



Secure Mobile Access 500v 10.2

Getting Started Guide

for Azure

SONICWALL®

Contents

Introduction	3
Before You Begin	4
Supported Platforms	4
Creating a MySonicWall Account	4
Installing the SMA 500v for Azure Virtual Appliance	6
Installing SMA 500v for Azure	6
Configuring the SMA 500v for Azure Virtual Appliance	11
Viewing the SMA 500v for Azure Settings	11
Powering the Virtual Appliance On or Off	12
Connecting to the Web Interface	12
Connecting to the Command Line Interface	14
Using the Command Line Interface	14
Show Network Information	15
Reboot	15
Restart SMA 500v for Azure Services	15
Logout	15
Save TSR to Flash	15
Display EULA	15
Licensing and Registering Your Appliance	16
Registering the SMA 500v for Azure	17
De-registering an SMA 500v for Azure	17
Using the 30-day Trial Version	19
Deployment Considerations	19
Registering the 30-day Trial Virtual	20
Converting a Free Trial License to Full	21
SonicWall Support	22
About This Document	23

Introduction

This Getting Started Guide contains installation procedures and configuration guidelines for deploying the SonicWall SMA 500v for Azure Virtual Appliance on a server in your network. The SMA 500v for Azure includes a software appliance, which has been preinstalled and preconfigured for your virtual environment, and allows for the secure and easy development of the SMA 500v for Azure Virtual Appliance solutions within that virtual environment.

SonicWall takes the challenge of the rapid pace of cloud transformation and extends the security of the private cloud to public clouds with the SonicWall Secure Mobile Access 100 series. The SMA 500v for Azure provides you with economy-of-scale benefits of virtualization. This provides all the security advantages of a physical Secure Mobile Access 100 appliance with the operational and economic benefits of virtualization, including system scalability and agility, speed of system provisioning, simple management, and cost reduction.

The SMA 500v for Azure provides the following benefits:

- **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**
 - SMA 500v for Azure is compatible with other SonicWall platforms either as a stand-alone (All-in-One) unit, control center, or as a remote analyzer.
- **Security**
 - SMA 500v for Azure provides an optimized, non-tamperable software and hardware architecture.

Before You Begin

Topics:

- [Supported Platforms](#)
- [Creating a MySonicWall Account](#)

Supported Platforms

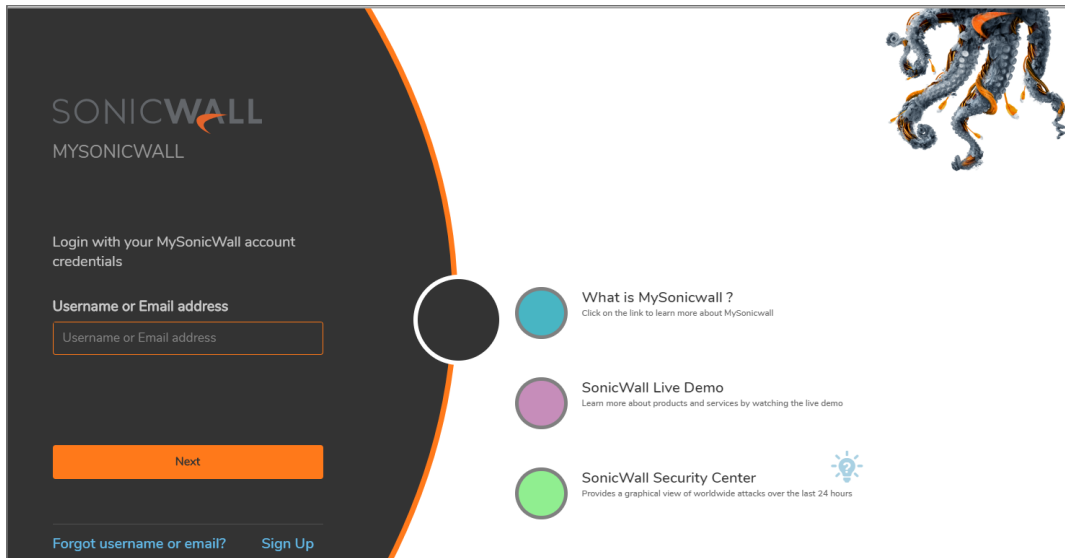
The elements of basic MS Azure infrastructure must be implemented prior to deploying SMA 500v for Azure.

Creating a MySonicWall Account

A MySonicWall account is required for product registration. If you already have an account, log in and continue to the [Registration](#) section.

To create a MySonicWall account:

1. In your browser, navigate to www.MySonicWall.com.
2. In the login screen, click the **Sign Up** link.



3. Complete the account information, including email and password.
 - ① | **NOTE:** Your password should be at least eight characters, but no more than 30 characters.
4. Enable two-factor authentication if desired.
5. If you enabled two-factor authentication, select one of the following authentication methods:
 - **Email (one-time passcode)** where an email with a one-time passcode is sent each time you log into your MySonicWall account.
 - **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code.
6. Click **CONTINUE** to go to the **Company** page.
7. Complete the company information and click **CONTINUE**.
8. On the **Your Info** page, select whether you want to receive security renewal emails.
9. Identify whether you are interested in beta testing new products.
10. Click **CONTINUE** to go to the **Extras** page.
11. Select whether you want to add additional contacts to be notified for contract renewals.
12. If you opted for additional contacts, input the information and click **ADD CONTACT**.
13. Click **DONE**.
14. Check your email for a verification code and enter it in the **Verification Code*** field. If you did not receive a code, contact Customer Support by clicking the link.
15. Click **DONE**. You are returned to the login window so you can login into MySonicWall with your new account.

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

Installing the SMA 500v for Azure Virtual Appliance

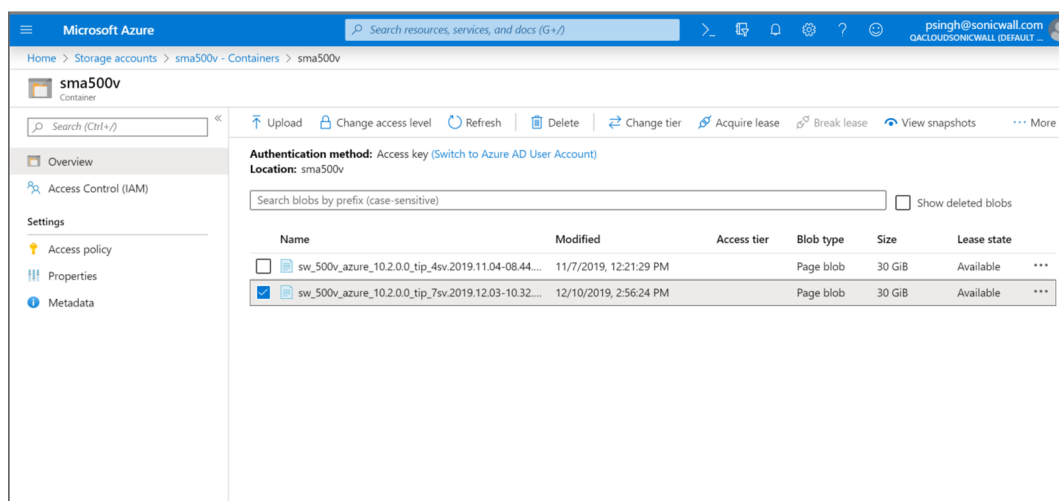
Topics:

- [Installing SMA 500v for Azure](#)

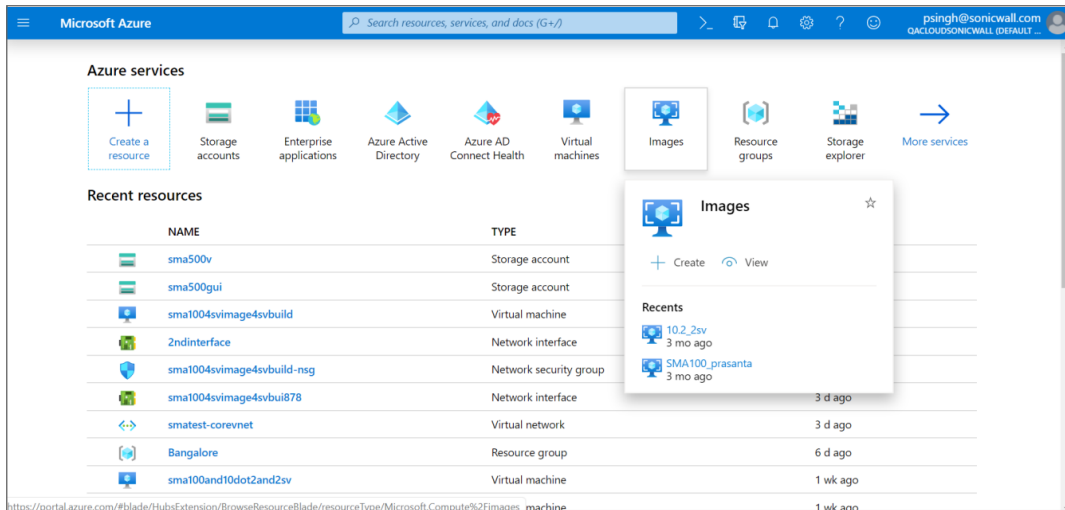
Installing SMA 500v for Azure

To install SonicWall SMA 500v for Azure:

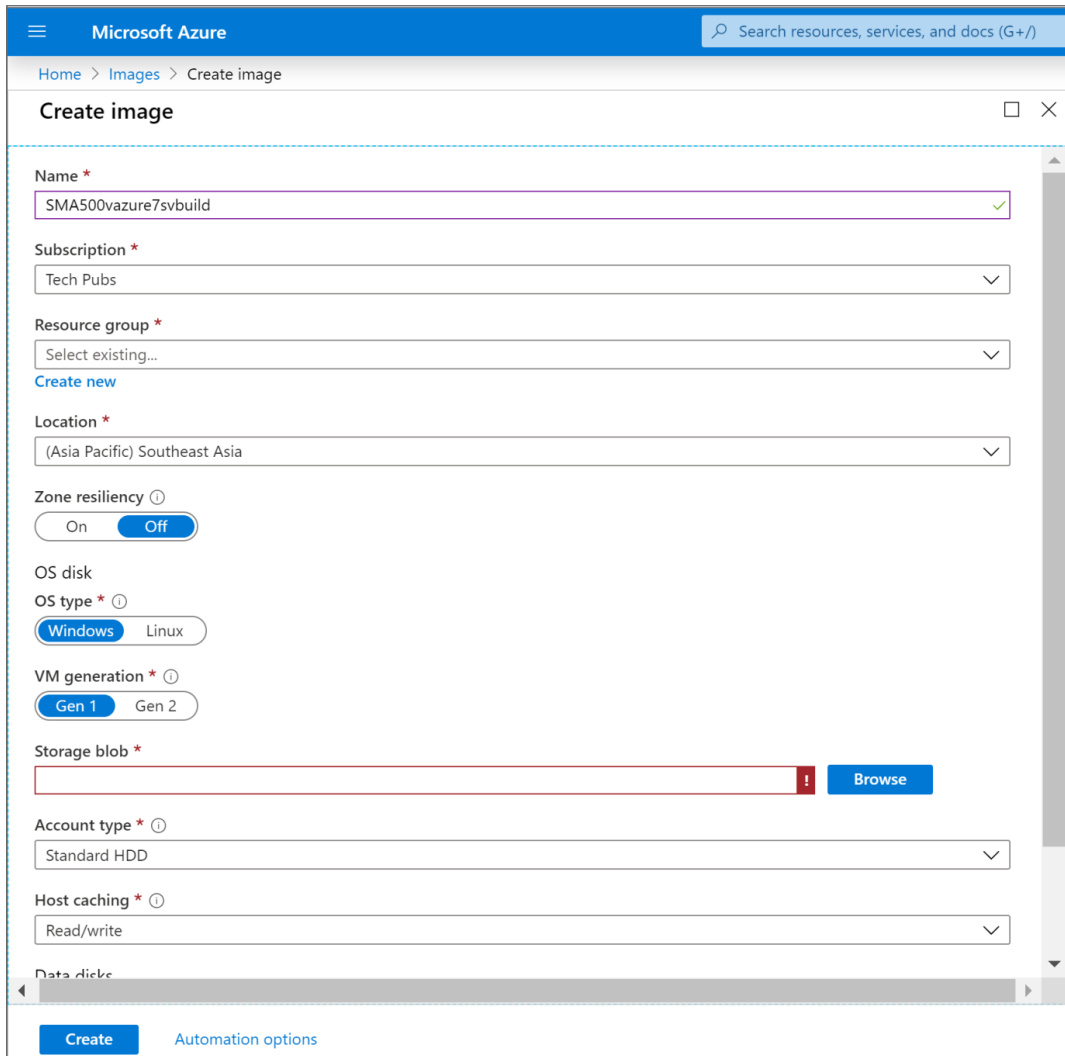
1. Log into your Microsoft Azure account at: <https://portal.azure.com>.
2. Click **Storage accounts** and navigate to the **Containers** of your storage account to make sure the current SMA 500v for Azure build is available.



3. On the Azure homepage, click **Images**.



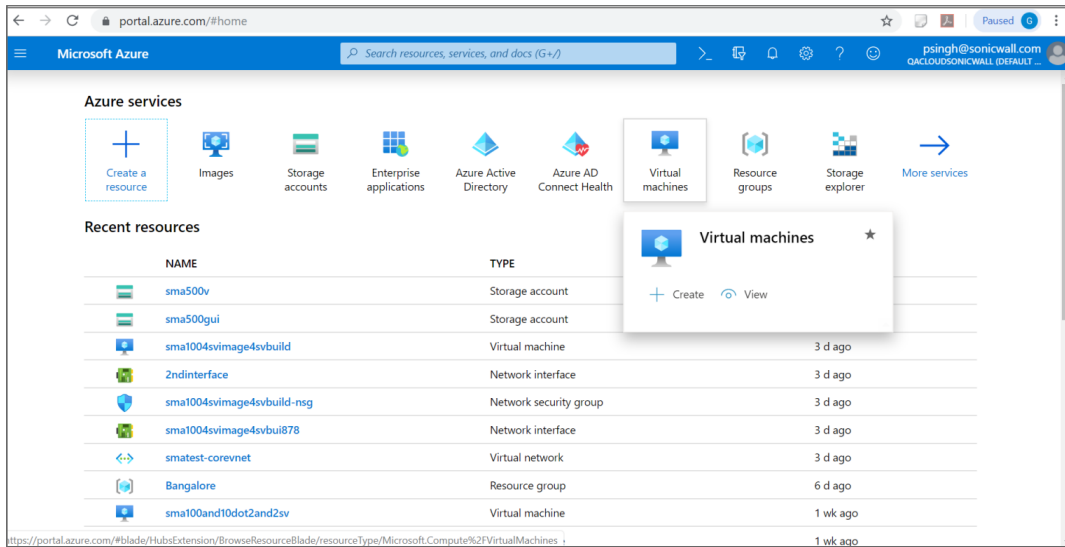
4. Click **+ Create**.
5. On the **Create image** dialog, configure the following options: **Name**, **Subscription**, **Resource group**, **Location**, **OS disk**.



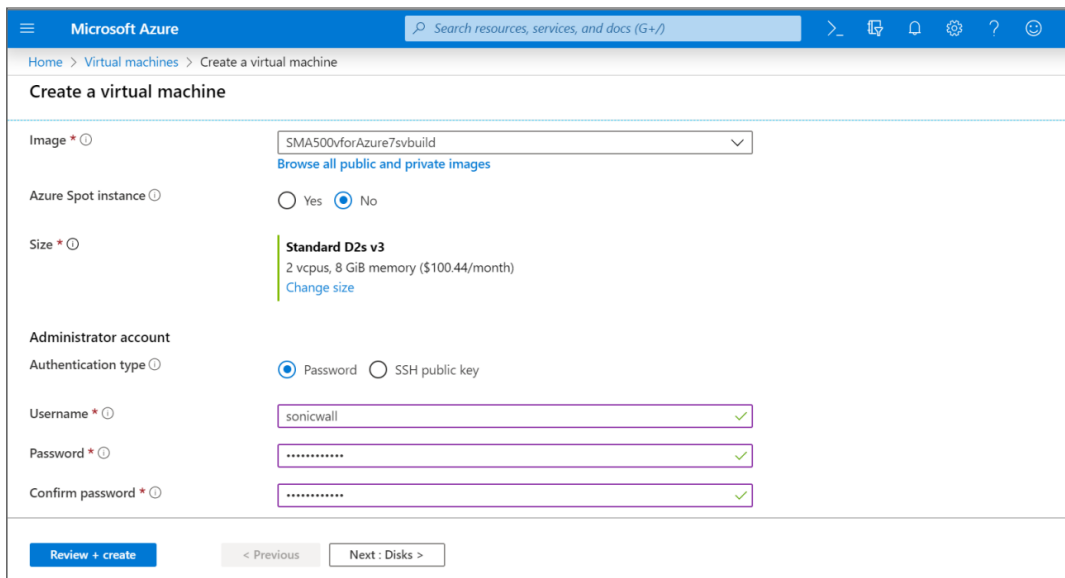
6. Browse and select the appropriate SMA 500v for Azure build in the **Storage blob** field. Click **Create** to build the image.

Wait some time for the image to be created for the SMA 500v for Azure current build.

7. Click **Notifications** to see the status of the image creation.
8. Navigate to the Azure Home page and click **Virtual machines**.



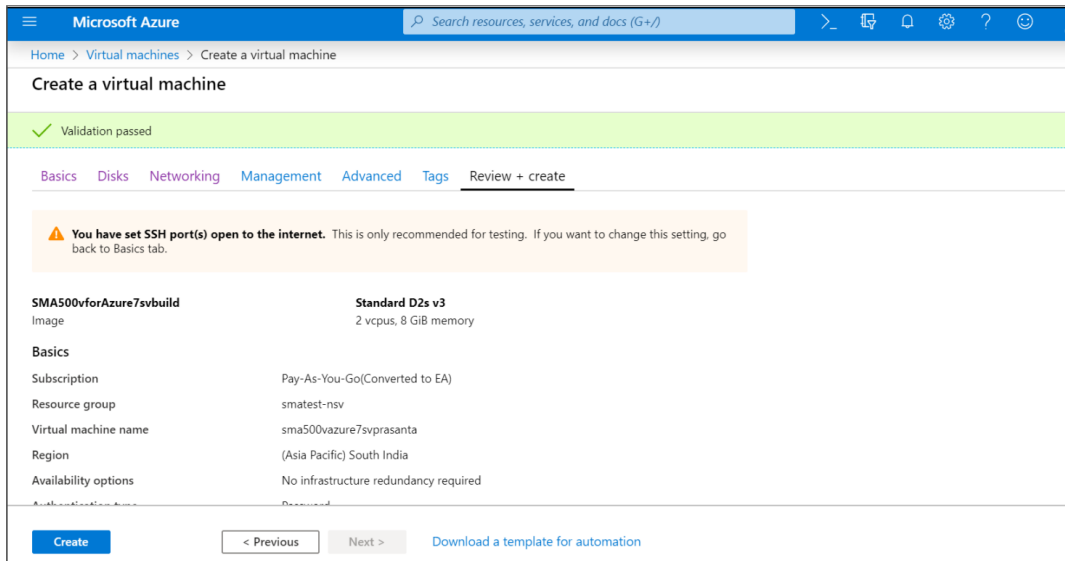
- On the **Virtual machines** page, click **+ Create** to create a virtual machine.



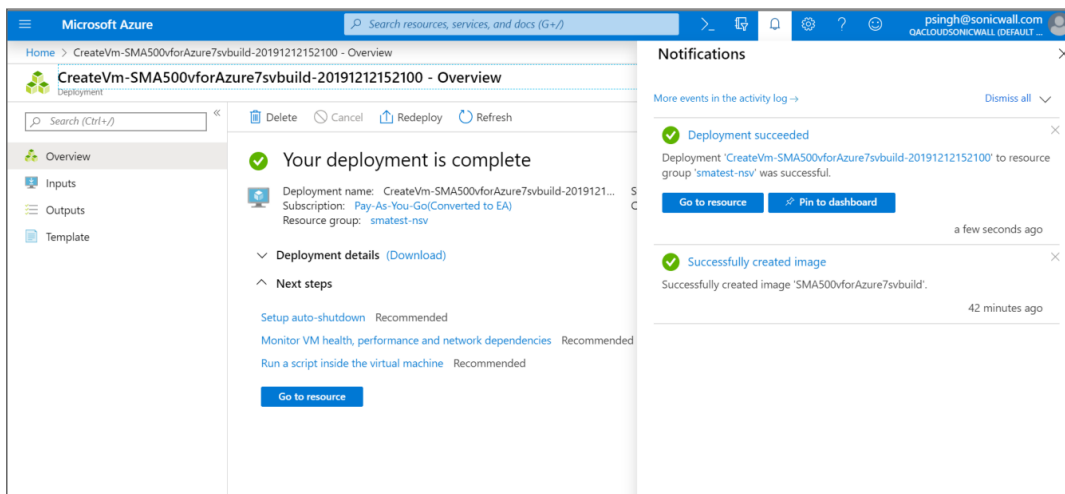
- On the **Create a virtual machine** page, configure the settings on the **Basics** tab:
 - Subscription**
 - Resource group**
 - Virtual machine name**
 - Image**—Click **Browse all public and private images > My items**, and select the image created for the current build.
 - Size**—Select the appropriate VM size. The default setting is **Standard D2s v3** (2vcpus, 8G memory).
 - In the **Administrator account** section, select one of the authentication methods and configure the settings for the selected authentication method:
 - Password**
 - SSH public key**

- Choose to open the inbound port.
11. Leave the remaining default settings and click **Review + Create** at the bottom of the page to continue.

Verify the configuration and then click **Create**.



12. Click **Notifications** to check the deployment status.



① **TIP:** Navigate to **Home > Virtual machines**, and click the newly created virtual machine to see the public IP address of the machine.

Configuring the SMA 500v for Azure Virtual Appliance

This section describes how to power on and configure basic settings on the SMA 500v for Azure Virtual Appliance, including virtual hardware settings and networking settings.

Topics:

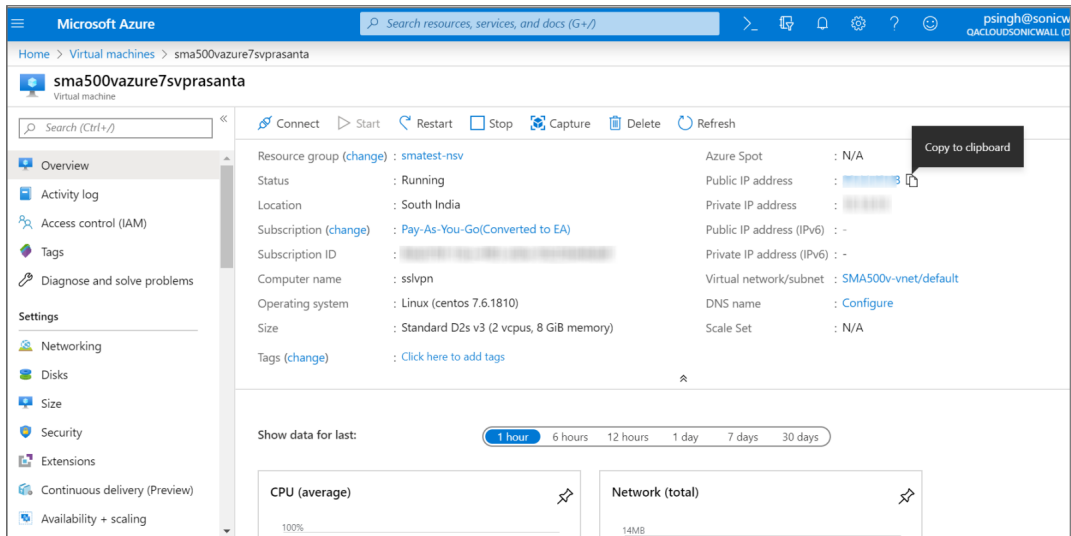
- [Viewing the SMA 500v for Azure Settings](#)
- [Powering the Virtual Appliance On or Off](#)
- [Connecting to the Web Interface](#)
- [Connecting to the Command Line Interface](#)
- [Using the Command Line Interface](#)

Viewing the SMA 500v for Azure Settings

To display the SMA 500v for Azure 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 the SMA 500v for Azure virtual machine to display the control and settings for it.

The **Overview** page displays.



Powering the Virtual Appliance On or Off

The SMA 500v for Azure virtual appliance automatically starts after you click **Create** at the end of the installation process.

To stop, restart, or start the SMA 500v for Azure:

1. Display the **Overview** page as described in [Viewing the Settings](#).
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 available here, including **Connect**, **Capture**, **Move**, **Delete**, and **Refresh**.

Connecting to the Web Interface

The SMA 500v for Azure virtual appliance is accessible at the public IP address automatically assigned by Azure using DHCP addressing.

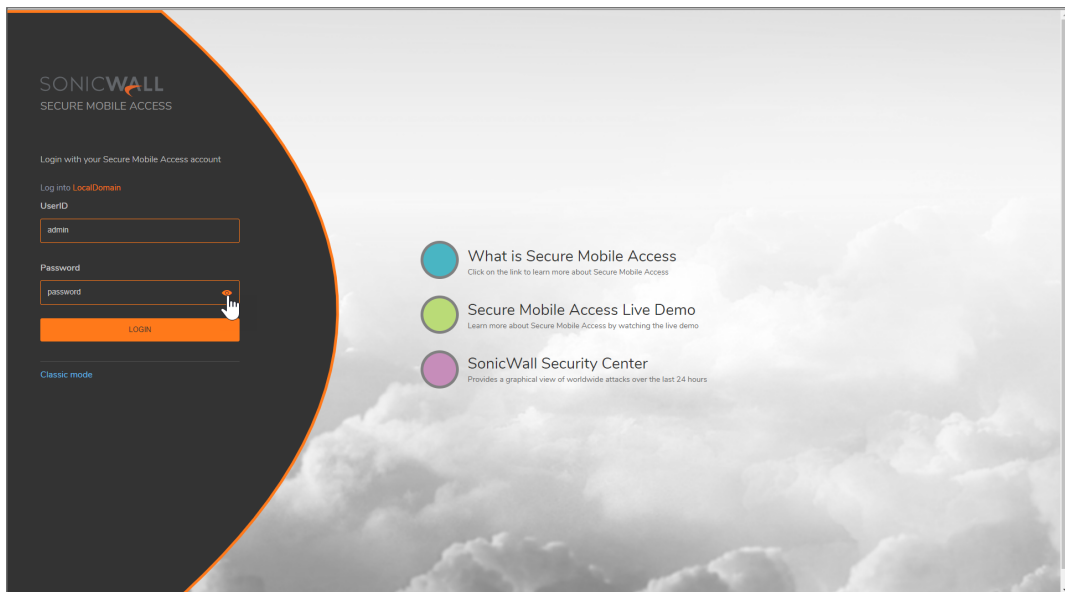
To connect to the SMA 500v for Azure:

1. Navigate to the **Overview** page of your appliance as described in [Viewing the Settings](#).
2. Locate the **Public IP address**.
3. In a browser, enter the public IP address using https. We use default port 443 to access the SMA 500v for Azure appliance.

Generally, this is: `https://<SMA 500v for Azure Public IP>/`

4. In the SMA 500v for Azure login screen, enter the default administrator credentials, **admin /**

password, and then click **LOGIN**.



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**.
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 **Dashboard** page displays. To register the SMA 500v for Azure and begin management and configuration, see *Registering the SMA 500v for Azure*.



Connecting to the Command Line Interface

The Command Line Interface (CLI) is a text-only mechanism for interacting with the SMA 500v for Azure virtual appliance by typing commands to perform specific tasks. The CLI can be launched over SSH.

To connect to the SMA 500v for Azure over SSH:

1. Display the **Overview** page as described in [Viewing the SMA 500v for Azure Settings](#).
2. Locate the **Public IP address**.
3. In an SSH application, type in the command using your SMA 500v for Azure private key to authenticate:

```
• ssh -i SMAPrivateKey.key admin@<SMA 500v for Azure Public IP>
```

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

① | **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:wIWc15lqVyvtPxbv0HjRD70WDT0WXE0Vl9UJ1obsL9k.  
Are you sure you want to continue connecting (yes/no)? yes
```

Continue to [Using the Command Line Interface](#).

Using the Command Line Interface

The Command Line Interface (CLI) is a text-only mechanism for interacting with a computer operating system or software by typing commands to perform specific tasks. It is a critical part of the deployment of the SMA 500v for Azure Virtual Appliance, where basic networking needs to be configured from the console.

While the physical SMA 500v for Azure Virtual Appliance has a default IP address and network configuration that requires a client's network settings to be reconfigured to connect, as the network settings in the VMware virtual environment might conflict with the SonicWall defaults. The CLI utility remedies this by allowing basic configuration of the network settings when deploying the SMA 500v for Azure Virtual Appliance.

After the SMA 500v for Azure Virtual Appliance firmware has fully booted, a login prompt is displayed.

To access the CLI, login as admin. The password is the same as the password for the "admin" account configured on the appliance. The default is password.

```
sslvpn login: admin  
Password: <password>
```

If an incorrect password is entered, the login prompt is displayed again. If the correct password is entered, the CLI is launched.

① | **NOTE:** The User input used in the examples highlighted in red indicates text entered by the user, there is no coloring of text done on the actual CLI.

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

The main menu has six selections:

- [Show Network Information](#)
- [Reboot](#)
- [Restart SSL VPN Services](#)
- [Restart SMA 500v for Azure Services](#)
- [Logout](#)
- [Save TSR to Flash](#)
- [Display EULA](#)

Show Network Information

① **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:

```
Reboot
Are you sure you want to reboot (y/n)?
```

Restart SMA 500v for Azure Services

This option displays a confirmation prompt, and then restarts the web server and the related SMA 500v for Azure Services.

Logout

The logout option ends the CLI session and returns to the login prompt.

Save TSR to Flash

Saves the Technical Support Report (TSR) to flash memory on the SMA 500v for Azure Virtual Appliance.

Display EULA

Displays the End User License Agreement (EULA) associated with the SMA 500v for Azure Virtual Appliance.

Licensing and Registering Your Appliance

This section contains information about licensing and registering your SMA 500v for Azure Virtual Appliance.

You must purchase a license and register your SMA 500v for Azure before first use. Registration is performed using the management interface. After the registration is completed, the SMA 500v for Azure is licensed and ready to use. For the 30-Day Trial Virtual Appliance registration process, refer to Registering the 30-day Trial Virtual Appliance.

① **NOTE:** The SMA 500v for Azure shares the same SKU and license structure as the SMA 500v for Azure. After you have purchased an SMA 500v for Azure Virtual Appliance from MySonicWall, you can use the serial number and authorization code you get to register the SMA 500v for Azure or for SMA 500v for Azure. However, you cannot use the same serial number and authorization code to register both.

SMA 500v for Azure provides user-based licensing. By default, the virtual appliance comes with a 5-user license. Extra licenses can be added in 5, 10, and 25 user denominations, up to a maximum that allows for 50 concurrent user sessions.

Licensing is controlled by SonicWall's license manager service, and customers can add licenses through their MySonicWall accounts. 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 SMA 500v for Azure Virtual Appliance management interface, on the Licenses & Registration section of the **System > Status** page.

Communication with the SonicWall Licensing Manager is necessary while using the SMA 500v for Azure Virtual Appliance, and requires Internet access.

If a user attempts to log in to the Virtual Office portal and there are no more available user licenses, the login page displays the error, "No more User Licenses available. Please contact your administrator." The same error is displayed when a user launches the NetExtender client when all user licenses are in use. These login attempts are logged with a similar message in the log entries, and displayed in the **Log > View** page. You can add user licenses if this occurs regularly. For occasional spikes in remote access needs, you can purchase a Spike License to temporarily increase the number of remote users your virtual appliance can support. See the *SMA Administration Guide* for more information.

Topics:

- [Registering the SMA 500v for Azure](#)
- [De-registering an SMA 500v for Azure](#)

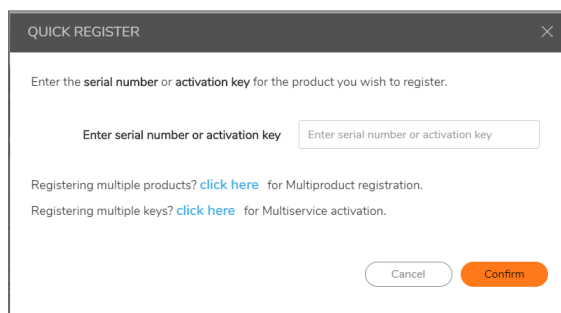
Registering the SMA 500v for Azure

After you have installed and configured the network settings for your SMA 500v for Azure Virtual Appliance, you can log into the management console and register it to your MySonicWall account. Registration of your SonicWall SMA 500v for Azure Virtual Appliance follows the same process as for other SonicWall hardware-based appliances.

① | **NOTE:** System functionality is extremely limited when registration is not completed.

To register your SMA 500v for Azure Virtual Appliance:

1. Log in to your SMA 500v for Azure. Navigate to the **System > Licenses** page.
2. Under **Manage Security Services Online**, click **Activate, Upgrade, or Renew services**. This should take you to a MySonicWall login.
3. Enter your MySonicWall.com account username or email address and password in the appropriate fields. Click **Submit**.
4. The **Dashboard** displays. Click the **Add Product** icon in the top button bar.



5. Enter the **Serial Number** or **Activation Key** for your new appliance. Click **Confirm** to finish the registration process.
6. You have successfully registered your SMA 500v for Azure. Click **Continue** to view the Manage Licenses screen or continue configuring other settings within the appliance.

De-registering an SMA 500v for Azure

You can de-register an SMA 500v for Azure directly from the Secure Mobile Access interface. Removing the registration puts the virtual appliance into an unregistered state and deletes the binding between it and its serial number in MySonicWall. At that point, you can use that serial number to register the same or another SMA 500v for Azure instance. Only one SMA 500v for Azure instance is allowed per serial number.

To De-register an SMA 500v for Azure:

1. Log into the Secure Mobile Access management interface on your SMA 500v for Azure Virtual Appliance.
2. Navigate to the **System > Settings** page.
3. Under **Settings Management**, click **Export Settings** to export a copy of your current configuration

settings before de-registering your SMA 500v for Azure. This makes it possible to import these settings to another SMA 500v for Azure instance.

 **CAUTION:** Be sure to export your configuration settings before de-registering your SMA 500v for Azure. You cannot recover them after de-registration.

4. Navigate to **System > Licenses**.
5. Under **Manage Security Services Online**, click **Activate, Upgrade, or Renew services** and log into your MySonicWall account.
6. Navigate to **Product Management > My Products**, and select the SMA 500v for Azure you would like to de-register. Click **Delete Product** on the far right of the row. A dialog box appears requesting the reason.
7. Click **Confirm**.
8. If the de-registration is successful, the SMA 500v for Azure returns to the unregistered state.

Using the 30-day Trial Version

The SMA 500v for Azure 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 SMA 500v for Azure, 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.

To upgrade to the full version:

- Purchase the full SMA 500v for Azure.
- Export your settings from the 30-day Trial version.
- Install and register the full SMA 500v for Azure.
- Import your settings.

You must install the SMA 500v for Azure software before registering your 30-Day Trial. For more information on obtaining the software, see [Downloading the Virtual Appliance Software](#).

Topics:

- [Deployment Considerations](#)
- [Registering the 30-day Trial Virtual Appliance](#)
- [Converting a Free Trial License to Full License](#)

Deployment Considerations

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

- The SMA 500v for Azure is disabled after 30 days.
- A maximum of two concurrent users are allowed to login to the appliance.
- Trial versions of Web Application Firewall are activated during registration.
- No paid add-on licenses or services can be added.
- Communication with the SonicWall Licensing Manager is required during the entire trial period.
- It is recommended to save a copy of your appliance's configuration settings before upgrading to the actual version of the SMA 500v for Azure.

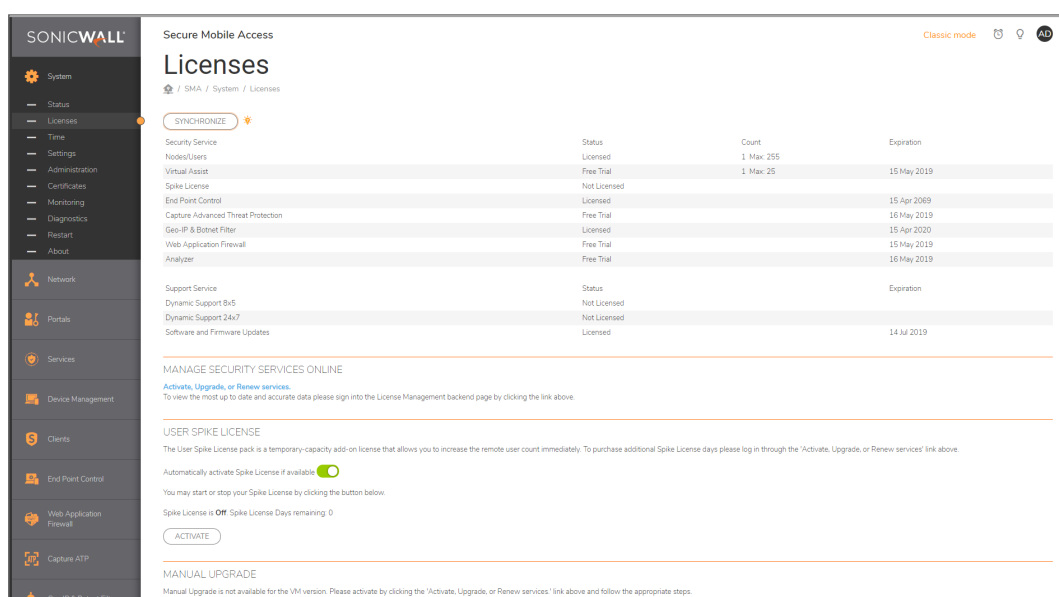
Registering the 30-day Trial Virtual

This section details registration of the SonicWall 30-day Trial Virtual Appliance.

- ① **NOTE:** Before starting the registration process, contact SonicWall Sales to obtain a serial number and authorization code.

To register the 30-day Trial:

1. Log in to your SMA 500v for Azure Virtual Appliance.
2. Navigate to the **System > Licenses** page.



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

The screenshot shows the 'License Management' login form. It includes a 'Synchronize' button with a refresh icon. The form has two input fields: 'MySonicWALL username/email:' and 'Password:'. Below the password field is a 'Submit' button. At the bottom left, there is a link: 'Forgot your Username or Password?'.

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**.

Converting a Free Trial License to Full

An SMA 500v for Azure instance installed as a 30-day free trial can easily be converted to a full production licensed SMA 500v for Azure instance.

To convert your free trial to a production version:

1. Purchase an SMA 500v for Azure license from a distributor. You should receive a fulfillment email with the new serial number and authentication code.
2. Log in to Secure Mobile Access on your free trial instance.
3. Navigate to the **System > Licenses** page.
4. Under **Manage Security Services Online**, click **Activate, Upgrade, or Renew services** and log in to your MySonicWall account.
5. Navigate to your **My Products** page, and select the free instance of the SMA 500v for Azure you would like to unregister. Click **Deregister**.
6. Click **OK** in the confirmation dialog. The SMA 500v for Azure returns to the unregistered state.
7. In MySonicWall , click to **Register** a new instance.
8. Enter the **Serial Number** and **Authentication Code** you received after purchasing your SMA 500v for Azure instance. Your SMA 500v for Azure is now registered.

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
- 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

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.

Secure Mobile Access 500v for Azure Getting Started Guide

Updated - June 2021

Software Version - 10.2

232-005647-00 Rev A

Copyright © 2021 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