Secure Mobile Access 12.4

SMA and CMS on Azure Getting Started Guide

Contents

1

Overview

This Getting Start Guide contains installation procedures and configuration guidelines for deploying the SonicWall SMA 8200v-standalone (Virtual Appliance) and CMS in your Microsoft Azure cloud network.

SonicWall takes the challenge of rapid pace of cloud transformation and extends the security of the private cloud to public clouds with SonicWall Secure Mobile Access 1000 (SMA 8200v) series. The SMA 8200v gives you economy-of-scale benefits of virtualization. This gives you all the security advantages of a physical SMA 1000 appliance with the operational and economic benefits of virtualization, including system scalability and agility, speed of system provisioning, simple management and cost reduction.

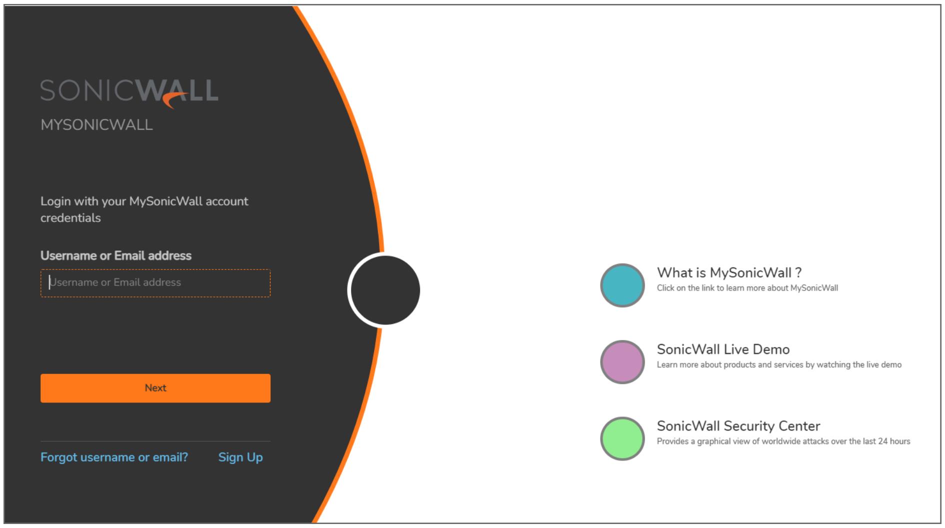
Before You Begin

Creating a MySonicWall Account

A MySonicWall account is required for product registration. If you already have an account, continue to the section on Registering the SMA 8200v-Standalone and CMS.

To create a MySonicWall account:

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


SONICWALL
MYSONICWALL
Login with your MySonicWall account credentials
Username or Email address
Username or Email address
Next
Forgot username or email?
Sign Up
What is MySonicWall ?
Click on the link to learn more about MySonicWall
SonicWall Live Demo
Learn more about products and services by watching the live demo
SonicWall Security Center
Provides a graphical view of worldwide attacks over the last 24 hours

3. Complete the account information, including email and password.

   ⓘ | **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.

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

3

Installing SMA 8200v-Standalone and CMS on Azure

This section explains how to deploy the SonicWall SMA 8200v-standalone and CMS in your Azure environment.

> ⓘ **NOTE:** Installation of SMA 8200v-standalone and CMS on Azure is supported only from the SMA 12.4 and above firmware versions.

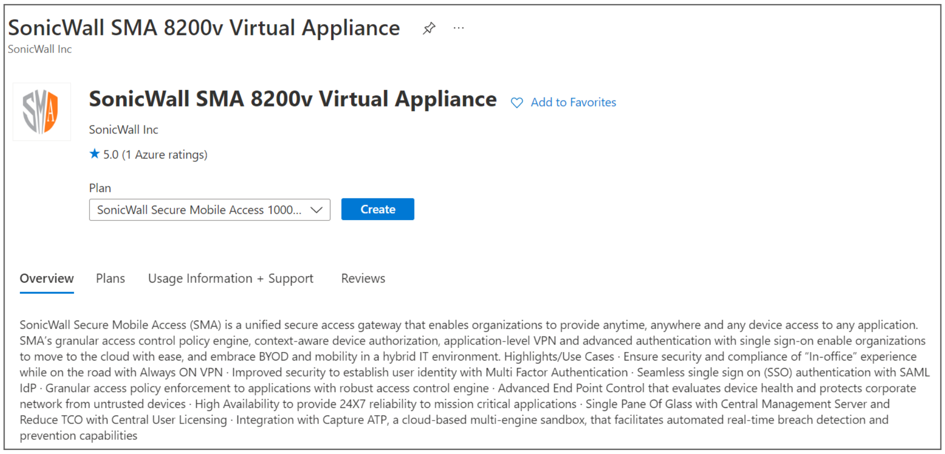
Deployment Guidelines

For details on deployment guidelines, refer SMA 8200v Azure/AWS Deployment Guidelines | SonicWall

To install the SMA 8200v-standalone and CMS for Azure:

1. Log into your Azure account at https://portal.azure.com.
2. In the Azure Marketplace, search for and select the SonicWall SMA 8200v listing, then click **Get It Now**.

   The **SonicWall SMA 8200v Virtual Appliance** page displays.

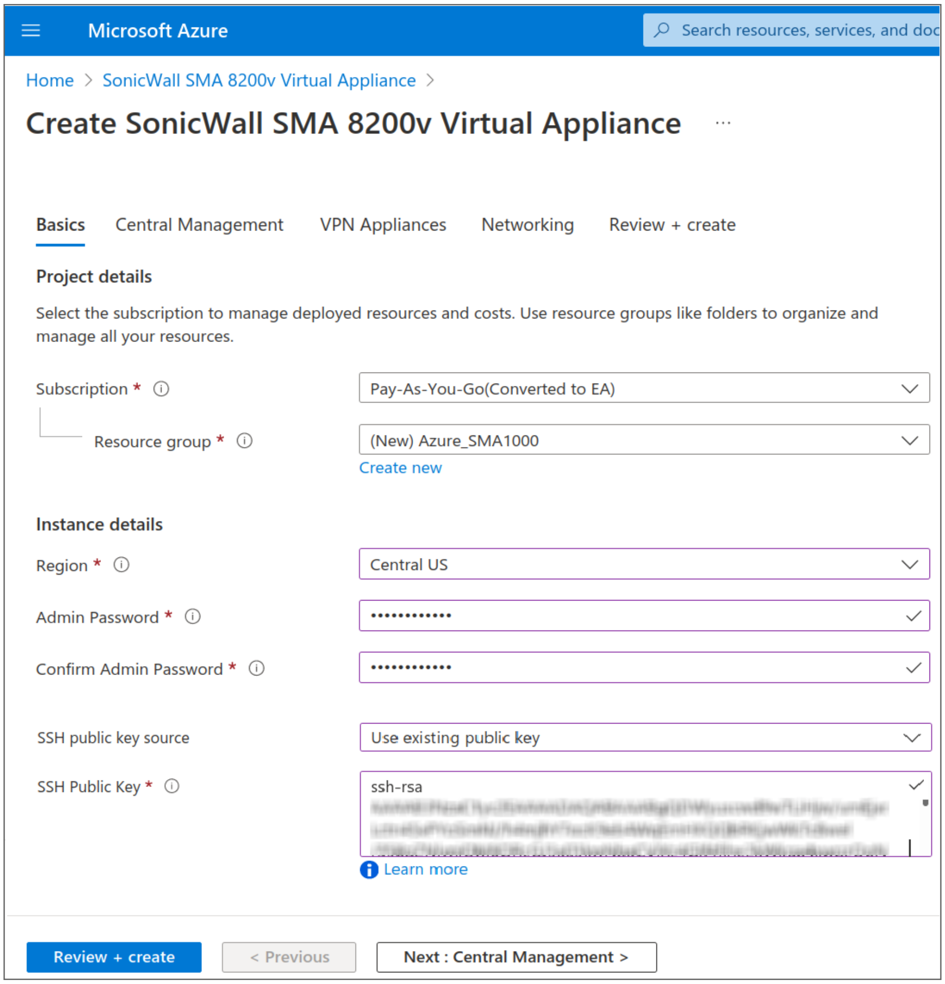

SonicWall SMA 8200v Virtual Appliance
SonicWall Inc
SonicWall SMA 8200v Virtual Appliance
Add to Favorites
SonicWall Inc
★ 5.0 (1 Azure ratings)
Plan
SonicWall Secure Mobile Access 1000...
Create
Overview
Plans
Usage Information + Support
Reviews

SonicWall Secure Mobile Access (SMA) is a unified secure access gateway that enables organizations to provide anytime, anywhere and any device access to any application. SMA's granular access control policy engine, context-aware device authorization, application-level VPN and advanced authentication with single sign-on enable organizations to move to the cloud with ease, and embrace BYOD and mobility in a hybrid IT environment. Highlights/Use Cases · Ensure security and compliance of "In-office" experience while on the road with Always ON VPN · Improved security to establish user identity with Multi Factor Authentication · Seamless single sign on (SSO) authentication with SAML IdP · Granular access policy enforcement to applications with robust access control engine · Advanced End Point Control that evaluates device health and protects corporate network from untrusted devices · High Availability to provide 24X7 reliability to mission critical applications · Single Pane Of Glass with Central Management Server and Reduce TCO with Central User Licensing · Integration with Capture ATP, a cloud-based multi-engine sandbox, that facilitates automated real-time breach detection and prevention capabilities

3. In the **SonicWall SMA 8200v Virtual Appliance** page, click **Create**.

   The **Basics** page displays.

4. By default, the **Subscription** field is selected based on your currently active Azure subscription. Based on your subscription type, SMA1000 deployment will be created in and billed. If you have multiple subscriptions, you can select a different one in the drop-down menu.
5. In the **Resource group** field, select the existing resource group from the drop-down or click **Create new** to create a new resource group. This is the resource group your SMA 8200v-standalone deployment will be created in.
6. In the **Region** field, select the location for these virtual appliance(s).
7. In the **Admin Password** and **Confirm Admin Password** fields, enter the password.



Create SonicWall SMA 8200v Virtual Appliance

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Pay-As-You-Go(Converted to EA)

Resource group * : (New) Azure_SMA1000

Instance details

Region * : Central US

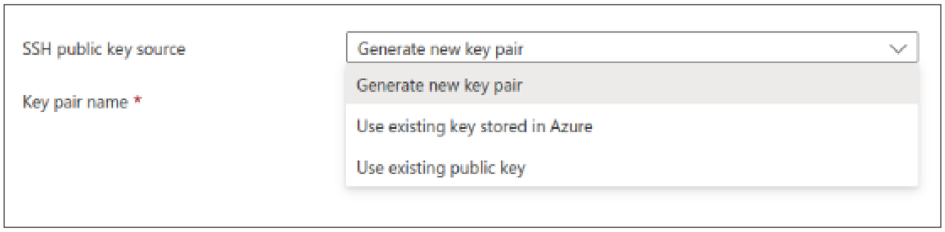
Admin Password * : ••••••••••••

Confirm Admin Password * : ••••••••••••

SSH public key source : Use existing public key

SSH Public Key * : ssh-rsa [redacted]

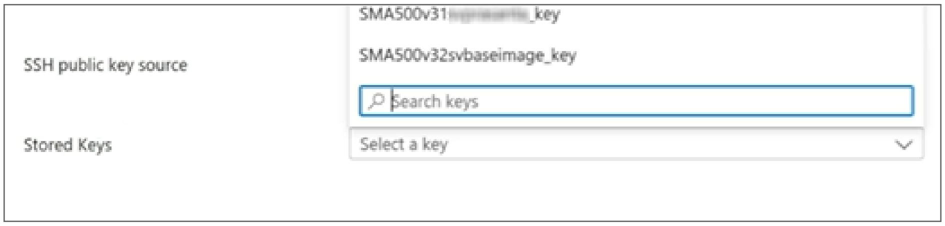
8. In the **SSH public key source** field, select the following options from the drop-down.
   - **Generate new key pair** - If you don't have an existing SSH public key for your Azure account, you can create new key and select the key pair name in the **Key pair name** field.



SSH public key source: Generate new key pair

Key pair name *

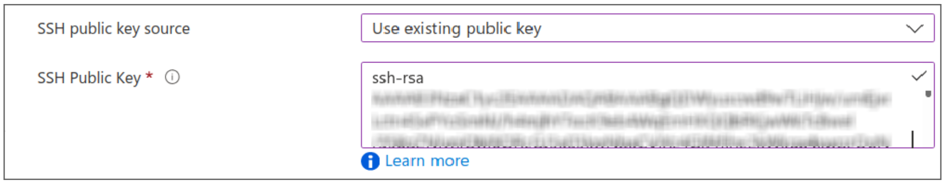
- **Use existing key stored in Azure** - If you have an existing stored SSH key for your Azure account, under **Stored Keys** field, select a key from the drop-down.



SSH public key source

Stored Keys: Select a key

- **Use existing public key** - If you have an existing SSH public key for your Azure account, enter the text of your existing key into the **SSH public key** field.



SSH public key source: Use existing public key

SSH Public Key *: ssh-rsa [redacted]

9. Click **Next: Central Management >**.

   The **Central Management** page displays.

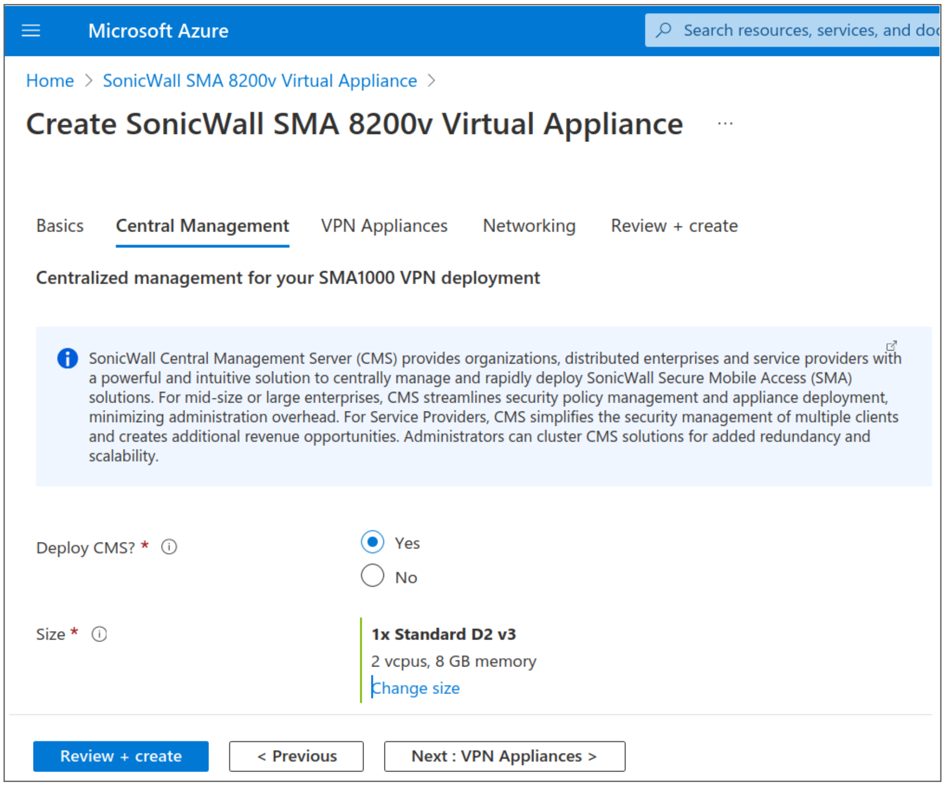
10. In the **Deploy CMS?**, select the following options based on your requirement.

    Select **Yes** - To deploy CMS on Azure.

    Select **No** - Not to deploy CMS on Azure.

    In the **Size** field, the default memory size displays in the above field. If you wish to select a different configuration, click **Change size** and select the memory size based on your requirements.

    ⓘ | **NOTE:** The minimum recommended memory size for CMS is 1x Standard D2 v3.


Microsoft Azure
Search resources, services, and doc
Home > SonicWall SMA 8200v Virtual Appliance >

Create SonicWall SMA 8200v Virtual Appliance

Basics
Central Management
VPN Appliances
Networking
Review + create

Centralized management for your SMA1000 VPN deployment

SonicWall Central Management Server (CMS) provides organizations, distributed enterprises and service providers with a powerful and intuitive solution to centrally manage and rapidly deploy SonicWall Secure Mobile Access (SMA) solutions. For mid-size or large enterprises, CMS streamlines security policy management and appliance deployment, minimizing administration overhead. For Service Providers, CMS simplifies the security management of multiple clients and creates additional revenue opportunities. Administrators can cluster CMS solutions for added redundancy and scalability.

Deploy CMS? * ● Yes ○ No

Size * 1x Standard D2 v3
2 vcpus, 8 GB memory
Change size

11. Click **Next: VPN Appliances >**.

    The **VPN Appliances** page displays.

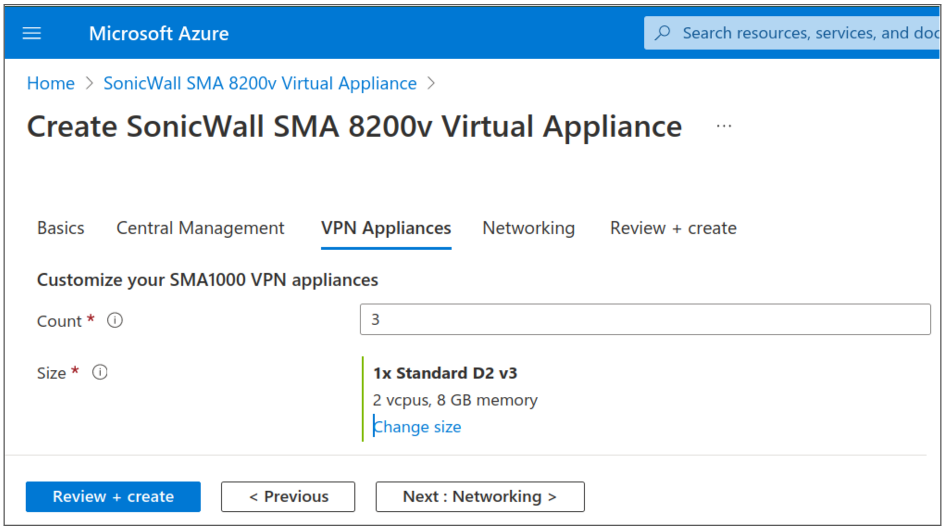
12. In the **Count** field, enter the number of SMA 8200v-standalone appliances you need to deploy. If you do not need to deploy SMA 8200v-standalone appliance on Azure, then enter the count as 0 in the count field.

13. In the **Size** field, the default memory size displays based on the SMA 8200v-standalone count entered in the above field. If you wish to select a different configuration, click **Change size** and select the memory size based on your requirements.

    ⓘ | **NOTE:** The minimum recommended memory size is 2 vcpus and 8 GB RAM.

    The following recommendations are intended as guidelines to instance type selection, derived from extensive lab-based testing and analysis. It is extremely important to keep in mind that inherent differences in deployment-specific usage patterns may necessitate use of larger, or smaller, instance types than these general-purpose recommendations.

Expected User Count	Recommended Instance Type	Specification
Up to 500	F2	2 core, 4GB RAM
Up to 2000	F4s_v2	4 core, 8GB RAM
Up to 5000	F8s_v2	8 core, 16GB RAM



Create SonicWall SMA 8200v Virtual Appliance

Customize your SMA1000 VPN appliances

Count * 3

Size * 1x Standard D2 v3
2 vcpus, 8 GB memory

14. Click **Next: Networking**.

    The **Networking** page displays.

15. In the **Networking** page, configure the virtual network based on your requirements.

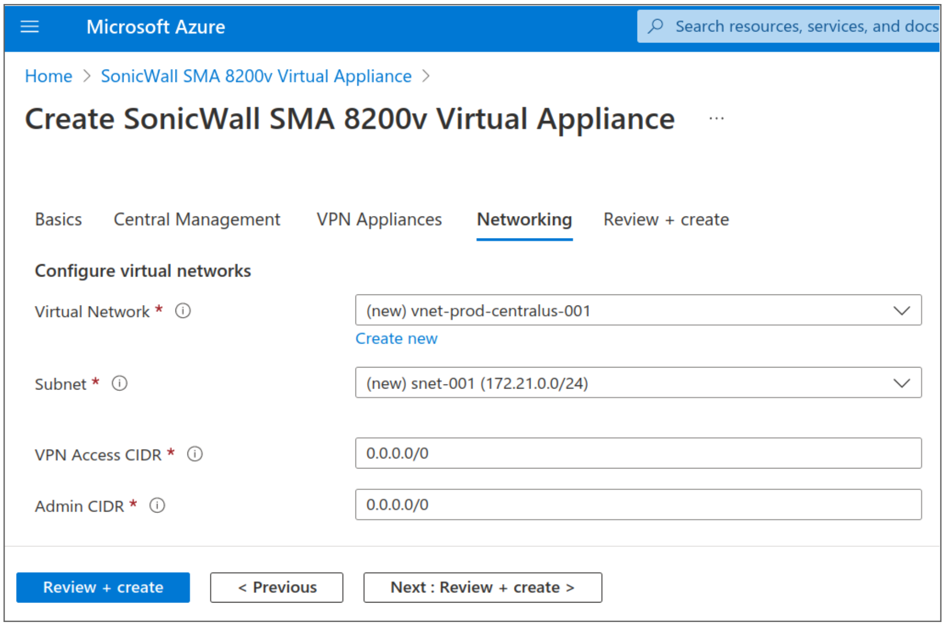
    a. In the **Virtual Network** field, select an existing virtual network from the drop-down or click **Create new** to create a new virtual network.

    b. In the **Subnet** field, select a subnet from the drop-down.

    c. By default, the **VPN Access CIDR** field is set to 0.0.0.0/0 which allows you to access VPN from any place. If you want to limit VPN access to a trusted IP range, enter that IP range in this field.

    d. By default, the **Admin CIDR** field is set to 0.0.0.0/0 which allows you to access AMC and SSH from any place. If you want to limit AMC and SSH access to a trusted IP range, enter that IP range in this field.

    ⓘ **NOTE:** For details on how to configure static IP pools for VPN tunnels in Azure, see SMA 8200v Azure/AWS Deployment Guidelines | SonicWall


Microsoft Azure
Search resources, services, and docs
Home > SonicWall SMA 8200v Virtual Appliance >
Create SonicWall SMA 8200v Virtual Appliance ...
Basics
Central Management
VPN Appliances
Networking
Review + create

Configure virtual networks

Virtual Network * : (new) vnet-prod-centralus-001

Create new

Subnet * : (new) snet-001 (172.21.0.0/24)

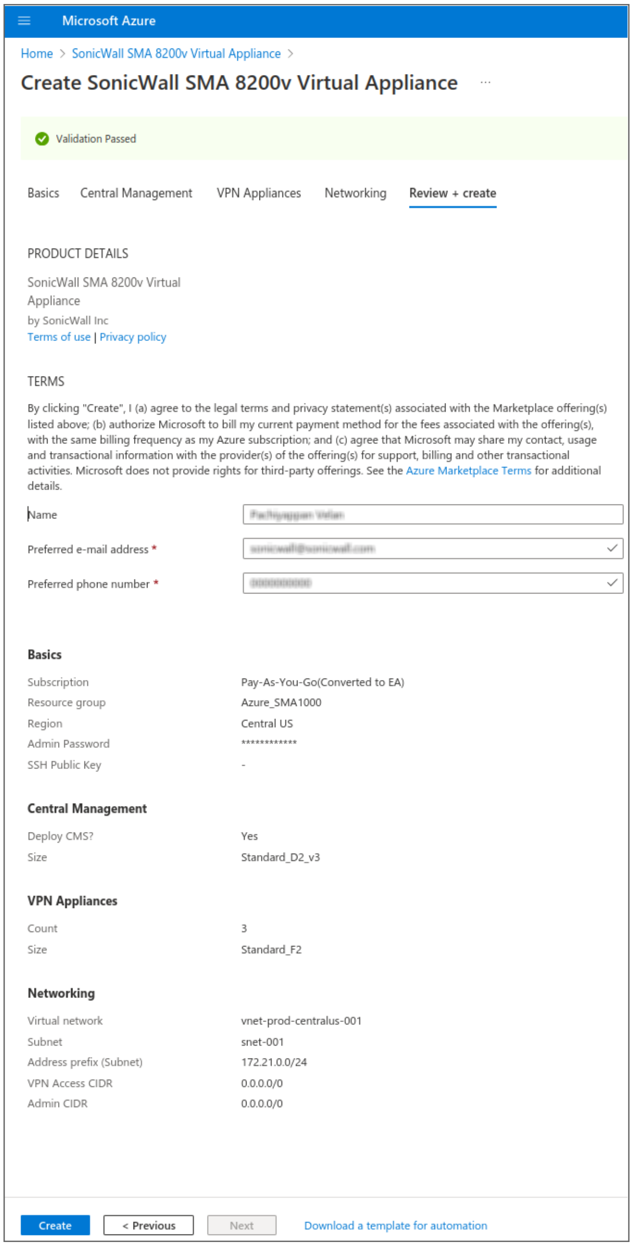
VPN Access CIDR * : 0.0.0.0/0

Admin CIDR * : 0.0.0.0/0

Review + create
< Previous
Next : Review + create >

16. Click **Next: Review + create >**.

The **Review + create >** page displays.



Create SonicWall SMA 8200v Virtual Appliance

Validation Passed

PRODUCT DETAILS

SonicWall SMA 8200v Virtual Appliance
by SonicWall Inc
Terms of use | Privacy policy

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Name	[redacted]
Preferred e-mail address *	[redacted]
Preferred phone number *	[redacted]

Basics

Subscription	Pay-As-You-Go(Converted to EA)
Resource group	Azure_SMA1000
Region	Central US
Admin Password	************
SSH Public Key	-

Central Management

Deploy CMS?	Yes
Size	Standard_D2_v3

VPN Appliances

Count	3
Size	Standard_F2

Networking

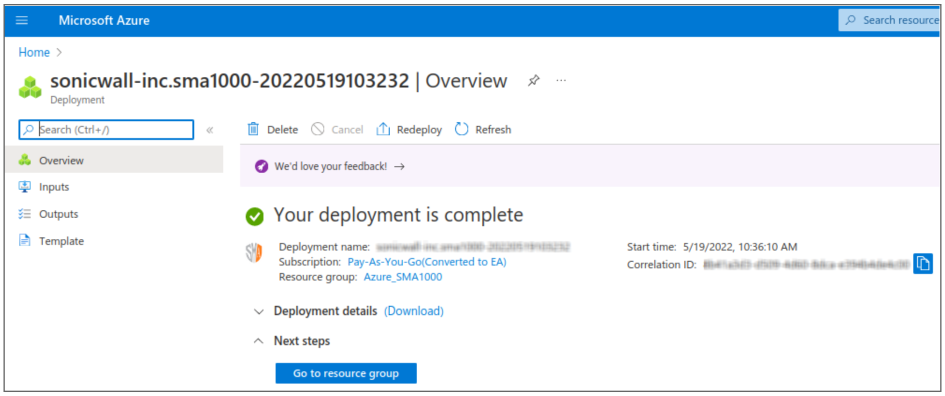
Virtual network	vnet-prod-centralus-001
Subnet	snet-001
Address prefix (Subnet)	172.21.0.0/24
VPN Access CIDR	0.0.0.0/0
Admin CIDR	0.0.0.0/0

17. Verify the instance details shown in the screen and click **Create**.

ⓘ **NOTE:** The SMA 8200v-standalone and CMS for Azure is automatically started at the end of the installation process.

A pop up screen with deployment status displays.

18. Once the deployment is complete, the following screen displays.



sonicwall-inc.sma1000-20220519103232 | Overview

Your deployment is complete

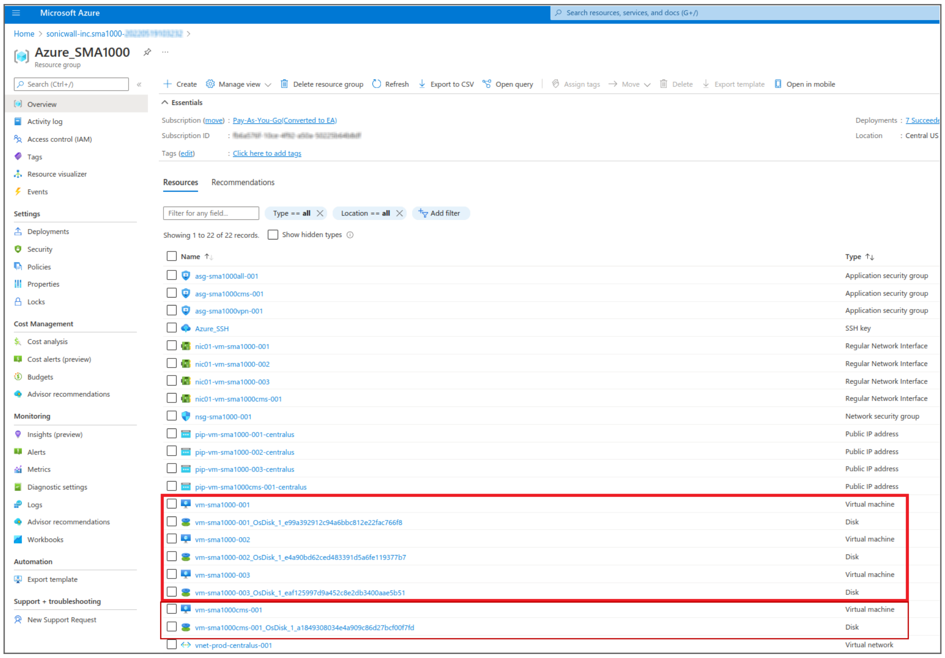
Deployment name: [redacted]
Subscription: Pay-As-You-Go(Converted to EA)
Resource group: Azure_SMA1000

Start time: 5/19/2022, 10:36:10 AM
Correlation ID: [redacted]

Deployment details (Download)

Next steps

19. Click **Go to resource group** and select the virtual machine that you want to manage.



Azure_SMA1000

Subscription (move) : Pay-As-You-Go(Converted to EA)
Subscription ID : [redacted]
Tags (edit) : Click here to add tags

Deployments : 7 Succeede
Location : Central US

Showing 1 to 22 of 22 records.

Name	Type
asg-sma1000all-001	Application security group
asg-sma1000cms-001	Application security group
asg-sma1000vpn-001	Application security group
Azure_SSH	SSH key
nic01-vm-sma1000-001	Regular Network Interface
nic01-vm-sma1000-002	Regular Network Interface
nic01-vm-sma1000-003	Regular Network Interface
nic01-vm-sma1000cms-001	Regular Network Interface
nsg-sma1000-001	Network security group
pip-vm-sma1000-001-centralus	Public IP address
pip-vm-sma1000-002-centralus	Public IP address
pip-vm-sma1000-003-centralus	Public IP address
pip-vm-sma1000cms-001-centralus	Public IP address
vm-sma1000-001	Virtual machine
vm-sma1000-001_OsDisk_1_e99a392912c94a6bbc812e22fac766f8	Disk
vm-sma1000-002	Virtual machine
vm-sma1000-002_OsDisk_1_e4a90bd62ced483391d5a6fe119377b7	Disk
vm-sma1000-003	Virtual machine
vm-sma1000-003_OsDisk_1_eaf125997d9a452c8e2db3400aae5b51	Disk
vm-sma1000cms-001	Virtual machine
vm-sma1000cms-001_OsDisk_1_a1849308034e4a909c86d27bcf00f7fd	Disk
vnet-prod-centralus-001	Virtual network

After the SMA 8200v-standalone and CMS instance is launched, you can access the appliance from a browser. See Connecting to the Web Interface for details.

Console access is available via the `ssh` command with the username 'admin' and the SSH key you specified during deployment. See Connecting to the Command Line Interface for details.

You are now ready to begin using your SMA 8200v-standalone and CMS appliance. See:

- Configuring SMA 8200v-Standalone and CMS on Azure
- Connecting to the Web Interface
- Using the 30-day Trial Version

Configuring SMA 8200v-Standalone and CMS on Azure

This section describes how to configure basic settings on the SMA 8200v-Standalone and CMS.

Topics:

- Viewing the SMA 8200v-Standalone and CMS Azure Settings
- Connecting to the Web Interface
- Connecting to the Command Line Interface
- Using the Command Line Interface

Viewing the SMA 8200v-Standalone and CMS Azure Settings

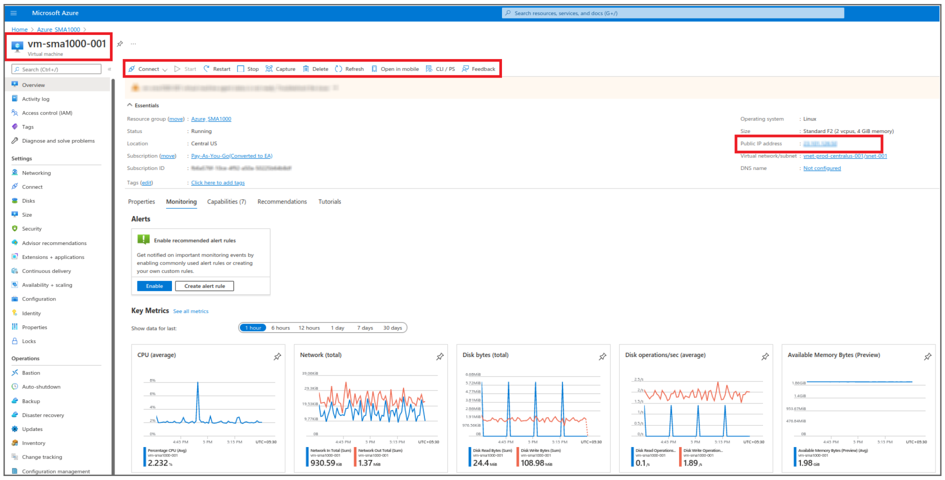
To display the SMA 8200v-standalone and CMS settings and virtual appliance controls:

1. Click **Virtual machines** in the Azure left pane.

   All the virtual machines in your account are displayed.

2. Click the SMA 8200v-standalone virtual machines to display the control and settings for it.

   The **Overview** page displays.



[redacted]

Resource group (move) : Azure_SMA1000
Status : Running
Location : Central US
Subscription (move) : Pay-As-You-Go(Converted to EA)
Subscription ID : [redacted]
Tags (edit) : Click here to add tags

Operating system : Linux
Size : Standard F2 (2 vcpus, 4 GiB memory)
Public IP address : [redacted]
Virtual network/subnet : vnet-prod-centralus-001/snet-001
DNS name : Not configured

Alerts

Enable recommended alert rules

Get notified on important monitoring events by enabling commonly used alert rules or creating your own custom rules.

Key Metrics

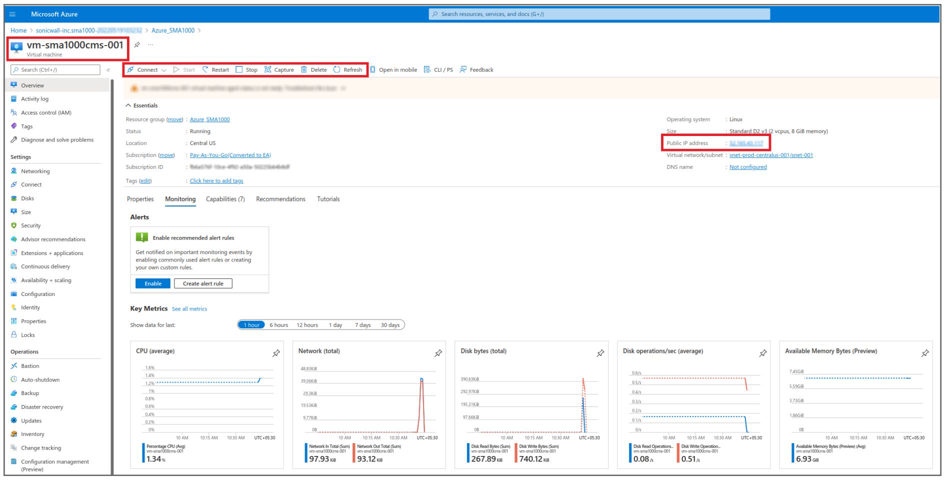
Show data for last: 1 hour

Percentage CPU (Avg) vm-sma1000-001: 2.232 %
Network In Total (Sum) vm-sma1000-001: 930.59 KiB
Network Out Total (Sum) vm-sma1000-001: 1.37 MiB
Disk Read Bytes (Sum) vm-sma1000-001: 24.4 MiB
Disk Write Bytes (Sum) vm-sma1000-001: 108.98 MiB
Disk Read Operations... vm-sma1000-001: 0.1 /s
Disk Write Operation... vm-sma1000-001: 1.89 /s
Available Memory Bytes (Preview) (Avg) vm-sma1000-001: 1.98 GiB

   The SMA 8200v-standalone for Azure is automatically started at the end of the installation process.

3. Click the CMS virtual machines to display the control and settings for it.

The **Overview** page displays.



[redacted]

Resource group (move) : Azure_SMA1000
Status : Running
Location : Central US
Subscription (move) : Pay-As-You-Go(Converted to EA)
Subscription ID : [redacted]
Tags (edit) : Click here to add tags

Operating system : Linux
Size : Standard D2 v3 (2 vcpus, 8 GiB memory)
Public IP address : [redacted]
Virtual network/subnet : vnet-prod-centralus-001/snet-001
DNS name : Not configured

Get notified on important monitoring events by enabling commonly used alert rules or creating your own custom rules.

The CMS for Azure is automatically started at the end of the installation process.

To stop, restart, or start the SMA 8200v-Standalone and CMS for Azure:

1. Navigate to the **Overview** page as described in Viewing the SMA 8200v-Standalone and CMS Azure 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 also available here, including **Connect**, **Capture**, **Move**, **Delete**, and **Refresh**.

Connecting to the Web Interface

The SMA 8200v-standalone and CMS for Azure is accessible at the public IP address automatically assigned by Azure using DHCP addressing.

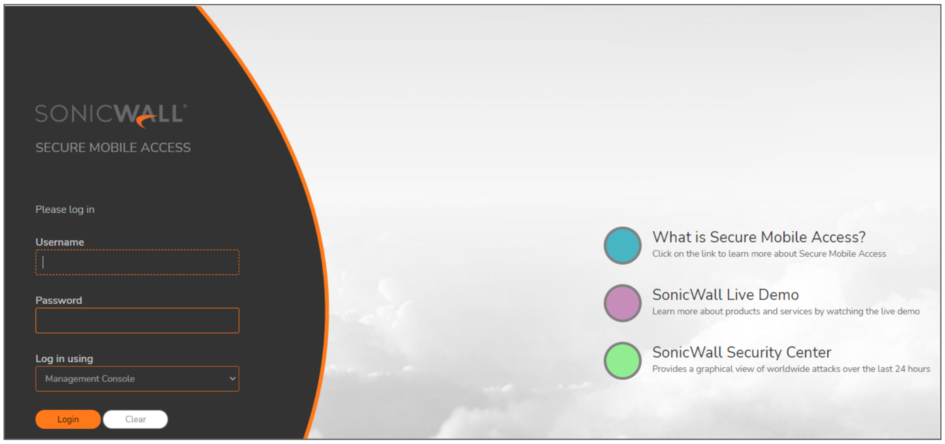
ⓘ **NOTE:** The IP address of the internal interface and external interface cannot be changed on a cloud-based appliance and also in SMA UI or API.

To connect to the SMA 8200v-Standalone and CMS for Azure:

1. Navigate to the **Overview** page of your appliance as described in Viewing the SMA 8200v-Standalone and CMS Azure Settings.
2. Locate the **Public IP address**.
3. In a browser, enter the public IP address using https.
   a. Use default port 8443 to access SMA 8200v-standalone appliance. For example : *https://<SMA 8200v Public IP>:8443/*

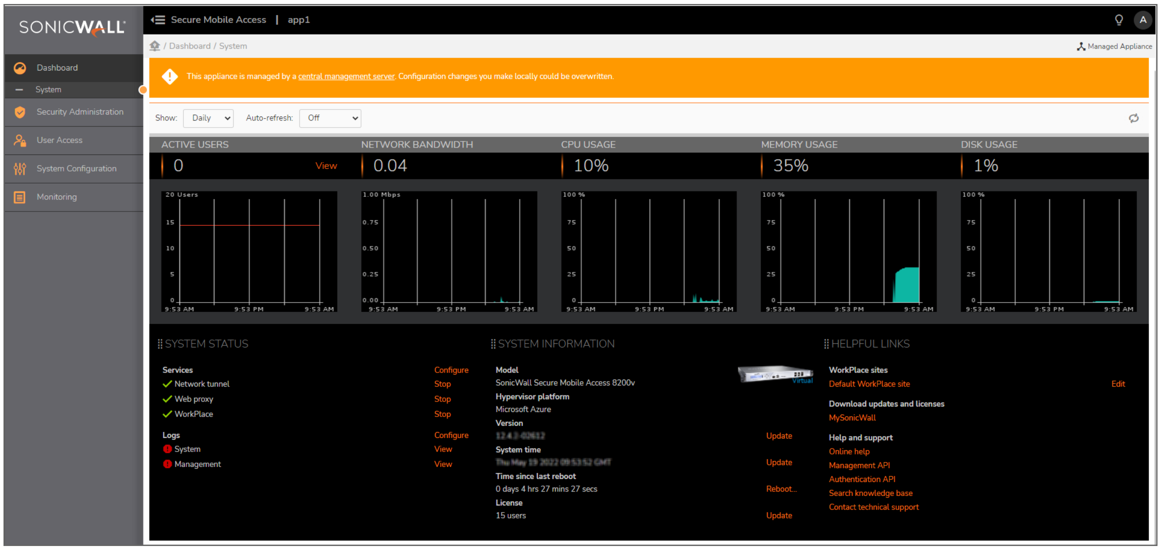
b. Use default port 8443 to access CMS. For example : *https://<SMA CMS Public IP>:8443/*

4. In the SMA 8200v-standalone and CMS for Azure login screen, enter the username 'admin' and the password specified during deployment and then click **Login**.



SONICWALL
SECURE MOBILE ACCESS
Please log in
Username
Password
Log in using
Management Console
Login
Clear
What is Secure Mobile Access?
Click on the link to learn more about Secure Mobile Access
SonicWall Live Demo
Learn more about products and services by watching the live demo
SonicWall Security Center
Provides a graphical view of worldwide attacks over the last 24 hours

The SMA 8200v-standalone **Dashboard** page displays.



This appliance is managed by a central management server. Configuration changes you make locally could be overwritten.

Show: Daily Auto-refresh: Off

ACTIVE USERS	NETWORK BANDWIDTH	CPU USAGE	MEMORY USAGE	DISK USAGE
0 View	0.04	10%	35%	1%

SYSTEM STATUS

Services — Configure
✓ Network tunnel — Stop
✓ Web proxy — Stop
✓ WorkPlace — Stop

Logs — Configure
● System — View
● Management — View

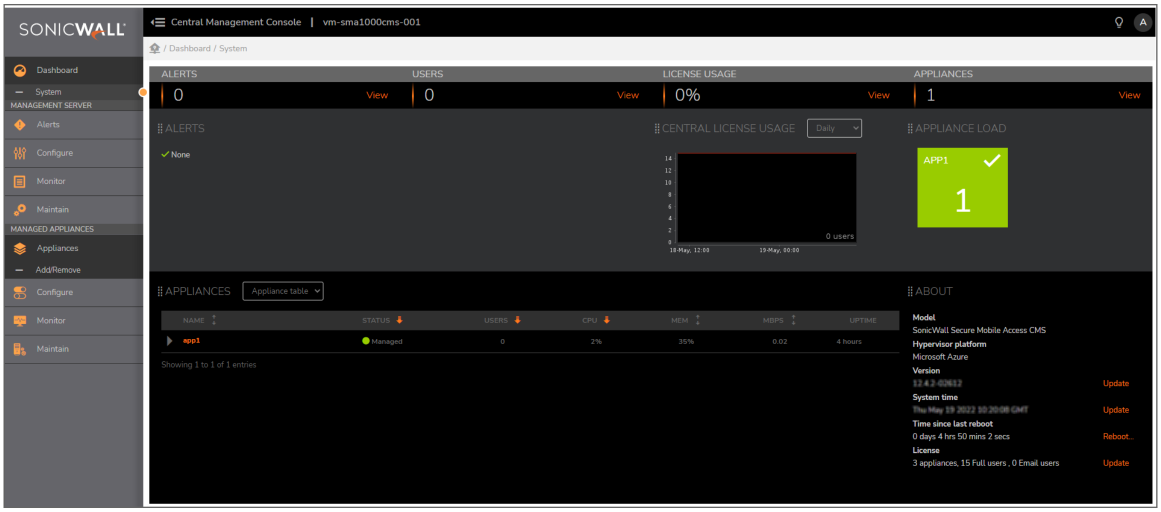
SYSTEM INFORMATION

Model
SonicWall Secure Mobile Access 8200v
Hypervisor platform
Microsoft Azure
Version
[redacted] — Update
System time
[redacted] — Update
Time since last reboot
0 days 4 hrs 27 mins 27 secs — Reboot...
License
15 users — Update

HELPFUL LINKS

WorkPlace sites
Default WorkPlace site — Edit
Download updates and licenses
MySonicWall
Help and support
Online help
Management API
Authentication API
Search knowledge base
Contact technical support

The CMS **Dashboard** page displays.



NAME	STATUS	USERS	CPU	MEM	MBPS	UPTIME
app1	Managed	0	2%	35%	0.02	4 hours

Showing 1 to 1 of 1 entries

Model
SonicWall Secure Mobile Access CMS
Hypervisor platform
Microsoft Azure
Version
[redacted] Update
System time
[redacted] Update
Time since last reboot
0 days 4 hrs 50 mins 2 secs Reboot...
License
3 appliances, 15 Full users , 0 Email users Update

To register the SMA 8200v-standalone and CMS for Azure and begin management and configuration, see Registering the SMA 8200v-Standalone and CMS.

Connecting to the Command Line Interface

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

ⓘ **NOTE:** SSH connections as root are not supported on cloud instances. For root access, connect as 'admin' and then enter `sudo su`.

To connect to SMA 8200v-Standalone and CMS over SSH:

1. Navigate to the **Overview** page as described in Viewing the SMA 8200v-Standalone and CMS Azure Settings.
2. Locate the **Public IP address**.

   SMA 8200v-standalone: `<SMA 8200v Public IP/ Host name>`

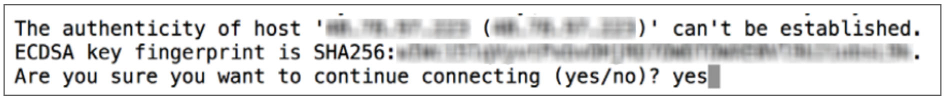
   CMS: `<SMA CMS Public IP/ Host name>`
3. In an SSH application, type in the command using your Azure private key to authenticate:

   `ssh -i AzurePrivateKey.key admin@<SMA 8200v Public IP/ Host name>` - To connect SMA 8200v-standalone.

   `ssh -i AzurePrivateKey.key admin@<SMA CMS Public IP/ Host name>` - To connect CMS.

   For example, `ssh -i xxxxkey.pem admin@xx.xx.xx.xx/Host name`.

   ⓘ | **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 '[redacted] ([redacted])' can't be established.
ECDSA key fingerprint is SHA256:[redacted].
Are you sure you want to continue connecting (yes/no)? yes
```

5. Continue to Using the Command Line Interface.

Using the Command Line Interface

The CLI is a text-only mechanism for interacting with the SMA 8200v-standalone and CMS for Azure virtual appliance by typing commands to perform specific tasks. The CLI is launched as described in Connecting to the Command Line Interface.

Type in the commands to perform the tasks on SMA 8200v-standalone appliance and CMS.

4

Licensing and Registering Your Appliance

This section contains information about licensing and registering your SMA 8200v-standalone and CMS for Azure Virtual Appliance.

You must purchase a license and register your SMA 8200v-standalone and CMS on Azure before first use. Registration is performed using the management interface. After the registration is completed, the SMA 8200v-standalone and CMS on Azure is licensed and ready to use. For the 30-Day Trial Virtual Appliance registration process, refer to Using the 30-day Trial Version.

SMA 8200v-standalone and CMS on 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 8200v-standalone for Azure Virtual Appliance management interface, on the **System Configuration > General Settings > Licensing** page.

License status is displayed in the CMS for Azure Virtual Appliance management interface, on the **Management Server> Configure> General Settings > Licensing** page.

Communication with the SonicWall Licensing Manager is necessary while using the SMA 8200v-standalone and CMS on Azure and requires Internet access.

Registering the SMA 8200v-Standalone and CMS

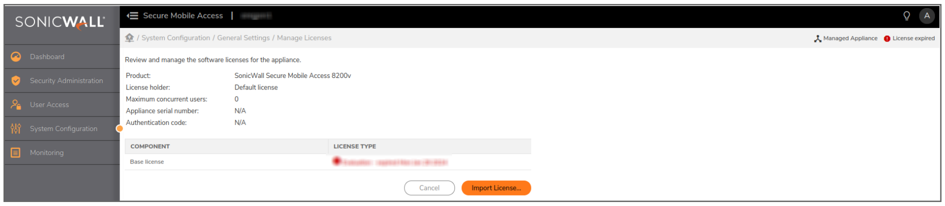
After you have installed and configured the network settings for your SMA 8200v-standalone and CMS on Azure, you can log into the management console and register it to your MySonicWall account. Registration of your SonicWall SMA 8200v-standalone and CMS on Azure follows the same process as for other SonicWall hardware-based appliances.

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

To register your SMA 8200v-standalone for Azure:

1. Log in to your SMA 8200v-standalone virtual machine.
2. In the **System Configuration** group, select **General Settings > Licensing > Edit**.

   The **Manage Licenses** page is displayed.

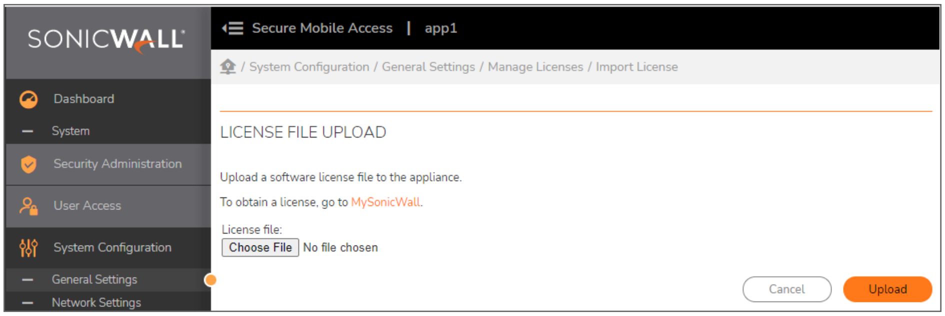


Review and manage the software licenses for the appliance.

Product: SonicWall Secure Mobile Access 8200v
License holder: Default license
Maximum concurrent users: 0
Appliance serial number: N/A
Authentication code: N/A

COMPONENT	LICENSE TYPE
Base license	[redacted]

3. In the **Manage Licenses** page, click **Import License**.
4. In the **Import License** page, click **Choose File** to select the license file and click **Upload**.



LICENSE FILE UPLOAD

Upload a software license file to the appliance.

To obtain a license, go to MySonicWall.

License file: No file chosen

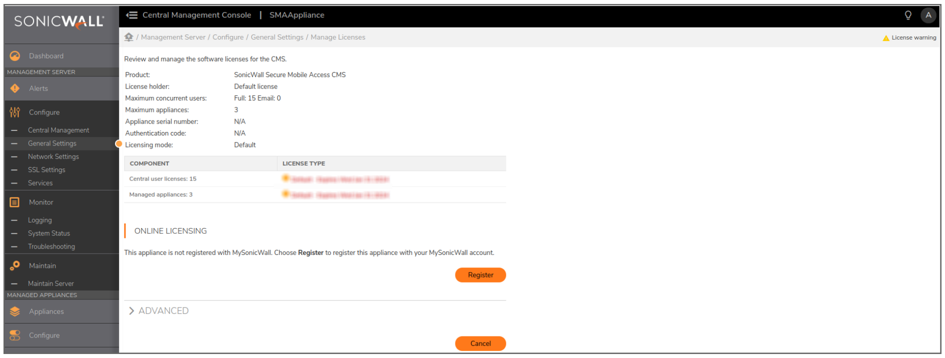
   The License file is uploaded into the appliance.

5. You have successfully registered your SMA 8200v-standalone virtual machine. Click **Continue** to view the **License Management** screen or continue configuring other settings within the appliance.

To register your CMS for Azure:

1. Log in to your CMS virtual machine.
2. In the **Management Server** group, select **Configure > General Settings > Licensing > Edit**.

   The **Manage Licenses** page is displayed.



Review and manage the software licenses for the CMS.

Product: SonicWall Secure Mobile Access CMS
License holder: Default license
Maximum concurrent users: Full: 15 Email: 0
Maximum appliances: 3
Appliance serial number: N/A
Authentication code: N/A
Licensing mode: Default

COMPONENT	LICENSE TYPE
Central user licenses: 15	[redacted]
Managed appliances: 3	[redacted]

ONLINE LICENSING

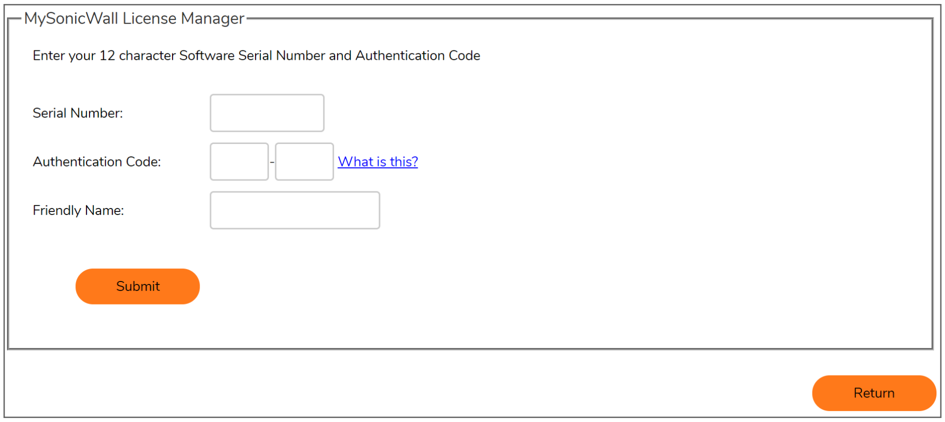
This appliance is not registered with MySonicWall. Choose **Register** to register this appliance with your MySonicWall account.

3. In the **Manage Licenses** page, under **Online Licensing**, click **Register**.

   This should take you to a MySonicWall login.

4. Enter your MySonicWall.com account username or email address and password in the appropriate fields and click **Submit**.

5. In the **License Management** page, enter the **Serial Number** or **Activation Key** for your new appliance. Enter the **Authentication Code** for your new appliance.



MySonicWall License Manager

Enter your 12 character Software Serial Number and Authentication Code

Serial Number:

Authentication Code: - What is this?

Friendly Name:

6. Enter a **Friendly Name**.

7. Click **Submit** to finish the registration process.

8. You have successfully registered your CMS virtual machine. Click **Continue** to view the **License Management screen** or continue configuring other settings within the appliance.

5

Using the 30-day Trial Version

The SMA 8200v-standalone and CMS for Azure 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 8200v-standalone and CMS, except for differences noted in Deployment Considerations section. 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 8200v-standalone and CMS for Azure.
- Export your settings from the 30-day Trial version.
- Install and register the full SMA 8200v-standalone and CMS for Azure.
- Import your settings.

You must install the SMA 8200v-standalone and CMS for Azure software before registering for your 30-Day Trial. For more information on obtaining the software, see Installing SMA 8200v-Standalone and CMS on Azure.

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 8200v-standalone and CMS for Azure is disabled after 30 days.
- A maximum of two concurrent users are allowed to log into the appliance.
- Communication with the SonicWall Licensing Manager is required during the entire trial period.
- It is recommended that you save a copy of your appliance configuration settings before upgrading to the full version of the SMA 8200v-standalone and CMS for Azure.

Registering the 30-day Trial Virtual Appliance

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

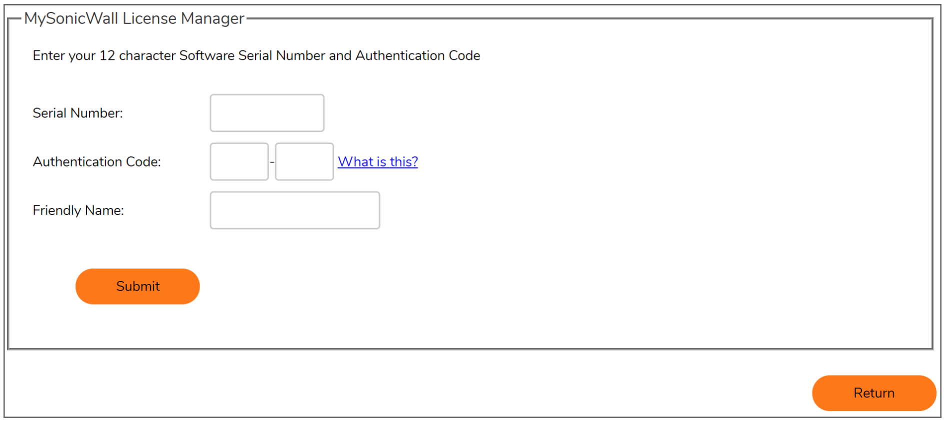
ⓘ **NOTE:** Before starting the registration process, contact SonicWall Sales to obtain your serial number and authorization code.

To register the 30-day Trial:

1. Log in to your SMA 8200v-standalone for Azure.
2. In the **System Configuration** group, select **General Settings > Licensing > Edit**.

   The **Manage Licenses** page displays.
3. Log in to your CMS for Azure.
4. In the **Management Server** group, select **Configure> General Settings > Licensing > Edit**.

   The **Manage Licenses** page displays.
5. Under **Online Licensing**, click **Register.** This should take you to a MySonicWall login.
6. Enter your MySonicWall.com account username or email address and password in the appropriate fields and click **Submit.**
7. In the **License Management** page, enter the **Serial Number** or **Activation Key** for your new appliance. Enter the **Authentication Code** for your new appliance.



MySonicWall License Manager

Enter your 12 character Software Serial Number and Authentication Code

Serial Number:

Authentication Code: - What is this?

Friendly Name:

8. Enter a **Friendly Name**.
9. Click **Submit** to finish the registration process.
10. You have successfully registered your SMA 8200v-standalone and CMS for Azure. Click **Continue** to view the **License Management** screen or continue configuring other settings within the appliance.
11. Click **Login**.
12. When the registration confirmation page displays, click **Continue**.

Converting a Free Trial License to Full License

An SMA 8200v-standalone and CMS for Azure instance is installed as a 30-day free trial can easily be converted to a full production license.

To convert your free trial to a production version:

1. Purchase an SMA 8200v-standalone and CMS for Azure license from a distributor. You should receive a fulfillment email with the new serial number and authentication code.
2. For SMA 8200v-standalone, In the **System Configuration** group, select **General Settings > Licensing > Edit**.

   The **Manage Licenses** page displays.
3. For CMS, In the **Management Server** group, select **Configure> General Settings > Licensing > Edit**.

   The **Manage Licenses** page displays.
4. In MySonicWall, click to **Register** a new instance.
5. Enter the **Serial Number** and **Authentication Code** you received after purchasing your SMA 8200v-standalone and CMS for Azure instance. Your SMA 8200v-standalone and CMS for Azure is now registered.

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your SMA 8200v-standalone and CMS for Azure configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your SMA 8200v-standalone and CMS for Azure, protecting all your existing settings in the event that it becomes necessary to return a previous configuration state.

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

Go to **AMC > Maintenance > Import/ Export** and save the settings file to your local machine. The default settings file is named *<SMAHostName>_12.4.3-<buildnumber>_<current date>-<current time>.aea*.

Go to **CMS > Management Server > Maintain Server > Maintenance > Import/ Export** and save the settings file to your local machine. The default settings file is named *<SMAHostName>_12.4.3-<buildnumber>_<current date>-<current time>.aea*.

6

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

Secure Mobile Access SMA and CMS on Azure Getting Started Guide
Updated - January 2024
Software Version - 12.4
232-005705-00 Rev C

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