



Secure Mobile Access on KVM 12.4

Getting Started Guide

SONICWALL®

Contents

| | |
|-------------------------------------------------------------|-----------|
| Introducing SMA 8200v for KVM | 3 |
| Installation File / Supported Platforms | 3 |
| KVM/QEMU | 3 |
| Hardware-Assisted Full Virtualization | 4 |
| Paravirtualization | 4 |
| Creating a MySonicWall Account | 4 |
| Installing SMA 8200v on KVM | 6 |
| Preparing the Linux Server System | 6 |
| Obtaining the SMA 8200v Image | 6 |
| Installing the SMA 8200v on Red Hat / Ubuntu-KVM/QEMU | 7 |
| Licensing and Registering Your SMA Appliance | 21 |
| Registering the SMA Appliance | 21 |
| Verifying the Installation | 22 |
| Using the Virtual Console | 24 |
| SonicWall Support | 26 |
| About This Document | 27 |

Introducing SMA 8200v for KVM

This Getting Started Guide describes how to install SonicWall SMA 8200v on Linux with KVM and QEMU environments and provides basic configuration information.

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 SMA 8200v (1000) series. The SMA 8200v gives you economy-of-scale benefits of virtualization. This gives you all the security advantages of a physical SMA appliance with the operational and economic benefits of virtualization, including system scalability and agility, speed of system provisioning, simple management and cost reduction.

Installation File / Supported Platforms

| Release Version | Supported Linux / Kernel / KVM / VMM Versions |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMA 8200v for Linux KVM/QEMU | Red Hat 8.x (latest) |
| | <ul style="list-style-type: none"> • Kernel: x86/x64 with kernel level 4.X or later • KVM version: 2.11.1 • Virtual machine manager: 1.5.1 |
| | Ubuntu 18.04 |
| | <ul style="list-style-type: none"> • Kernel: 5.4.0-51-generic • KVM version: 2.11.1 • Virtual machine manager: 1.5.1 |

KVM/QEMU

KVM, or Kernel-based Virtual Machine is a software module that allows Linux to operate as a hypervisor. QEMU, or Quick Emulator, allows guest operating systems to run on the KVM hypervisor and supports virtualization where applications executing in the user space can achieve near native speeds through full virtualization or paravirtualization.

Hardware-Assisted Full Virtualization

KVM features hardware-assisted full virtualization when the underlying x86 processor hardware supports Intel VT-x or AMD-V virtualization extensions. This allows SMA appliance to setup a virtual context and execute instructions directly on the processor's hardware.

For an overview of virtualization techniques, see: <https://www.unixarena.com/2017/12/para-virtualization-full-virtualization-hardware-assisted-virtualization.html/>

Paravirtualization

In hardware-assisted full virtualization, guest operating systems issue calls directly to the hardware. In paravirtualization, guest operating systems communicate with the hypervisor (KVM/QEMU) with an API (Virtio). This API defines paravirtual devices including Ethernet cards, disk I/O subsystems, and VGA interfaces with SPICE drivers.

For an overview of VirtIO, see https://www.cs.cmu.edu/~412/lectures/Virtio_2015-10-14.pdf.

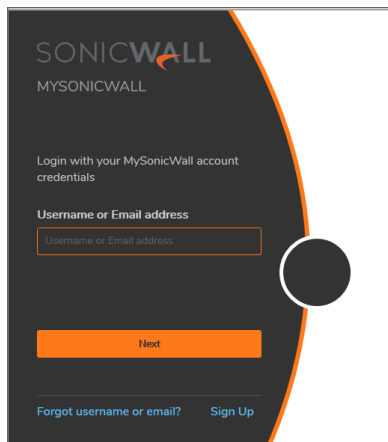
Creating a MySonicWall Account

A MySonicWall account is required to obtain the image file for initial installation of the SMA virtual appliance, for product registration to enable full functionality of SonicOS features, and for access to licensed security services. For a High Availability configuration, MySonicWall provides a way to associate a secondary SMA virtual appliance that can share security service licenses with your primary appliance.

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

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.



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. If you are using Microsoft or Google authenticator, scan the code or confirm authentication with a button.
15. Click **Done**.
You are returned to the login window so you can login into MySonicWall with your new account.

Installing SMA 8200v on KVM

Topics:

- [Preparing the Linux Server System](#)
- [Obtaining the SMA 8200v Image](#)
- [Installing the SMA 8200v on Red Hat / Ubuntu-KVM/QEMU](#)

Preparing the Linux Server System

Before installing SonicWall SMA 8200v on a Linux server, prepare the server:

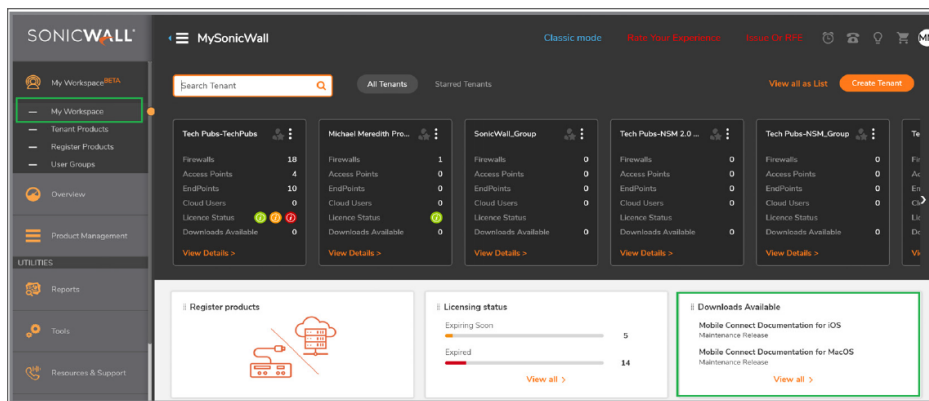
- Install Red Hat or Ubuntu on the server.
- Install KVM and QEMU on server.
- Connect the Linux Server system to an external switch.

Obtaining the SMA 8200v Image

After purchasing SMA 8200v, you will receive an email with a serial number and Authentication Code. Log into mysonicwall.com (refer to [Creating a MySonicWall Account](#)) and navigate to the Download Center.

To download image:

1. Login to MySonicWall.com and then navigate to **My Workspace > Downloads Available**.

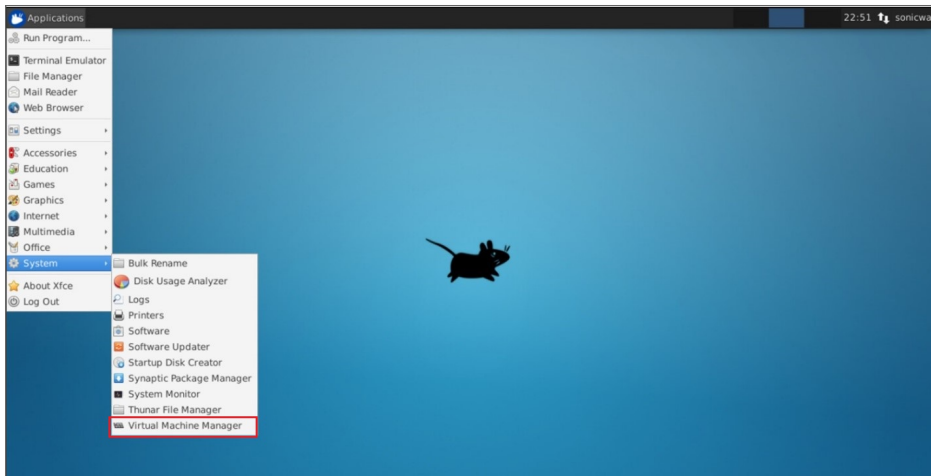


2. Click **View All**. The list of available downloads is displayed.
3. Identify the SMA 8200v product and click on the title; when the details appear, click on the download icon.
4. Keep the Serial number and Authentication code from the purchase confirmation email to complete product registration after the virtual firewall is installed.

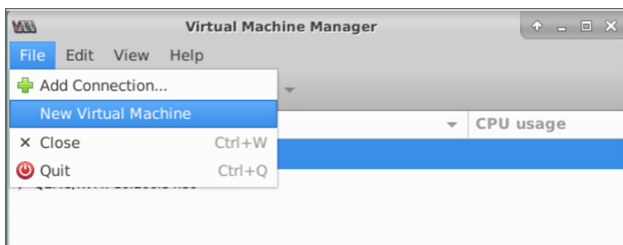
Installing the SMA 8200v on Red Hat / Ubuntu-KVM/QEMU

To install SMA 8200v on Ubuntu-KVM/QEMU:

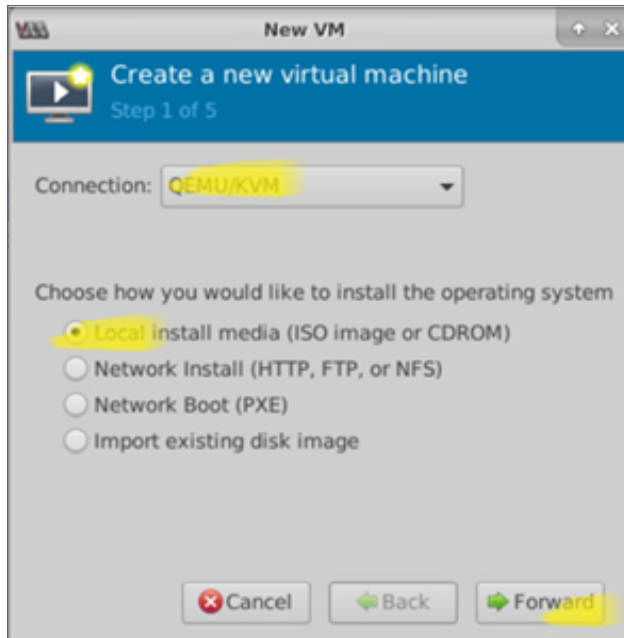
1. Download the SMA 8200v **qcow2** or **iso** file to a local folder in the Linux Server system.
2. Copy image file (for example: "12.4.x-xxxx.qcow2 or 12.4.x-xxxx.iso") into the directory **/var/lib/libvirt/images/**
3. Launch the Virtual Machine Manger (VMM) utility 1.5.1 or higher on Linux machine.



4. Create a VM in the Virtual Machine Manager to receive the image file. To create a VM, click **File** and select **New Virtual Machine** option.



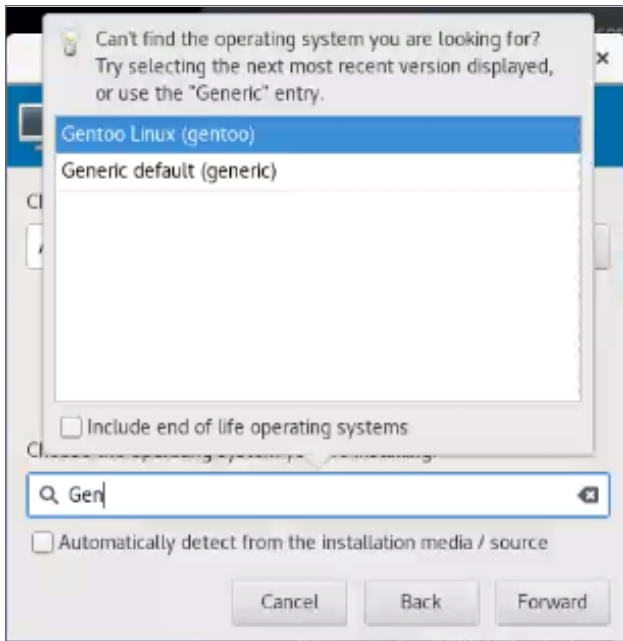
5. In the **Step 1** screen, start creating a new virtual machine ,choose the **Connection** as desired by user based on Ubuntu or Red hat kernel.
 - Select the **Local install media (ISO image or CDROM)** option to browse the **.iso** file as installation media for installing operating system and click **Forward** to next screen.



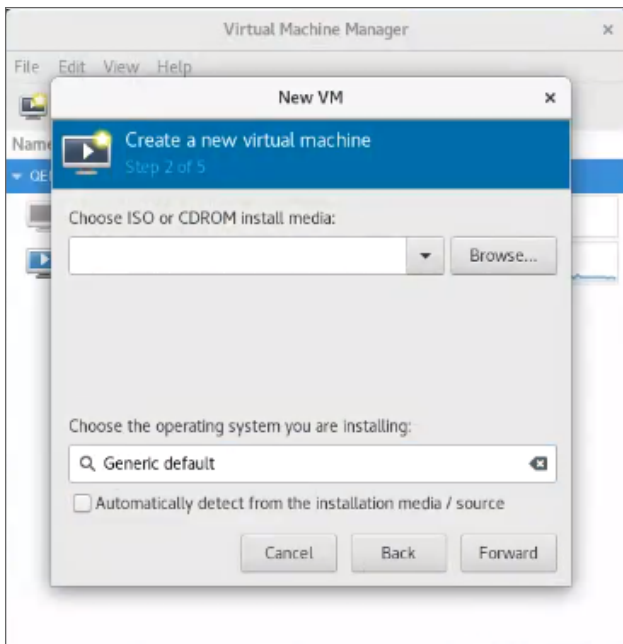
- Select the **Import existing disk image** option to browse the **.qcow2** image file for installing operating system and click **Forward** to next screen.



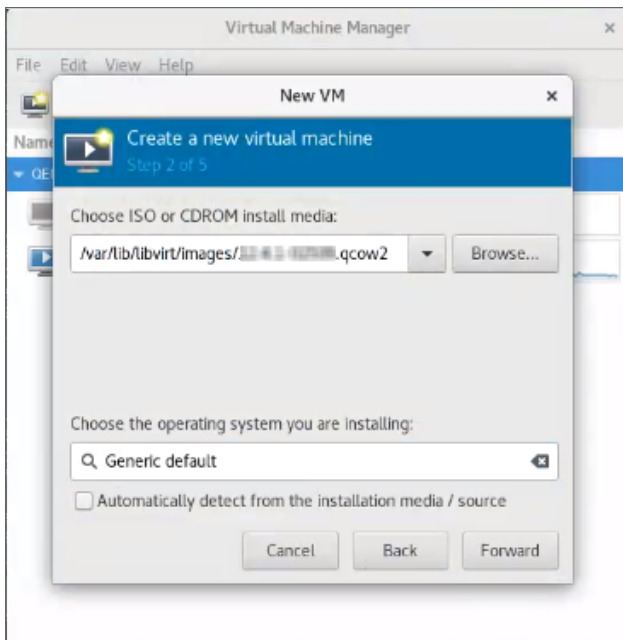
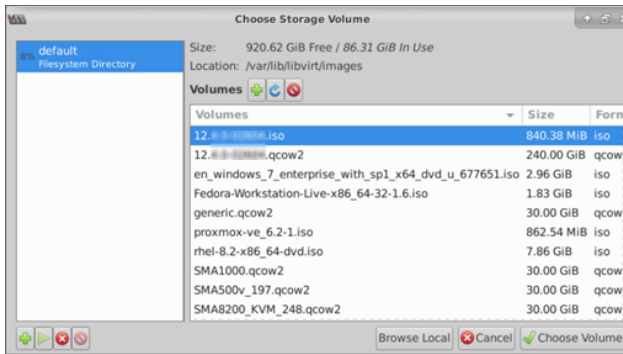
6. In the **Step 2** screen, enter **Gen** and select **Generic default (generic)** option in the text box next to **Choose the operating system you are installing** field.



7. In the **Step 2** screen, click **Browse** to locate the Installation media.



8. Select the installation media as **.qcow2** and click **Choose volume** in the **Choose Storage Volume** screen.

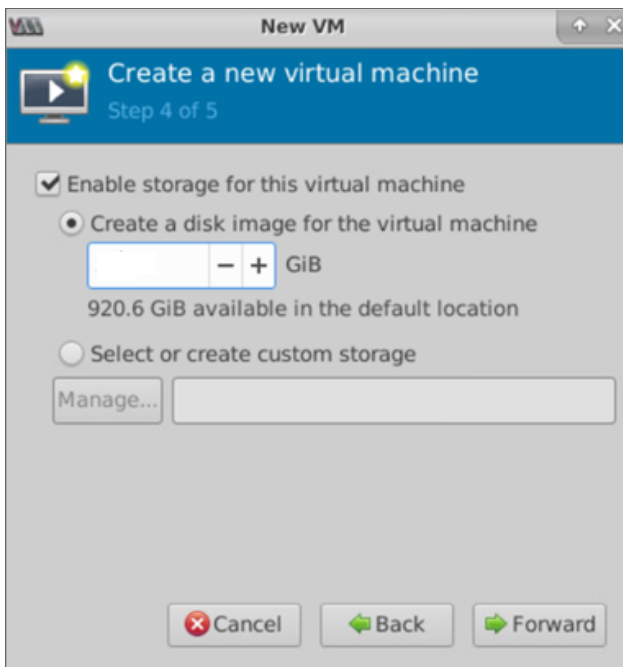


Click **Forward** for next screen.

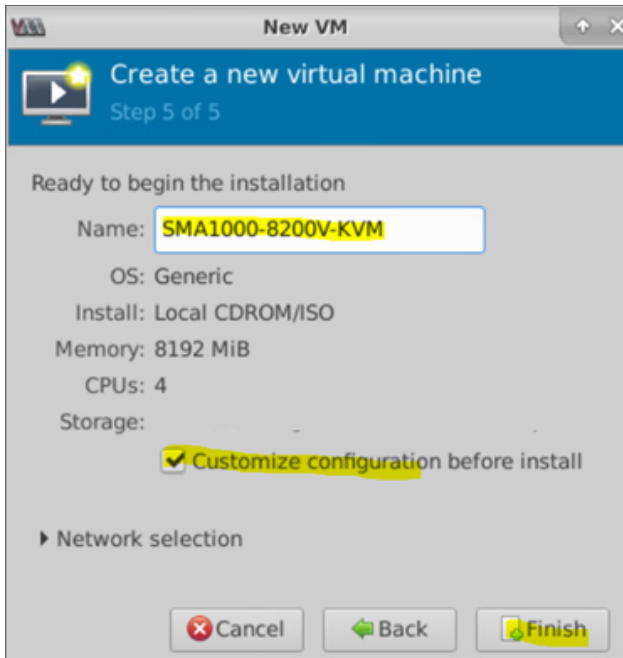
- In the **Step 3** screen, set the Memory and CPU settings, click **Forward**.
- ① | **NOTE:** The recommended Memory is 8 GB (8192 MiB) and CPUs to be set as 4.



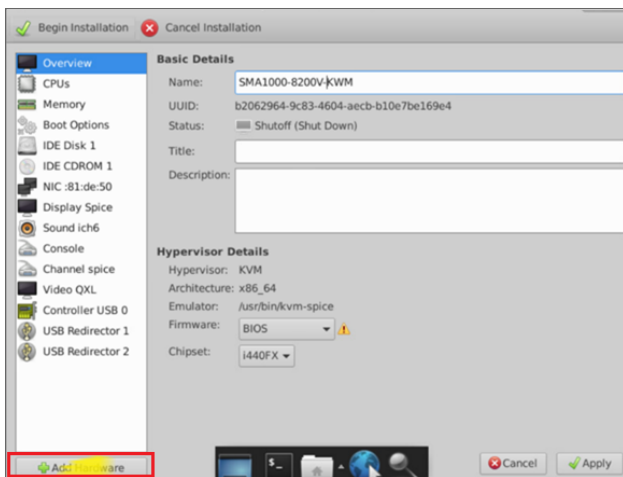
- In the **Step 4** screen, set the disk image for the virtual machine.
① | **NOTE:** The recommended volume is 250 GB.



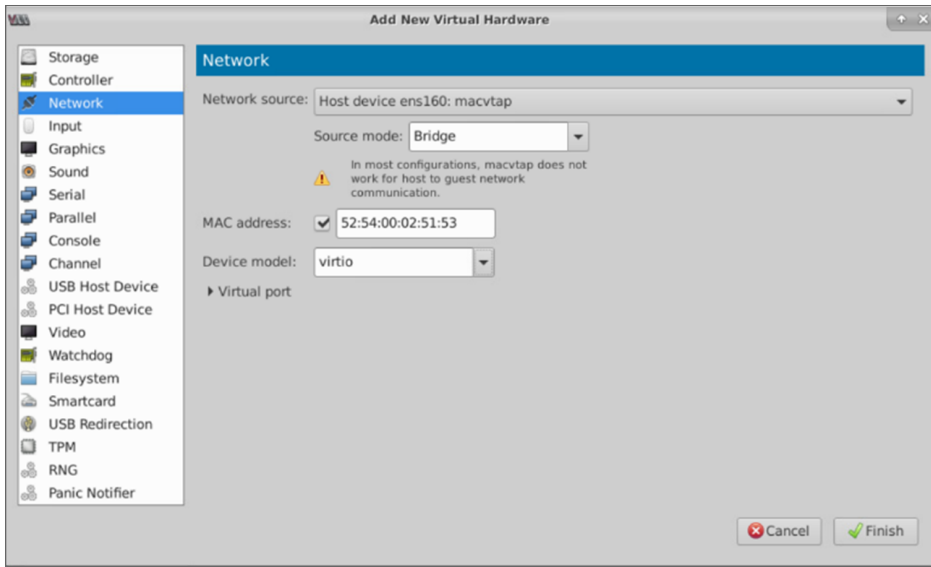
- In the **Step 5** screen, enter the desired name for the virtual machine and enable **Customize configuration before install** option.



12. In the **Step 5** screen, click **Finish**.
13. Click **Add Hardware** to deploy additional NIC for X0 and X1.



14. Select the desired network interface for X0 and X1 under **Network** option and set the **Device model** to "virtio".

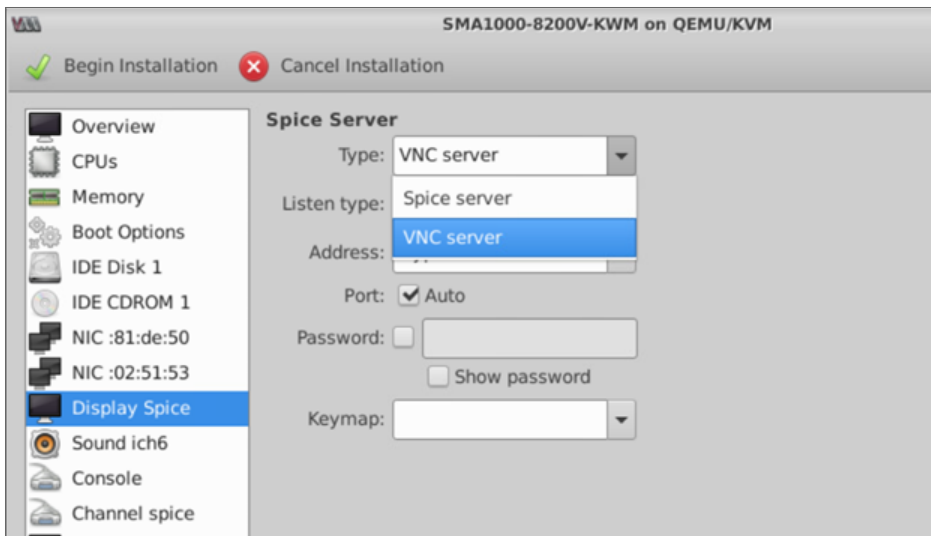


① **NOTE:** By choosing virtio, the VirtIO API is enabled. For more details on VirtIO, see [Paravirtualization](#).

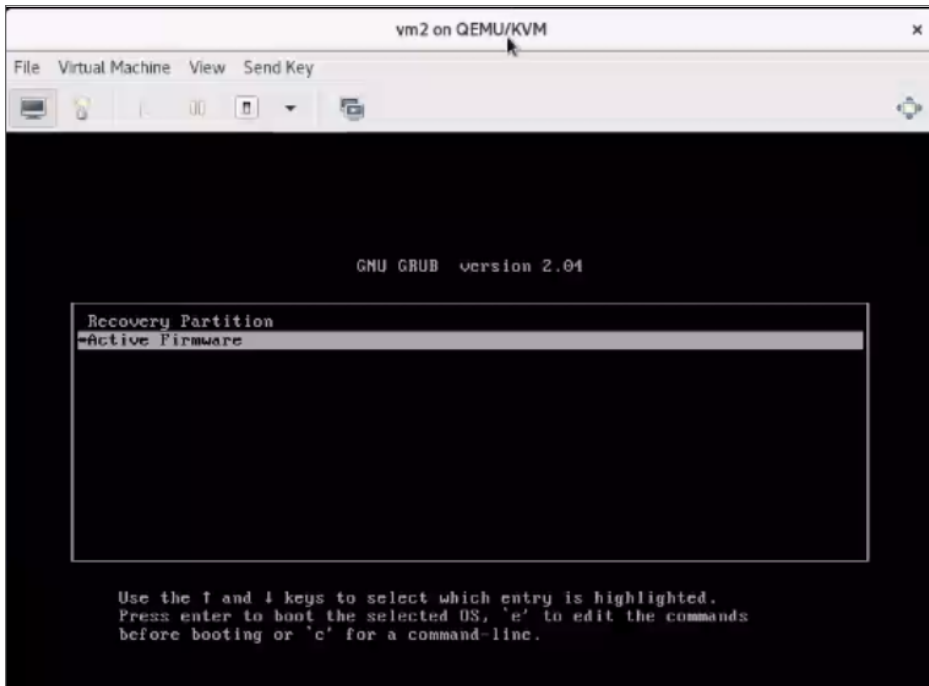
15. Click **Finish**.

16. Select **Display Spice** option and create a new VM with the **Type** set as **VNC server**. Otherwise you may not be able to use the keyboard with the new VM.

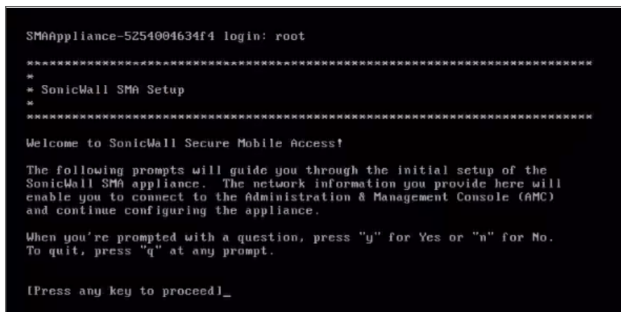
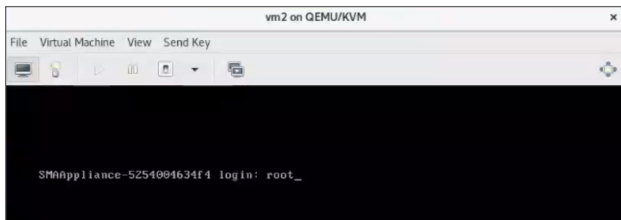
① **NOTE:** In the above dialog box, **Spice** refers to the Simple Protocol for Independent Computing Environment. In this context a Spice Display is one that can be accessed remotely through a standard protocol.



17. Click on **Begin Installation** to deploy SMA1000 8200v on KVM.
The Virtual machine is created.



18. Log in as a **root** user.



19. Run through the setup tool for setting up X0 Network interface for Administration access.

```
File Virtual Machine View Send Key
[Icons]

When you're prompted with a question, press "y" for Yes or "n" for No.
To quit, press "q" at any prompt.

[Press any key to proceed]

INTERNAL INTERFACE CONFIGURATION

Please enter network settings for the internal interface (labeled
"2" on the appliance). If you are on the same network as the appliance,
press ENTER when prompted for a gateway.

IP address: 192.168.1.100
Subnet mask: 255.255.0.0
Gateway: 192.168.0.1

Please review the information you provided. Press ENTER to accept the
current value, otherwise enter a new value.

IP address: 192.168.1.100:
Subnet mask: 255.255.0.0:
Gateway: 192.168.0.1:

Do you want to save and apply the configuration settings? (y)
```

```
File Virtual Machine View Send Key
[Icons]

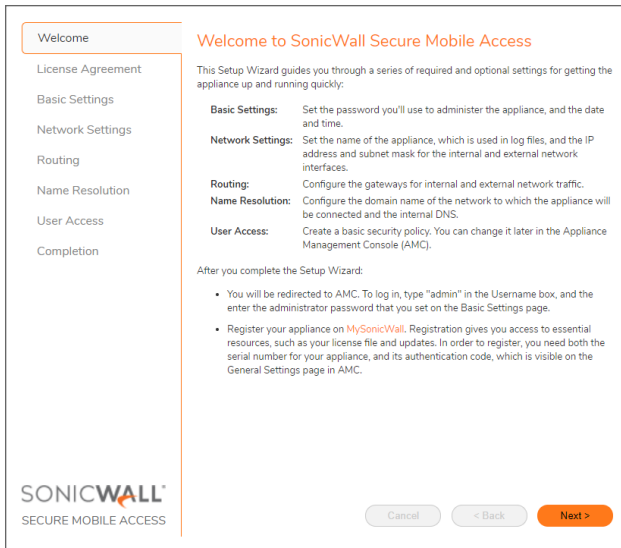
[ ok ] Stopping Appliance Management Console...done.
start-stop-daemon: matching on world-writable pidfile /var/run/zeroconf_beacon.p
id is insecure
Stopping Apple Darwin Multicast DNS / DNS Service Discovery daemon: mdnsd.
Killed old client process
[ ok ] Probing for network drivers... virtio_net e1000 e1000e.
Applying...
Stopping Apple Darwin Multicast DNS / DNS Service Discovery daemon: mdnsd.
[ ok ] Stopping MariaDB: mysqld.
[ ok ] Starting MariaDB: mysqld.
[ ok ] Stopping syslog-ng server...done.
[ ok ] Starting syslog-ng server...done.
[ ok ] Starting Appliance Management Console...done.
.....
Internal network interface configured
IP address: 192.168.1.100
Subnet mask: 255.255.0.0
Gateway: 192.168.0.1

Setup complete!

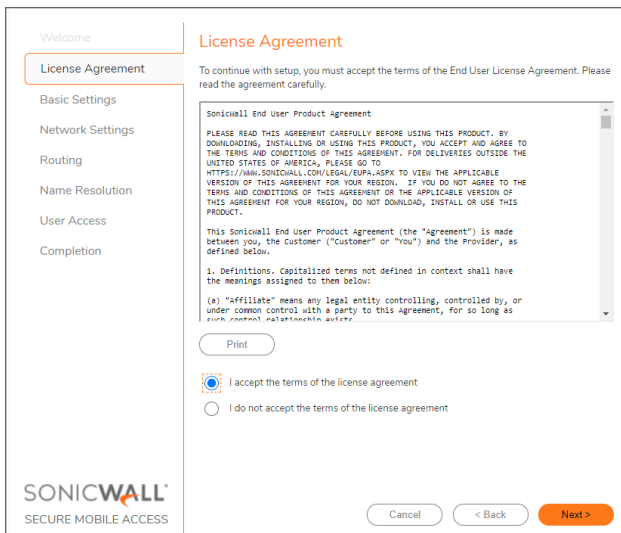
To continue configuring the appliance, connect to https://192.168.1.100.
See the product documentation for more information.

[Press any key to proceed]
```

- 20. Run through setup wizard for X1 Network interface for Workplace access. In the **Welcome** screen, click **Next**.



21. In the **License Agreement** screen, select **I accept the terms of the license agreement** option and click **Next**.



22. In the **Basic Settings** screen, under **Central Management** group, select **Configure this machine** as SMA appliance for standalone appliance.
OR
Select **Configure this machine as a CMS** to manage the licensing and configuration up to 100 SMA appliances.
23. Set the password and time zone as per your requirements and click **Next**.

Welcome

License Agreement

Basic Settings

Network Settings

Routing

Name Resolution

User Access

Completion

Basic Settings

Central Management

This machine can be configured as a central management server (CMS) to manage the licensing and configuration of up to 100 SMA appliances.

Configure this machine as an SMA appliance

Configure this machine as a CMS to manage the licensing and configuration of up to 100 SMA appliances

Administrator password

Specify the password you will use to access the Appliance Management Console (AMC). Your password must be at least eight characters long.

Enter password: *

Confirm password: *

Date and time

Please select a time zone below. To set the current time, click **Change**. If you wish to synchronize the time with an NTP server, it can be configured later in AMC.

Time zone:

Current time: Mon May 08:51:33 GMT [Change](#)

SONICWALL
SECURE MOBILE ACCESS

Cancel < Back Next >

24. Based on the **Central Management** option selected in the above screen, Interface is automatically selected.
Click **Next**.

Welcome

License Agreement

Basic Settings

Network Settings

Routing

Name Resolution

User Access

Completion

Network Settings

Enter a name to identify your appliance as well as the IP address and subnet mask for the internal and external network interfaces. If you are using a single gateway in your DMZ, you should select "Single Interface".

Appliance name: *

Dual interfaces Single interface

Internal Interface

IP address: * This is the interface connected to your private internal network.

Subnet mask: *

External Interface

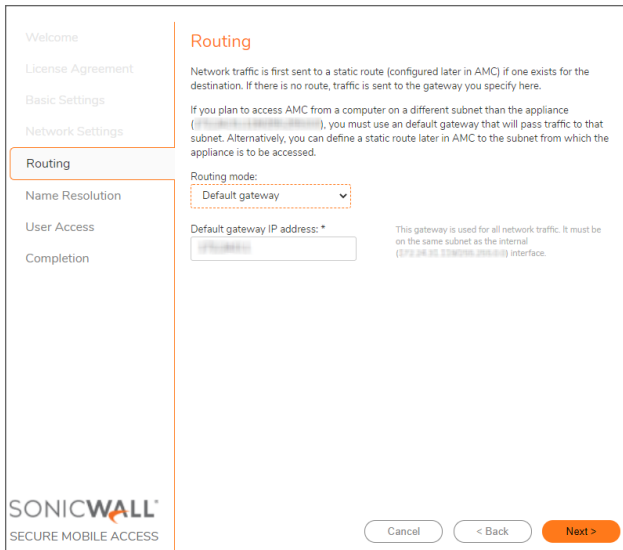
IP address: * This is the interface connected to the Internet.

Subnet mask: *

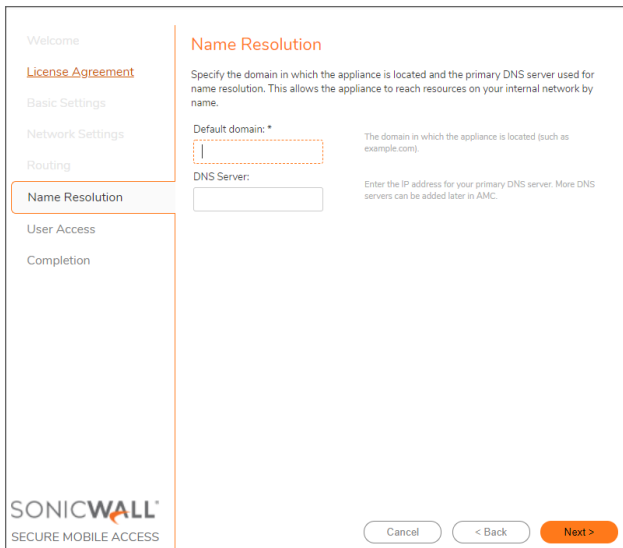
SONICWALL
SECURE MOBILE ACCESS

Cancel < Back Next >

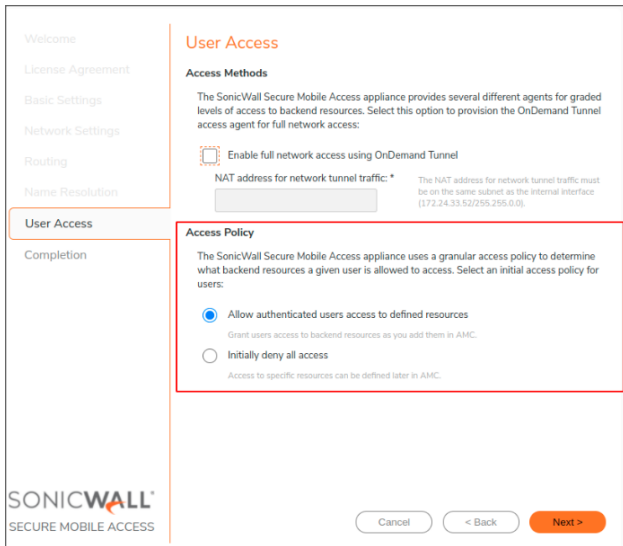
25. In the **Routing** screen, set the external gateway for X1 interface.



26. In the **Name Resolution** screen, set the domain as per your requirements.



27. In the **User Access** screen, select the **Access Methods** and **Access Policy** based on your need.



28. In the **Completion** screen, evaluate the settings and click **Finish** to complete the setup wizard.



Licensing and Registering Your SMA Appliance

This section contains information about licensing and registering your SMA 8200v on KVM.

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.

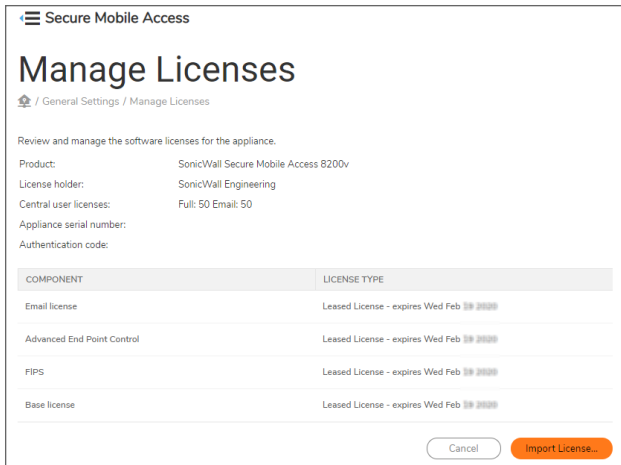
Registering the SMA Appliance

After you have installed and configured the network settings for your SMA 8200v on KVM, you can log into the management console and register it to your MySonicWall account. Registration of your SonicWall SMA 8200v on KVM 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 8200v for KVM:

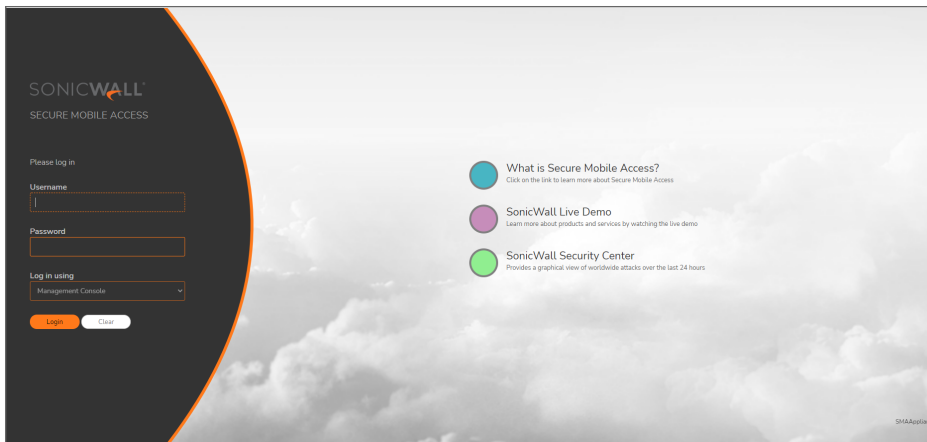
1. Log in to your SMA 8200v virtual machine.
2. In the **System Configuration** group, select **General Settings > Licensing > Edit**.
The **Manage Licenses** page is displayed.



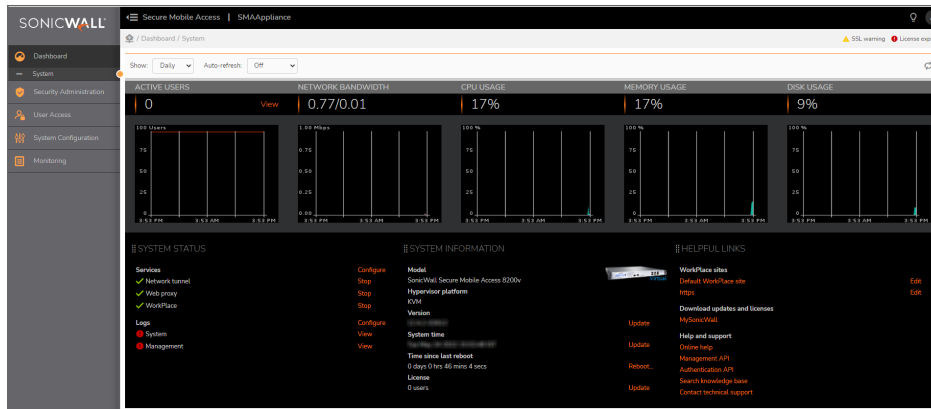
3. In the **Manage License** page, click **Import License**.
4. In the **Import License** page, click **Choose File** to select the license file and click **Upload**. The License file is uploaded into the appliance.
5. You have successfully registered your 8200v virtual machine. Click **Continue** to view the **License Management** screen or continue configuring other settings within the appliance.

Verifying the Installation

1. Log in to AMC using the credentials that you entered in the setup wizard.



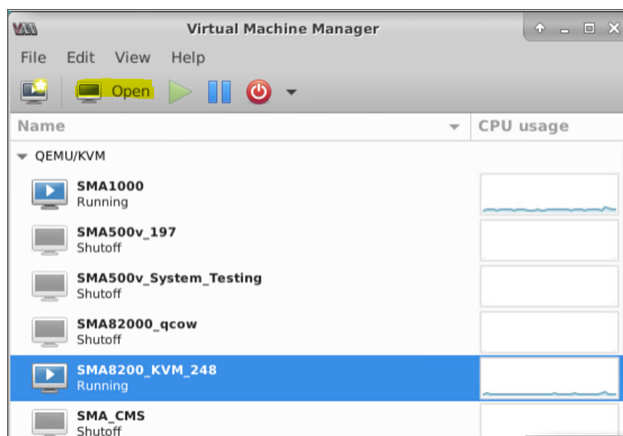
2. Verify the Hypervisor platform.
This should display as KVM.



Using the Virtual Console

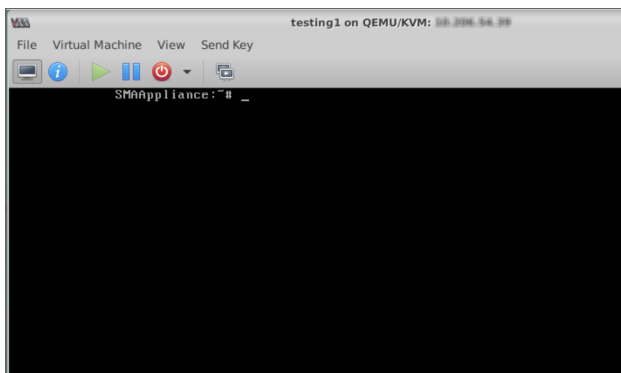
To connect to the management console through the Virtual Machine Manager:

1. Bring up the VMM, then double click on the deployed KVM SMA 1000 Virtual Appliance.

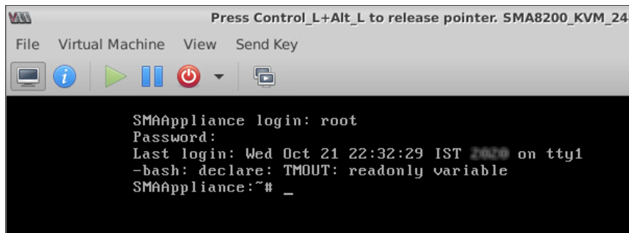


2. Wait for the SMA appliance to boot to the command line in the **Virtual Machine Connection** window and then login as **root** with the password: *password*

Virtual Console of Red Hat



Virtual Console of Ubuntu



```
Press Control_L+Alt_L to release pointer. SMA8200_KVM_24
File Virtual Machine View Send Key
SMAAppliance login: root
Password:
Last login: Wed Oct 21 22:32:29 IST 2020 on tty1
-bash: declare: TMOUT: readonly variable
SMAAppliance:~# _
```

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 on KVM Getting Started Guide

Updated - January 2024

Software Version - 12.4

232-005706-00 Rev C

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products.

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

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

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

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

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