access the SonicWall WAF BYOL page at one of:
   - Azure Marketplace
   - Azure Portal
     https://portal.azure.com/?pub_source=email&pub_status=success#create/sonicwall-inc.wafswl-waf-byol
You can also search for “SonicWall” in the public Azure marketplace to find this listing:

3 Click Create at the bottom of the page.
The Create Virtual Machine page displays.

4 In the **Name** field, type in a descriptive name for your WAF virtual appliance.

5 In the **User name** field, type in the name you will use to access the WAF instance.

6 Paste the text of your SSH public key into the **SSH public key** field. If you don’t already have an SSH public key for your Azure account, you can create one.

7 In the **Resource group** field, select one of:
   - **Create new** – to create a new resource group
   - **Use existing** – to use an existing resource group

8 In the **Location** field, select the location for this virtual appliance.
An example configuration for Basics is shown below:

9 Click OK.
The Size configuration screen displays.

10 Click on one of the recommended configurations and then click **Select**.
The **Settings** configuration screen displays.

<table>
<thead>
<tr>
<th>Create virtual machine</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Basics Done</td>
<td>High availability</td>
</tr>
<tr>
<td>2 Size Done</td>
<td>* Availability set: None</td>
</tr>
<tr>
<td>3 Settings</td>
<td>* Storage Use managed disks: Yes</td>
</tr>
<tr>
<td></td>
<td>Network:</td>
</tr>
<tr>
<td></td>
<td>* Virtual network: azurewaf_resourcergroup-vnet</td>
</tr>
<tr>
<td></td>
<td>* Subnet: default (10.1.6.0/24)</td>
</tr>
<tr>
<td></td>
<td>* Public IP address: (new) azure-sonicwall-waf2-ip</td>
</tr>
<tr>
<td></td>
<td>* Network security group (firewall): (new) azure-sonicwall-waf2-rsng</td>
</tr>
<tr>
<td>4 Summary</td>
<td>Extensions: No extensions</td>
</tr>
<tr>
<td></td>
<td>Auto-shutdown: Enable auto-shutdown: Off</td>
</tr>
<tr>
<td></td>
<td>Monitoring: Boot diagnostics: Enabled</td>
</tr>
</tbody>
</table>

11 Optionally make changes to any of the settings on this page, and then click **OK**.
The **Summary** screen displays.

12 Review the settings and click **Create** to create the WAF virtual appliance.

13 Click on the Alert icon at the top to see the notification information.
The notification changes when the deployment succeeds. Click the X to close the notification.

You are now ready to begin using your WAF virtual appliance. See:

- Configuring the WAF Virtual Appliance on page 15
- Registering Your WAF Virtual Appliance on page 21
Configuring the WAF Virtual Appliance

This section describes how to power on the WAF virtual appliance and log into it with either the web management interface or the command line interface.

Topics:
- Viewing the WAF Virtual Appliance Settings on page 15
- Powering the Virtual Appliance On or Off on page 16
- Connecting to the Web Interface on page 17
- Connecting to the Command Line Interface on page 18
- Using the Command Line Interface on page 19

Viewing the WAF Virtual Appliance Settings

To display the WAF settings and virtual appliance controls:

1. Click Virtual machines in the Azure left pane. All the virtual machines in your account are displayed.

2. Click on the WAF name to display the controls and settings for it.
Powering the Virtual Appliance On or Off

The WAF virtual appliance is automatically started after you click Create at the end of the installation process.

To stop, restart, or start the WAF:

1. Display the Overview page as described in Viewing the WAF Virtual Appliance Settings on page 15.
2. At the top of the right pane, click any of the controls for the virtual appliance:
   - Start – Starts the virtual appliance.
   - Restart – Restarts the virtual appliance.
   - Stop – Stops the virtual appliance.

Other controls are also available here, including Connect, Capture, Move, Delete, and Refresh.
## Connecting to the Web Interface

The WAF virtual appliance is accessible at the public IP address automatically assigned by Azure using DHCP addressing.

**To connect to the WAF:**

1. Display the Overview page as described in Viewing the WAF Virtual Appliance Settings on page 15.
2. Locate the Public IP address setting.
   - ![NOTE: The virtual appliance web interface listens on HTTPS at port 8443.](image)
3. In a browser, enter the public IP address using https, and specify port 8443 in the URL, such as:
   - `https://13.64.78.65:8443`
   - More generally, this is: `https://<WAF Public IP>:8443/`
4. In the WAF login screen, enter the default administrator credentials, admin / password, and then click LOGIN.

   ![Login Screen](image)

5. The first time you login, you are forced to change the password. Type the old and new passwords into the provided fields and then click CHANGE PASSWORD.

   ![Password Change Screen](image)
6. In the **End User Product Agreement** screen, read the agreement, click the **I Accept the terms of this Software Transaction Agreement** checkbox, and then click **Continue**.

The **System > Status** page is displayed, and you can register the WAF and begin management and configuration. See **Registering Your WAF Virtual Appliance** on page 21.

See the **SonicWall Web Application Firewall Administration Guide** for configuration information.

### Connecting to the Command Line Interface

The Command Line Interface (CLI) can be launched over SSH.

**To connect to SonicWall WAF over SSH:**

1. Display the Overview page as described in **Viewing the WAF Virtual Appliance Settings** on page 15.
2. Locate the **Public IP address** setting.
3. In an SSH application, type in the command using your Azure private key to authenticate:

   ```
   ssh -i AzurePrivateKey.key admin@<WAF Public IP>
   ```

   For example, `ssh -i AzurePrivateKey.key admin@13.64.78.65`

   **NOTE:** For management, log in using the **admin** account.

4. If you see a warning, type **yes** to proceed with the login.

   ```
   The authenticity of host '40.78.97.223 (40.78.97.223)' can't be established.
   ECDSA key fingerprint is SHA256:wIwC15lqVvYtPxBvOHjRD70wt0Xe0Vl9UJ1obsL9k.
   Are you sure you want to continue connecting (yes/no)? yes
   ```

Continue to **Using the Command Line Interface** on page 19.
Using the Command Line Interface

The CLI is a text-only mechanism for interacting with the WAF virtual appliance by typing commands to perform specific tasks. The CLI is launched as described in Connecting to the Command Line Interface on page 18.

The first-time login will require the admin to review the End User Product Agreement (EUPA) and accept it before proceeding. Press <SPACE> to scroll down.

Basic system information and network settings are displayed along with the main menu.

```
System Information
Model: WAF Virtual Appliance
Serial Number: Unknown
Version: 1.8.0.0-1waf
CPU (Utilization): Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz x 2 cores (19%)
Total Memory: 3.8 GB RAM (29%)
Hard Disk: 30 GB Disk (5%)
System Time: 2018/01/11 01:49:46
Up Time: 8 Days 06:40:24
X0 Auto-provision: Enabled
X0 IP Address: 10.1.6.4
X0 Subnet mask: 255.255.255.0
Default Gateway: 10.1.6.1 (X0)
Primary DNS: 168.63.120.16
Secondary DNS: n/a
Hostname: azure-sonicwall-waf
```

Main Menu
1. Show Network Info
2. Reboot
3. Restart WAF Services
4. Save TSR to Disk
5. Display EUPA
6. Logout

Press <Ctrl-c> at any time to cancel changes and logout.
Select a number (1-6): 

The main menu has six selections:

- **Show Network Info** on page 19
- **Reboot** on page 19
- **Restart WAF Services** on page 20
- **Save TSR to Disk** on page 20
- **Display EUPA** on page 20
- **Logout** on page 20

Show Network Info

**NOTE:** The X0 interface is the only interface configurable through the CLI. Currently, configuring any other interfaces using the CLI on a SonicWall WAF virtual appliance is not supported.

Reboot

Selecting this option displays a confirmation prompt, and then reboots.
Restart WAF Services
This option displays a confirmation prompt, and then restarts the web server and the related WAF Services.

Save TSR to Disk
Saves the current Technical Support Report to the hard disk on the WAF virtual appliance. This is useful for troubleshooting when the management console is not accessible, for example, in the case of a lockup.

Display EUPA
Displays the End User Product Agreement associated with the WAF virtual appliance.

Logout
The logout option ends the CLI session and returns to the login prompt.
Registering Your WAF Virtual Appliance

This section contains information about registering your WAF virtual appliance.

You must purchase a license and register your WAF on MySonicWall before first use. Registration is performed using the WAF web management interface. When registration is completed, WAF is licensed and ready to use.

Topics:
- About WAF Licensing on page 21
- Registering WAF on page 21

About WAF Licensing

Licensing is controlled by the SonicWall license manager service, and you can add licenses through your MySonicWall account. Unregistered units support the default license allotment for their model, but the unit must be registered in order to activate additional licensing from MySonicWall.

License status is displayed in the web management interface, in the Licenses & Registration section of the System > Status page.

Communication with the SonicWall License Manager is necessary while using the WAF virtual appliance, and requires internet access.

See WAF Virtual Appliance Requirements on page 4 and Internet Access Requirements on page 5 for more information.

Registering WAF

To register your WAF:

1. Log in to your WAF. The System > Status page displays.

2. Navigate to the System > Licenses page.

3. Click the register link.

4. Enter your MySonicWall account username and password in the appropriate fields. Click Submit.

5. The Administration section displays. Enter the Serial Number, Authentication Code, and Friendly Name for your SonicWall WAF virtual appliance.

6. Click Submit to finish the registration process.

7. You have successfully registered your WAF. Click Continue to view the Manage Licenses screen or continue configuring other settings within the virtual appliance.
Using the 30-day Trial Version

The WAF virtual appliance is offered in a 30-day Trial version. The installation, registration, and functionality of the 30-Day Trial appliance is the same as the full WAF, except for differences noted below in Deployment Considerations. An email is sent from the SonicWall License Manager to warn you when your trial is near its expiration date.

You must install the WAF software before registering for your 30-Day Trial. See Installing the WAF Virtual Appliance on page 7.

To upgrade to the full version:
1. Purchase the full WAF.
2. Export your settings from the 30-day Trial version.
3. Install and register the full WAF.
4. Import your settings.

Topics:
- Deployment Considerations on page 22
- Registering the 30-day Trial Virtual Appliance on page 22

Deployment Considerations

The following is a list of deployment considerations for the 30-day Trial version:

- The WAF is disabled after 30 days.
- Communication with the SonicWall License Manager is required during the entire trial period.
- It is recommended to save a copy of your WAF configuration settings before upgrading to the full version of SonicWall WAF.
- The elements of the basic MS Azure environment must be implemented prior to deploying the WAF.

Registering the 30-day Trial Virtual Appliance

This section details registration of the SonicWall 30-day Trial virtual appliance.

NOTE: Before starting the registration process, contact SonicWall Sales to obtain your serial number and authorization code.

To register the 30-day Trial:
1. Log in to your WAF.
2 Navigate to the System > Licenses page.

3 Click the Activate, Upgrade, or Renew services link.

4 Enter your MySonicWall account name and password, then click Submit.

5 Enter the Serial Number, Authentication Code, and a Friendly Name.

6 Click Submit.

7 When the registration confirmation page displays, click Continue.
Upgrading Your WAF Virtual Appliance

This section describes how to backup your WAF configuration settings and upgrade WAF software to a new version.

Topics:
- Exporting a Copy of Your Configuration Settings on page 24
- Backing up Settings Automatically on page 24
- Automatic Software Downloads on page 25
- Uploading a New WAF Image Manually on page 26

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your WAF virtual appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your WAF, protecting all your existing settings in the even that it becomes necessary to return a previous configuration state.

To export a copy of your configuration settings to a file on your local management station:

1. Log into your WAF virtual appliance and navigate to the System > Settings page.
2. Click the Export Settings button.
3. Save the settings file to your local machine.

The default settings file is named wafSettings.zip.

NOTE: To more easily restore settings in the future, rename the .zip file to include the version of the WAF image from which you are exporting the settings.

Backing up Settings Automatically

On the System > Settings page, WAF provides three options for automatic or scheduled settings backup:

- Automatically email settings on firmware upgrade
- Automatically send settings to external FTP server on firmware upgrade
- Enable scheduled settings backup
Enabling at least one of these settings backup options is highly recommended.

Automatic Software Downloads

WAF automatically downloads the latest official WAF software versions from the cloud. The new versions are displayed on the System > Software Update page. A description and Release Notes are available for each version. A System Alert is generated when a new software version is downloaded for update to notify the administrator. The new version can be installed by clicking on the Install Now button.

**NOTE:** It is highly recommended that the administrator reviews the latest software versions and keeps the WAF virtual appliance up-to-date.
Upgrading Your WAF Virtual Appliance

Uploading a New WAF Image Manually

To upload a new WAF virtual appliance image:

1. Download the WAF image file and save it to a location on your local computer.
3. Browse to the location where you saved the WAF virtual appliance image file, select the file, and click the Accept button.

The upload process can take up to one minute.

4. When the upload is complete, WAF installs the new image and automatically reboots the virtual appliance.
5. After successfully uploading the image to your WAF, the login screen is displayed. The updated image information is displayed on the System > Status page.

NOTE: WAF virtual appliances do not support downgrading an image and using the configuration settings file from a higher version. To downgrade to a previous version of a WAF image, you must create a new virtual appliance or load a snapshot taken earlier.
Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

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

The Support Portal enables you to:

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

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.
About This Document

Legend

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

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

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

WAF MS Azure Deployment Guide
Updated - April 2018
Software Version - 2.0
232-004271-00 Rev A

Copyright © 2018 SonicWall Inc. All rights reserved.

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

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

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

End User Product Agreement
To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements. Select the language based on your geographic location to see the EUPA that applies to your region.

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

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