SOPHOS
Security made simple.

Getting Started Guide

Sophos XG Firewall Virtual Device

Document Date: November 2016

Contents

Change Log 3
Preface 4
Minimum Hardware Requirement 4
Installation Procedure 4
Configuring XG Firewall 11
Activation and Registration 11
Basic Configuration 18
Copyright Notice 21

Change Log

Date	Change Description
November 14, 2016	Updated for SF-OS 16.01.2.
October 6, 2016	Updated for SF-OS v16.
July 06, 2016	Updated the images for SF-OS MR-3.
December 23, 2015	Rectified a broken link in Step 1 of the 'Installation Procedure' section.

Preface

Welcome to Getting Started Guide for Sophos XG Firewall Virtual Appliance (hereinafter referred to as "XG Firewall") for VMware ESX/ESXi platform. This guide describes how you can download, deploy and run XG Firewall as a virtual machine on VMware ESX/ESXi.

Minimum Hardware Requirement

1. One vCPU
2. 2GB vRAM
3. 2 vNIC
4. Primary Disk with a minimum of 4GB size
5. Report Disk with a minimum of 80GB size

XG Firewall will go in failsafe mode if the minimum requirements are not satisfied.

Note: To optimize the performance of your XG Firewall, configure vCPU and vRAM according to the license you have purchased. While configuring number of vCPUs, ensure that you do not exceed the maximum number limit specific to your license.

Installation Procedure

Pre-requisite:

Make sure that VMware ESX/ESXi version 5.0 or later is installed in your network. For VMware ESX/ESXi installation instructions, refer to the VMware documentation:

- http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

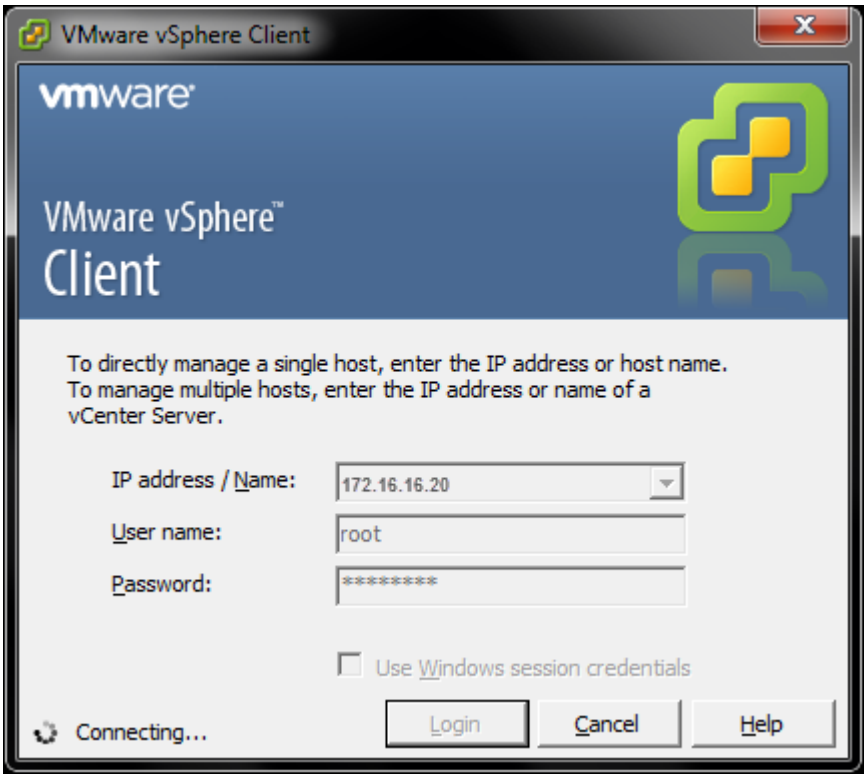
Step 1: Download and Extract OVF Image

Download the .zip file containing the OVF image from https://secure2.sophos.com/en-us/products/next-gen-firewall/free-trial.aspx and save in your machine.

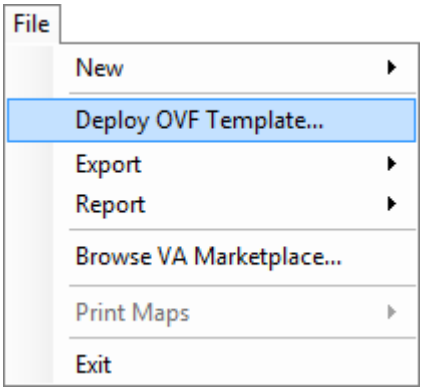
Step 2: Access ESX/ESXi Host via vSphere Client

Login to ESX/ESXi host server on which you want to deploy the OVF template through VMware vSphere Client.

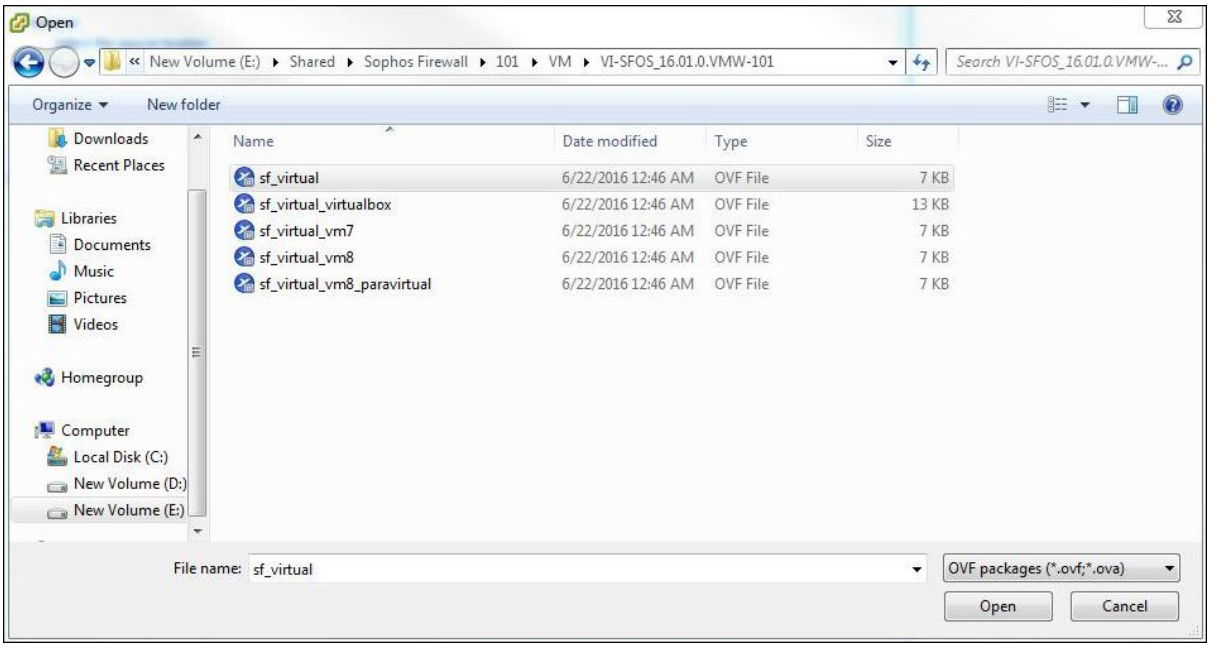
Note: In this guide we are using VMware vSphere client to connect to the ESX/ESXi host server on which the OVF template is to be deployed.



Go to **File → Deploy OVF Template** to open the downloaded .ovf file in the vSphere Client.

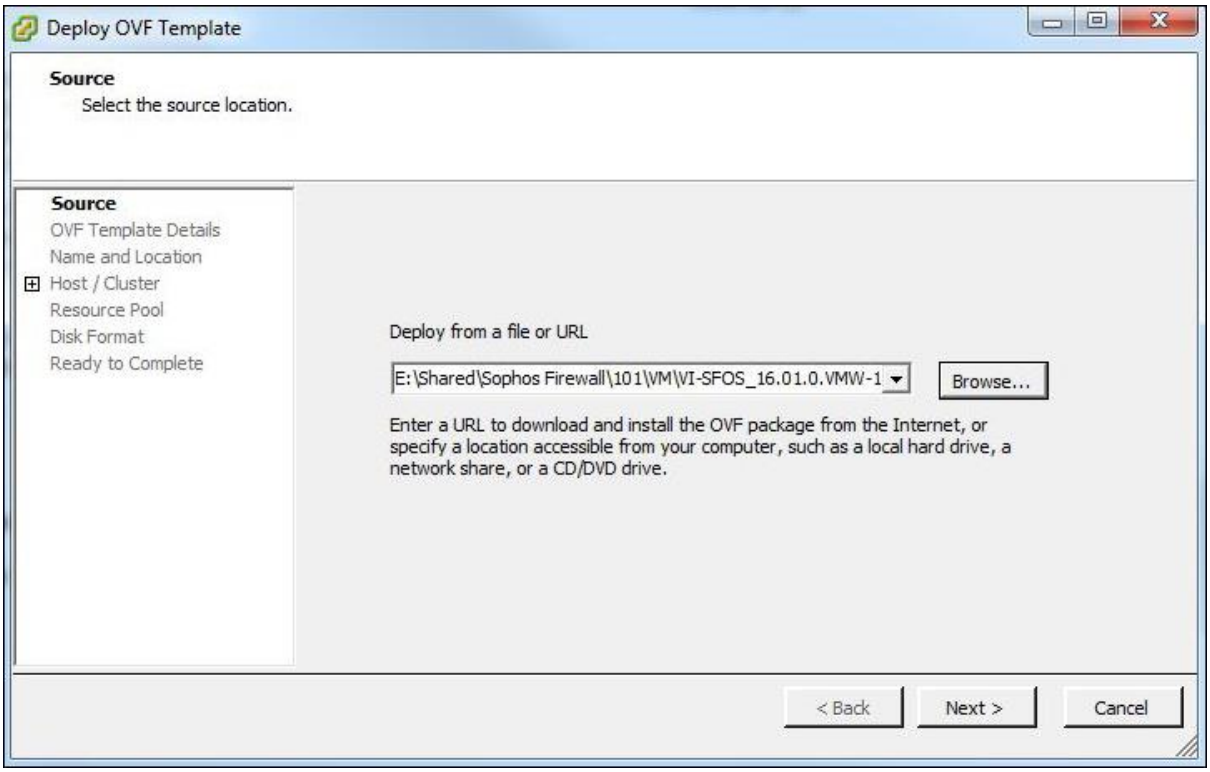


Select the **sf_virtual** file and click **Open**, as shown in the image below.

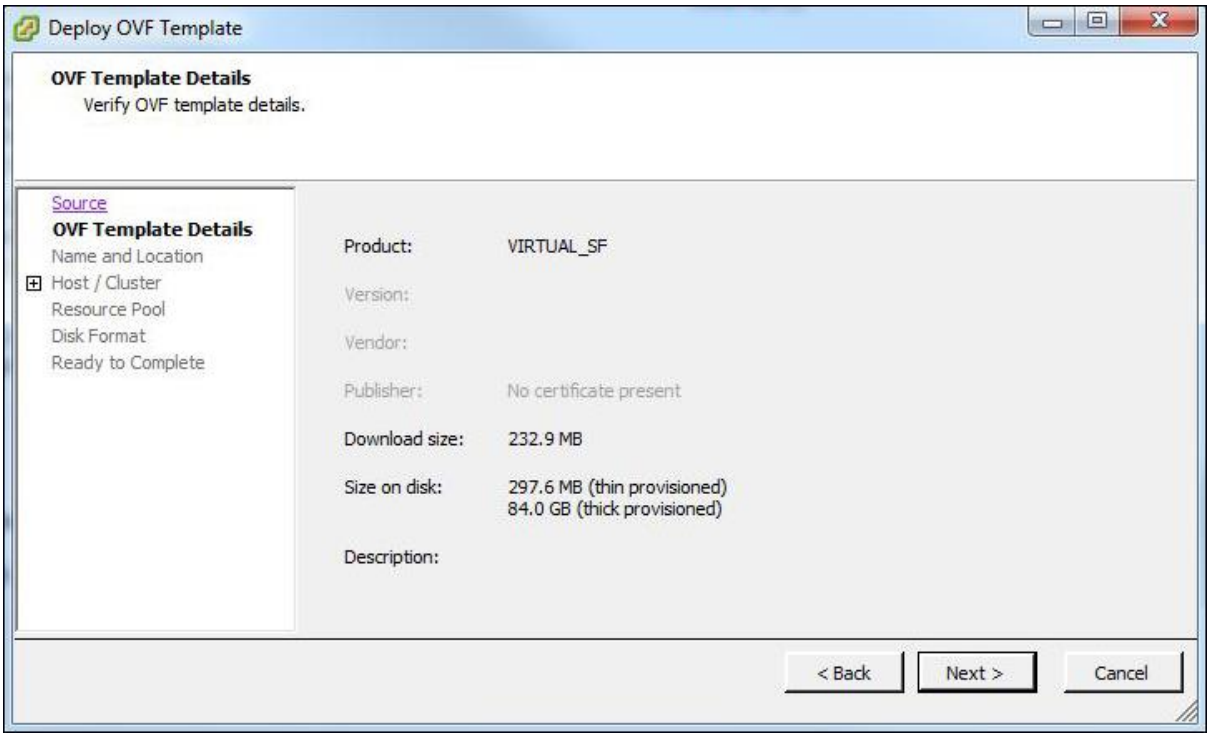


Step 3: Deploy OVF Template

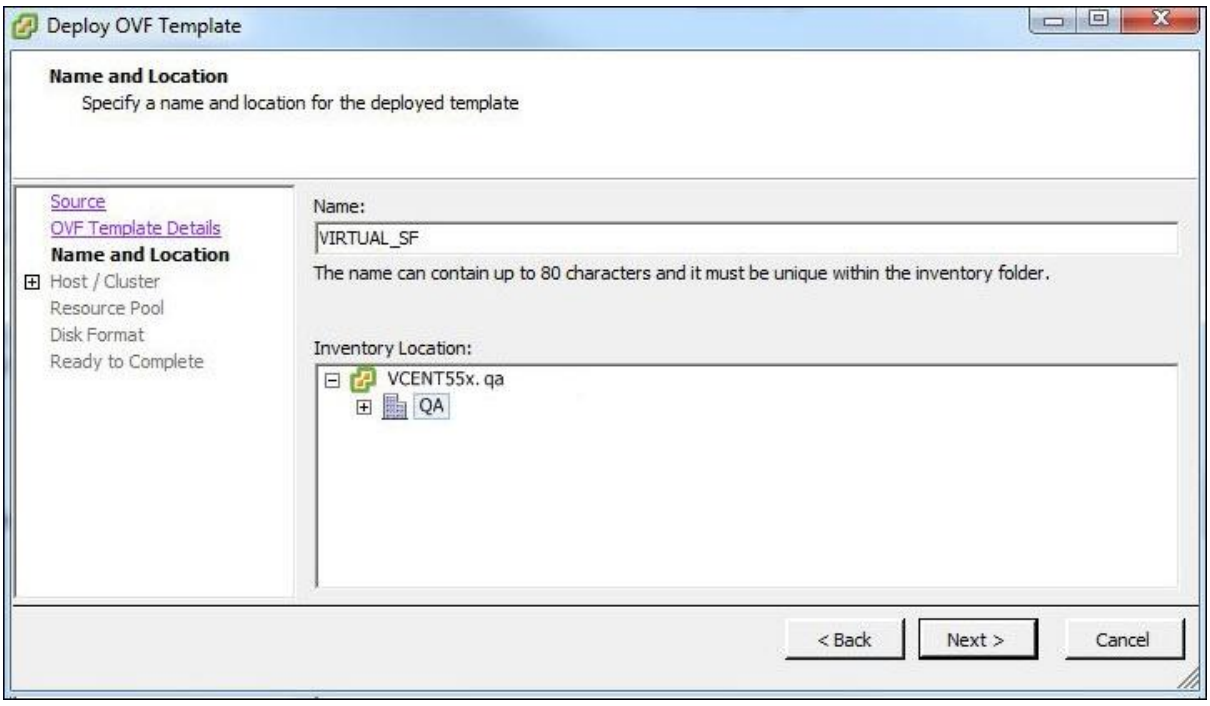
1. Select location of the .ovf file for XG Firewall and click **Next** to continue.



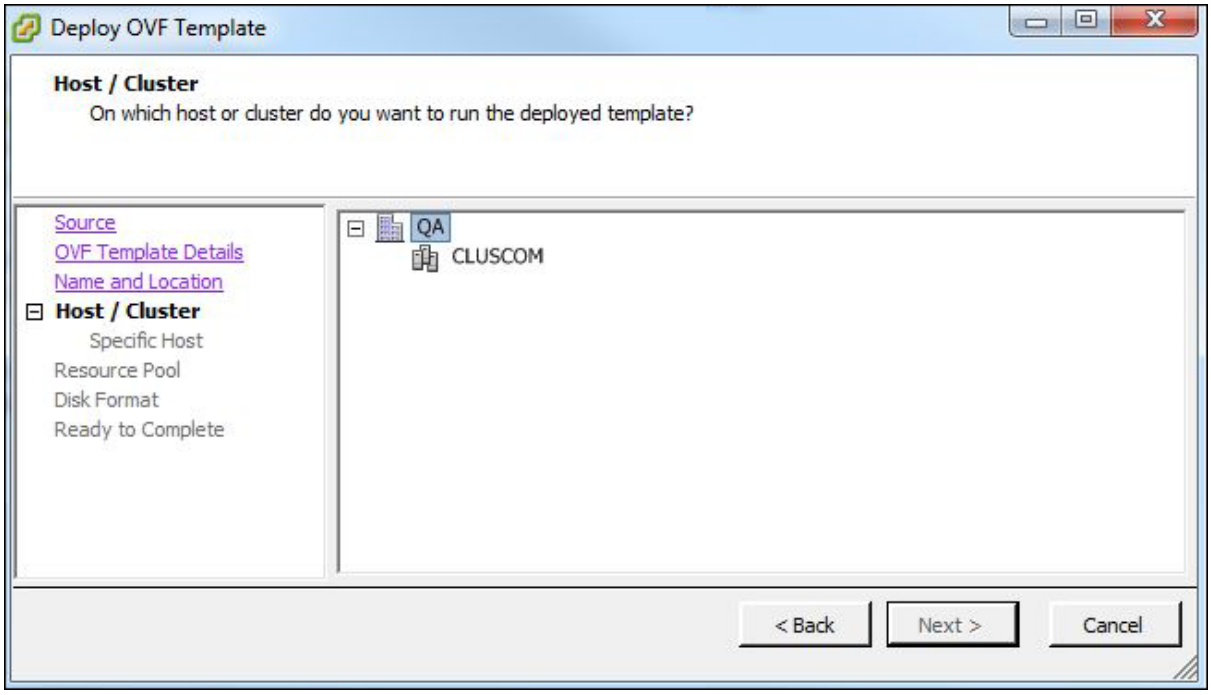
2. Verify the OVF template details and click **Next** to continue.



3. Specify a name and location for the OVF template to be deployed and click **Next** to continue.



4. Select the host / cluster within which you want to deploy the OVF template and click **Next** to continue.



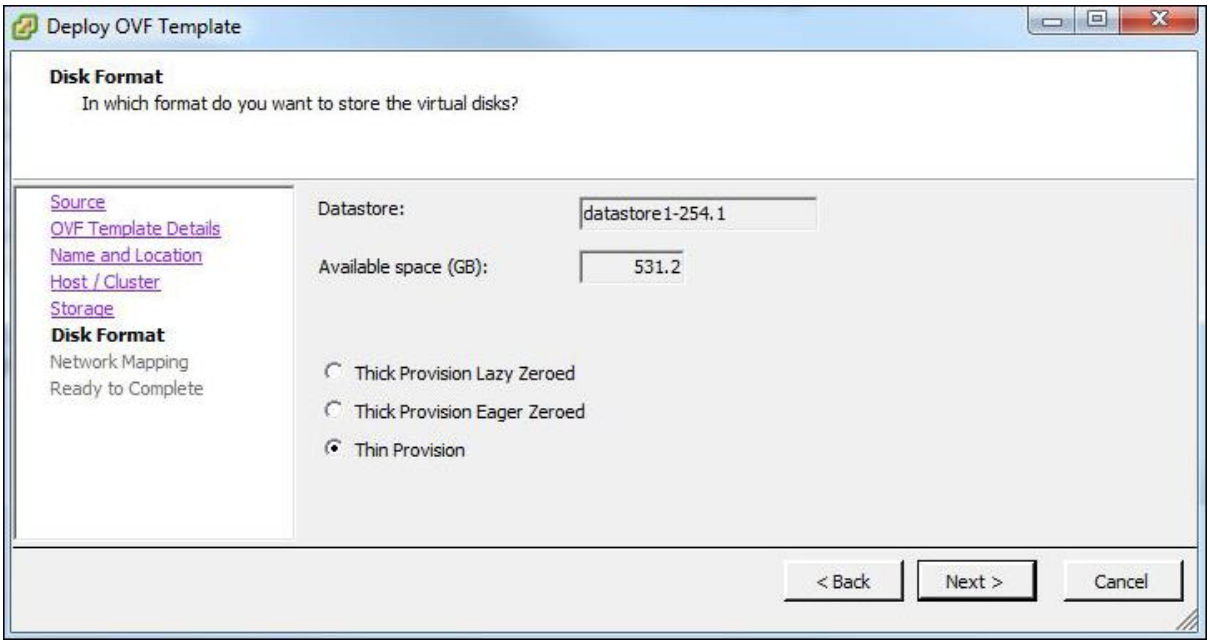
Note: Here, we are deploying the OVF template on a single/standalone server. The configuration may be different in a Cluster environment.

5. Select the format in which you want to store the virtual disks from the available options:

   Thin Provision: It uses minimum required space for the OVF template, saving the rest for other use.

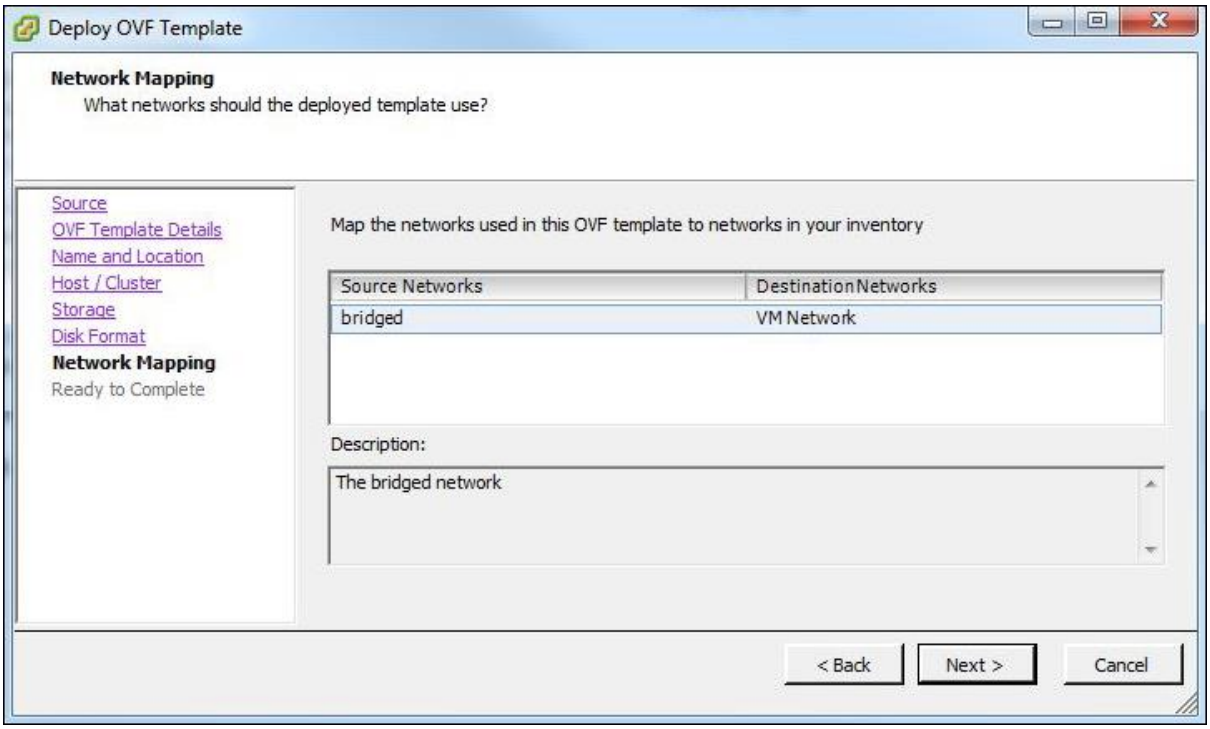
   Thick Provision: It uses the entire allotted virtual disk for OVF template installation, wiping out any additional data on the disk.

   In case of VMware ESXi 5.0 or later, three storage options are available: Thin Provision, Thick Provisioned Lazy Zeroed and Thick Provision Eager Zeroed. For more information, refer to http://www.vmware.com/.

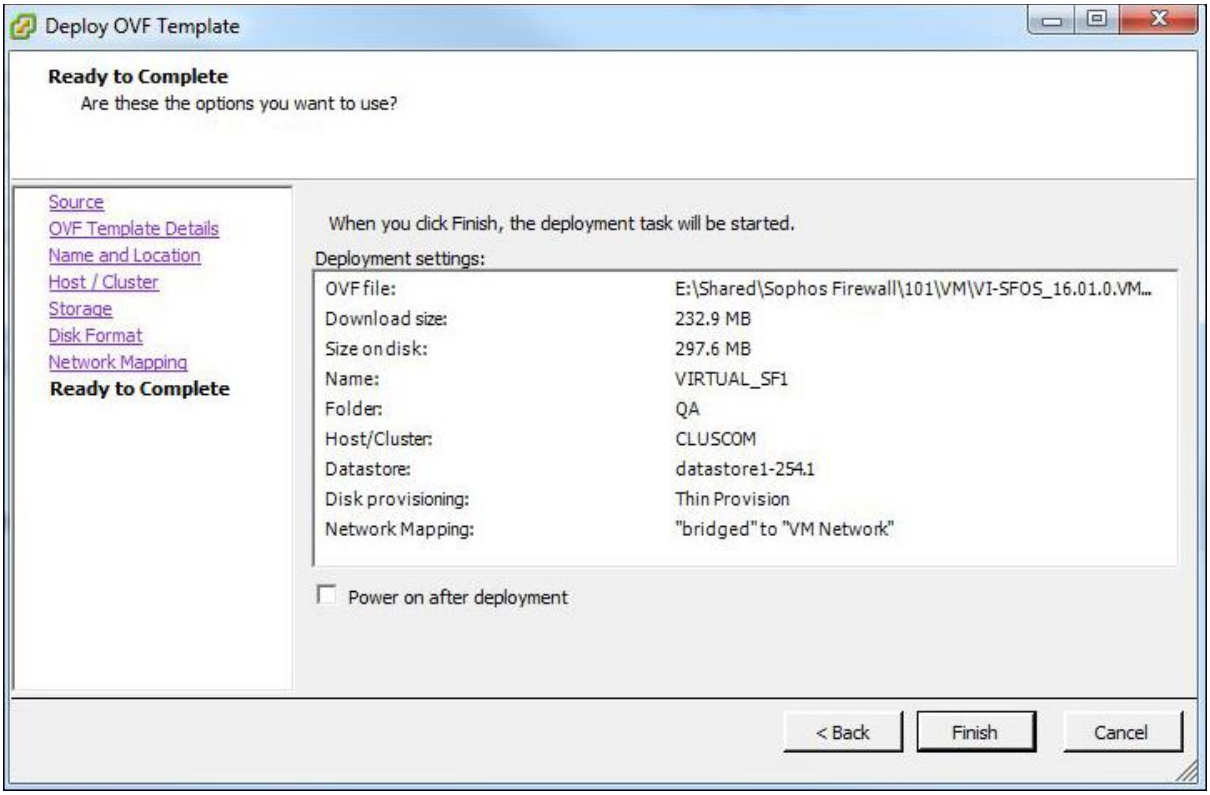


Click **Next** to continue.

Select the networks to be used by the OVF template and click **Next** to continue.



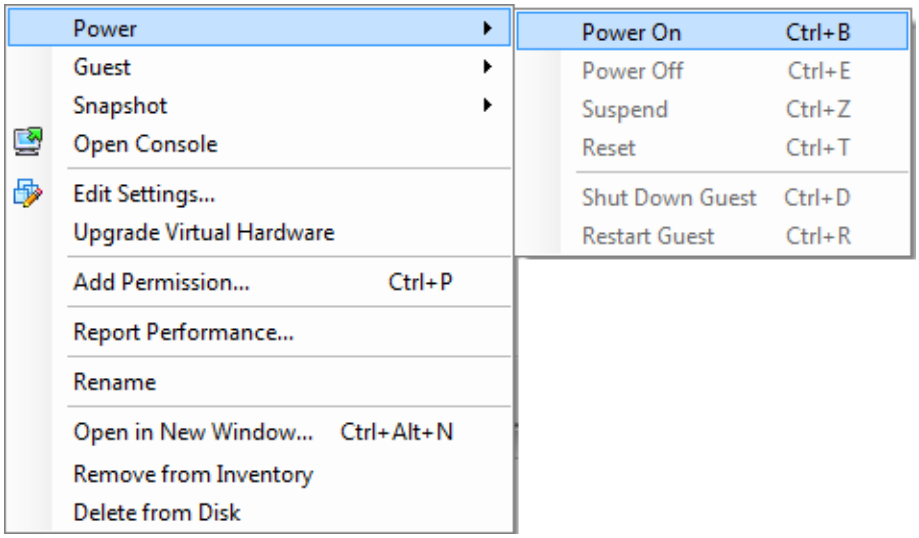
Verify the deployment settings for the OVF Template and click **Finish** to initiate the deployment process of XG Firewall.



This installs XG Firewall on your machine.

Step 4: Power on

Right click the deployed XG Firewall and go to **Power → Power On**.



Enter the administrator password - 'admin' to continue to the **Main Menu**.

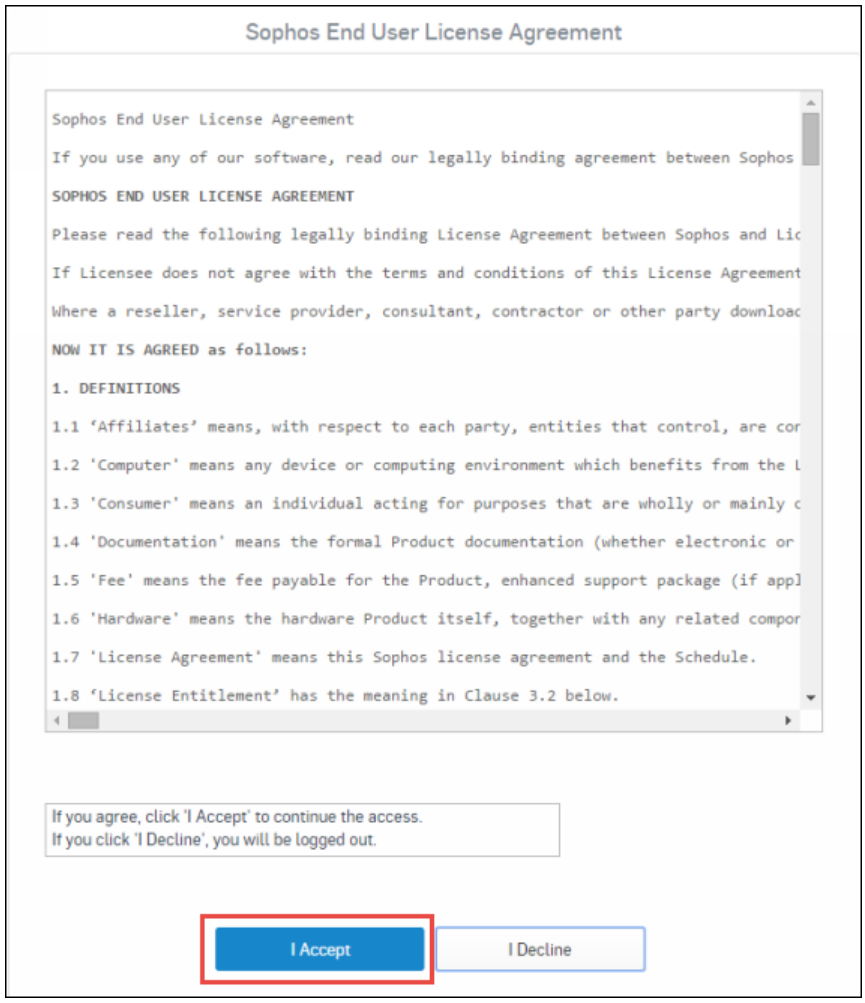
Configuring XG Firewall

Browse to https://172.16.16.16:4444 from the management computer and log on to Admin Console using the default credentials username – admin and password – admin.

Activation and Registration

Step 1: License Agreement

The moment you log in, you will be redirected to the Sophos End User License Agreement (EULA). You need to accept the agreement to proceed further.

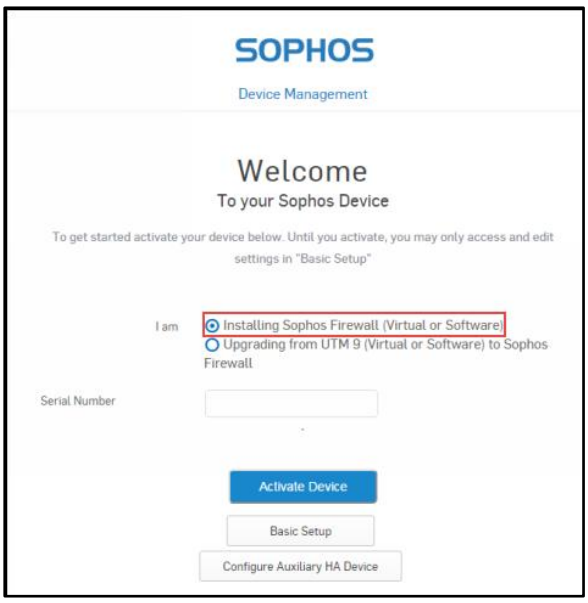


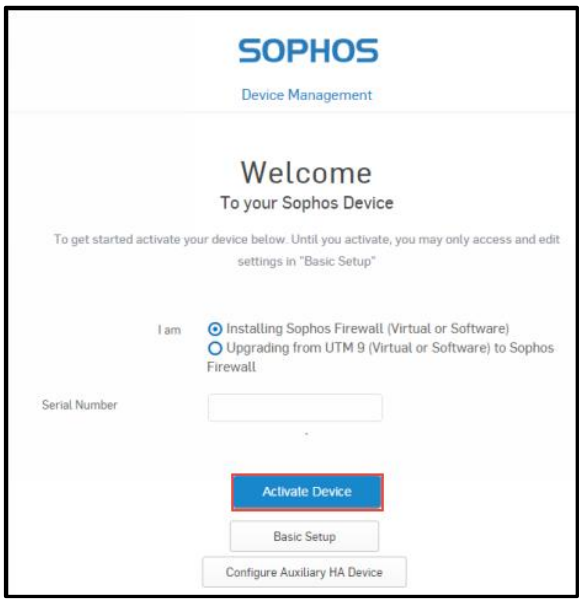
Click **I Accept** to navigate to the welcome page.

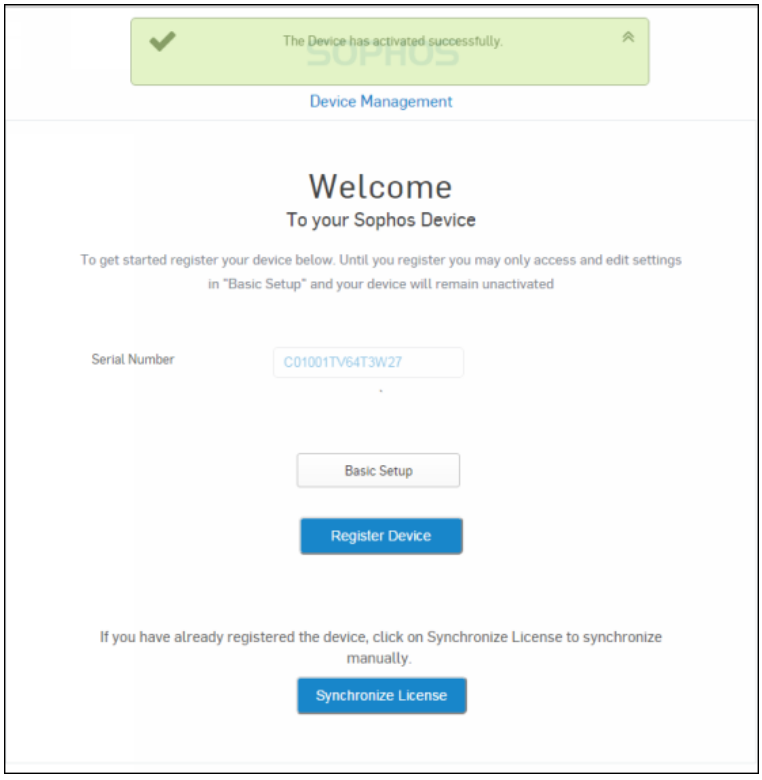
Step 2: Activating XG Firewall

Select **Installing Sophos Firewall (Virtual or Software)** option to continue the activation of XG Firewall. Specify serial number mailed at your registered email address and click **Activate Device** to proceed further

Note: Make sure your current network configuration allows XG Firewall to connect to the Internet for activation. If not, click **Basic Setup** to modify the network settings so that the Device can connect to the Internet.

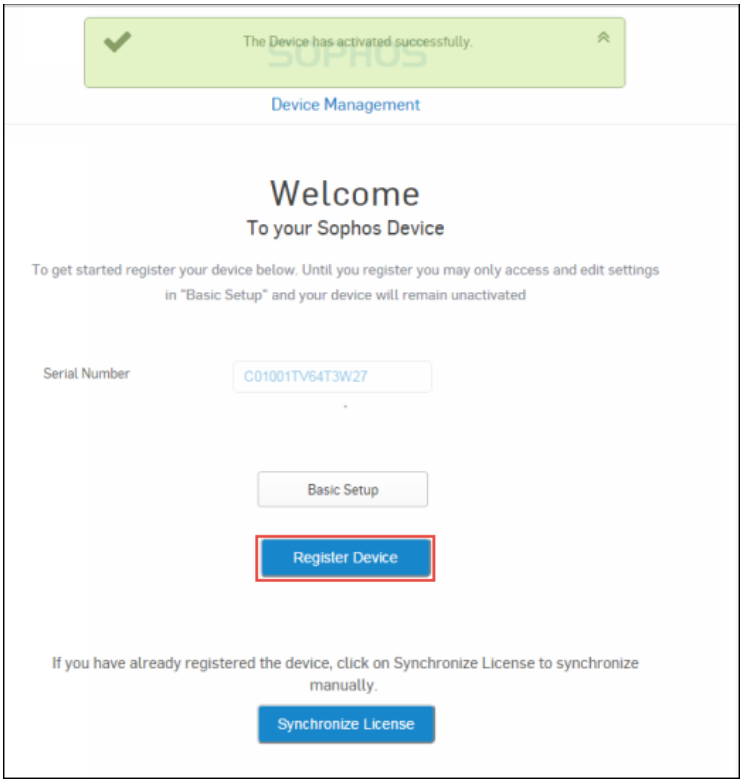

SOPHOS
Device Management
Welcome
To your Sophos Device
To get started activate your device below. Until you activate, you may only access and edit settings in "Basic Setup"
I am
Installing Sophos Firewall (Virtual or Software)
Upgrading from UTM 9 (Virtual or Software) to Sophos Firewall
Serial Number
Activate Device
Basic Setup
Configure Auxiliary HA Device


SOPHOS
Device Management
Welcome
To your Sophos Device
To get started activate your device below. Until you activate, you may only access and edit settings in "Basic Setup"
I am
Installing Sophos Firewall (Virtual or Software)
Upgrading from UTM 9 (Virtual or Software) to Sophos Firewall
Serial Number
Activate Device
Basic Setup
Configure Auxiliary HA Device

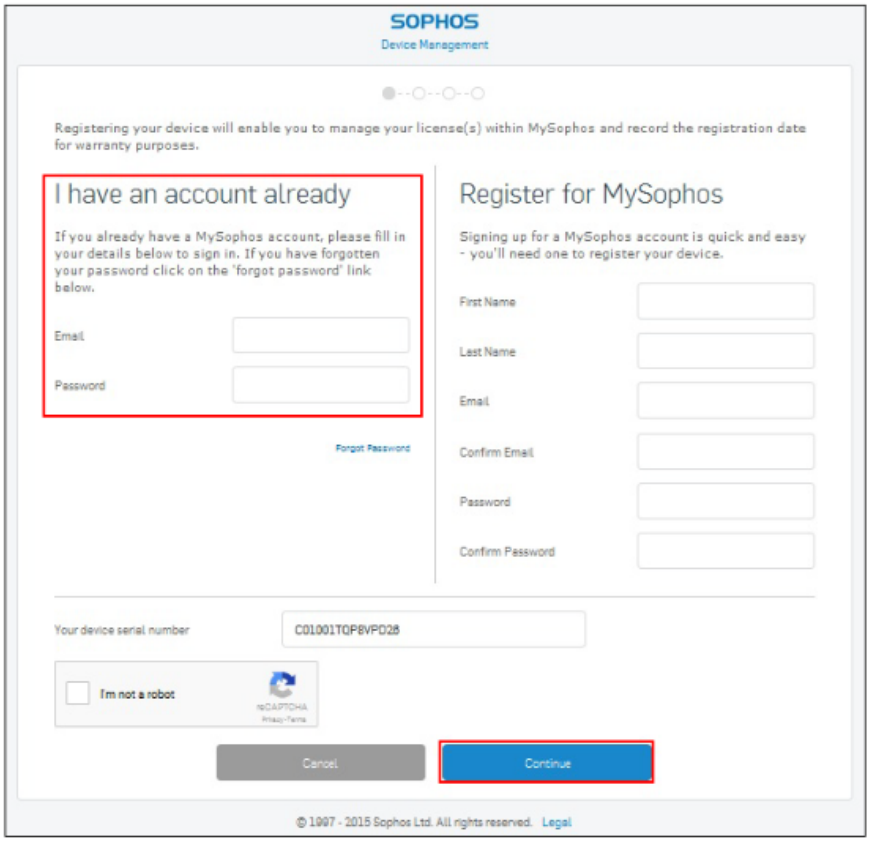

The Device has activated successfully.
Device Management
Welcome
To your Sophos Device
To get started register your device below. Until you register you may only access and edit settings in "Basic Setup" and your device will remain unactivated
Serial Number
C01001TV64T3W27
Basic Setup
Register Device
If you have already registered the device, click on Synchronize License to synchronize manually.
Synchronize License

Step 3: Registering Sophos Firewall

Click **Register Device** to initiate the registration process.



After clicking **Register Device**, you are redirected to the MySophos portal website. If you already have a MySophos account, specify your login credentials under "I have an account already". If you are a new user, sign up for a MySophos account by filling in the details under "Register for MySophos".

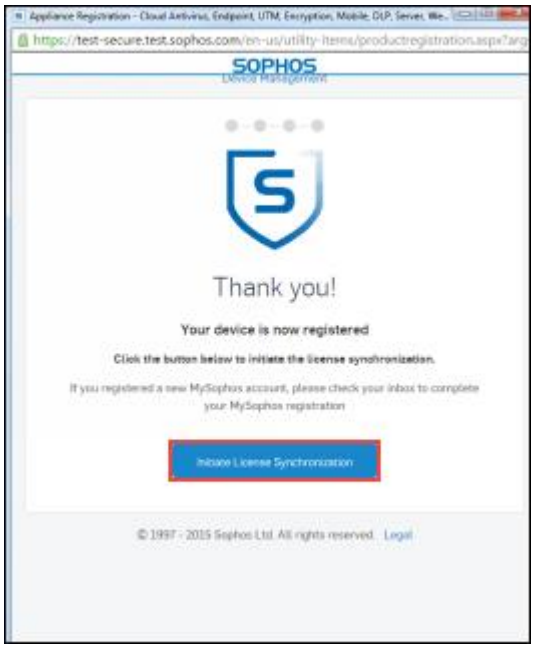


Click **Continue** to complete the registration process.

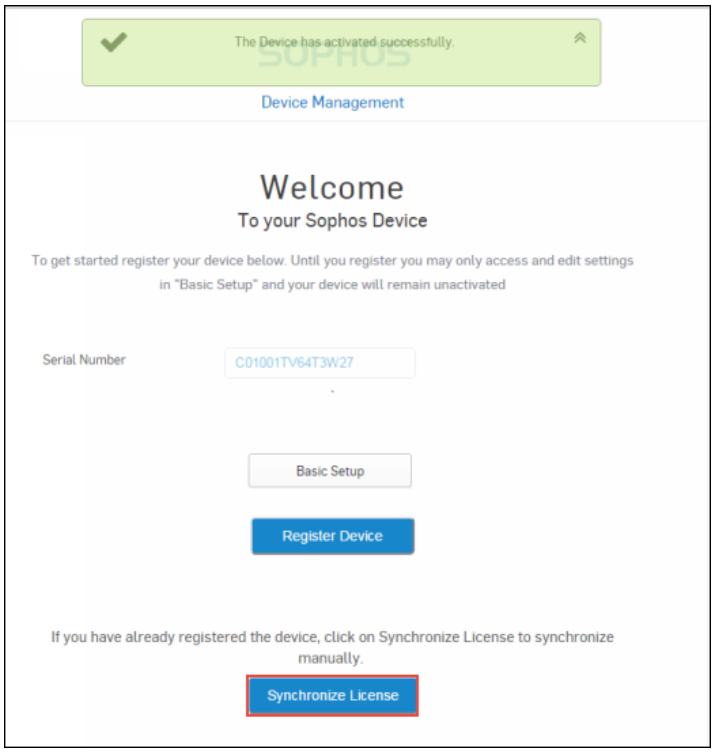
Step 4: Initiate License Synchronization

Post successful registration of the device, you need to synchronize license details with Sophos servers.

As shown in the image below, click **Initiate License Synchronization** to initiate the license synchronization process:

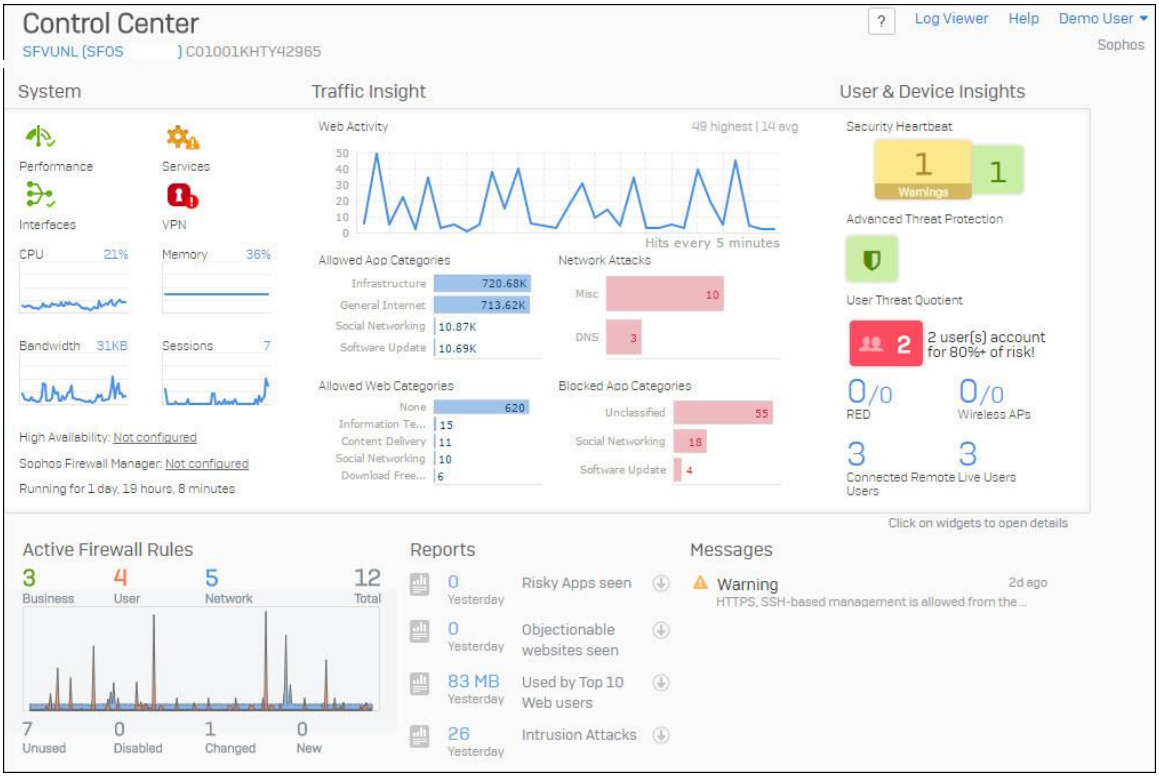


Click **Synchronize License** to synchronize licenses.



Click on **Click Here** in the image above to run the **Network Configuration Wizard**. The wizard walks you through the steps to setup initial configuration of your Sophos Firewall so that you can begin creating your security policies.

Click **Start** to begin the wizard and follow the on-screen instructions. Once the configuration is successfully done, Control Center will be displayed.



You can now use the Navigation pane on the left hand side of the UI to navigate and configure further settings.

Basic Configuration

a. Setting up interfaces

1. Network interfaces and RED connections are defined in the **Configure > Network > Interfaces** menu.
2. Wireless networks are defined in the **Protect > Wireless Networks** menu, and SSIDs will also be shown in the interfaces menu once created.
3. Access points may be configured or added, in **Protect > Wireless > Access Points**.

a. Creating Zones

Zones are central to the security model in SF. If you wish to create more zones than are offered by default, go to **Configure > Network > Zones**. You can then use those zones when creating interfaces, and security policies.

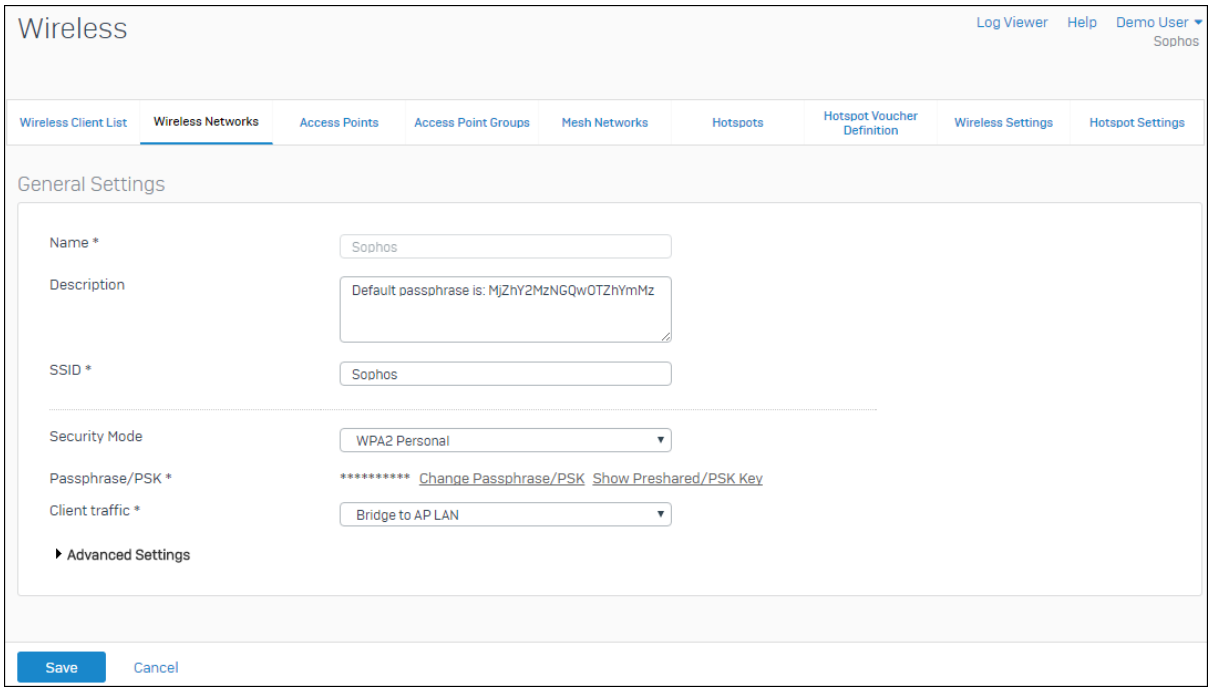
b. Setting up Firewall Rules

All security related policies are defined in the Firewall menu. There are two different firewall rule types available:

1. Business Applications Rule - If you are securing a server or service, use a business application rule to allow internal or external users to access that service.
2. User/Network Rule - If you are controlling what web and application content your protected users can access, or want to control traffic by source, service, destination, zone, (and user) then use a user/network rule.

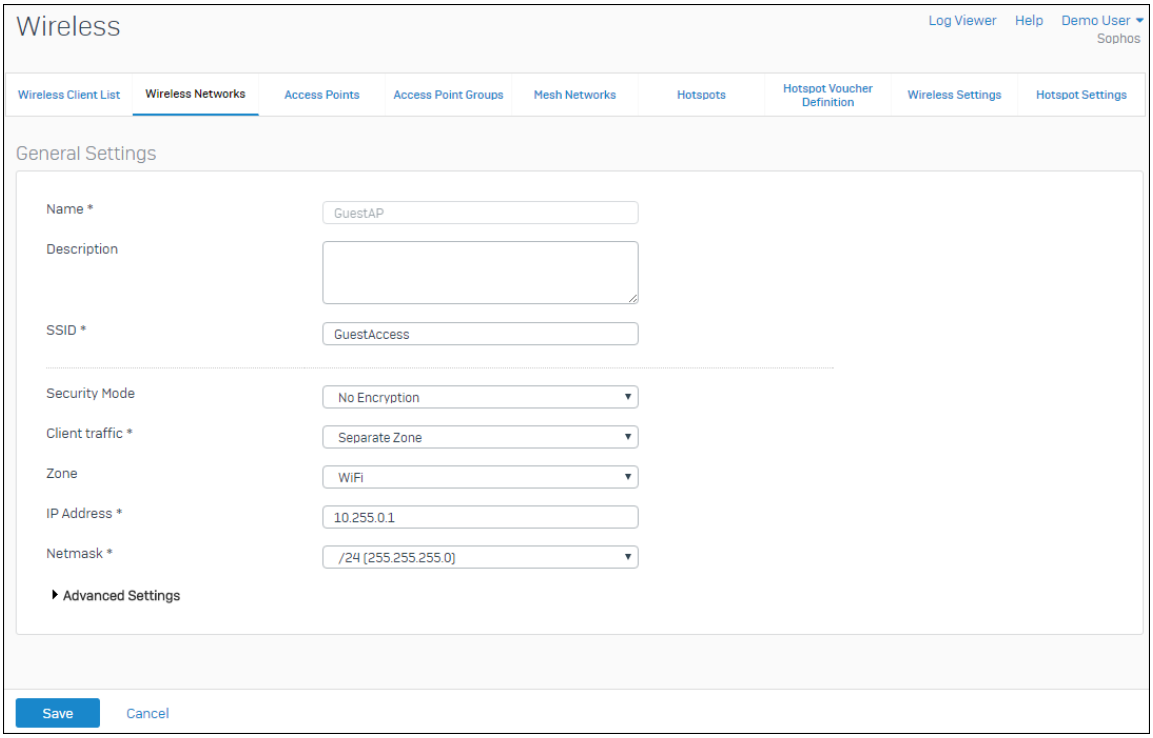
c. Setting up Wireless Network

1. Go to **Protect > Wireless > Wireless Networks**.
2. Click **Add** to add a new wireless network.
3. Configure the Wireless Network as shown in the screen below.

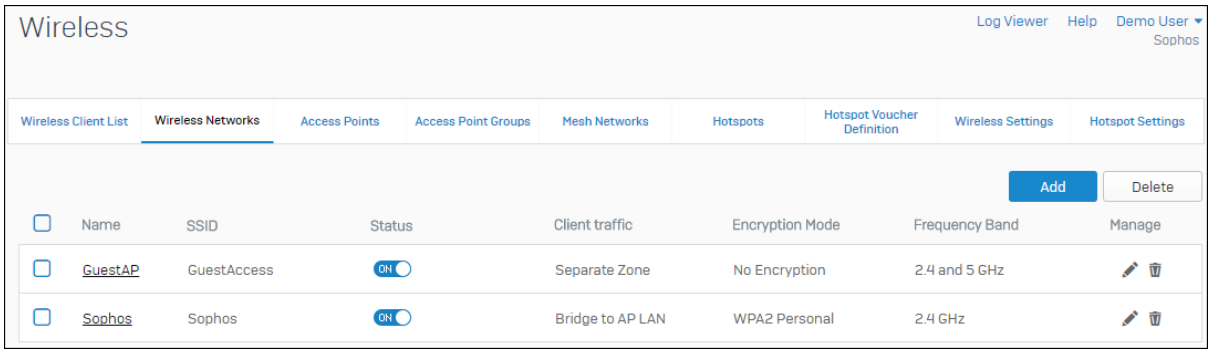


The wireless network will be added successfully.

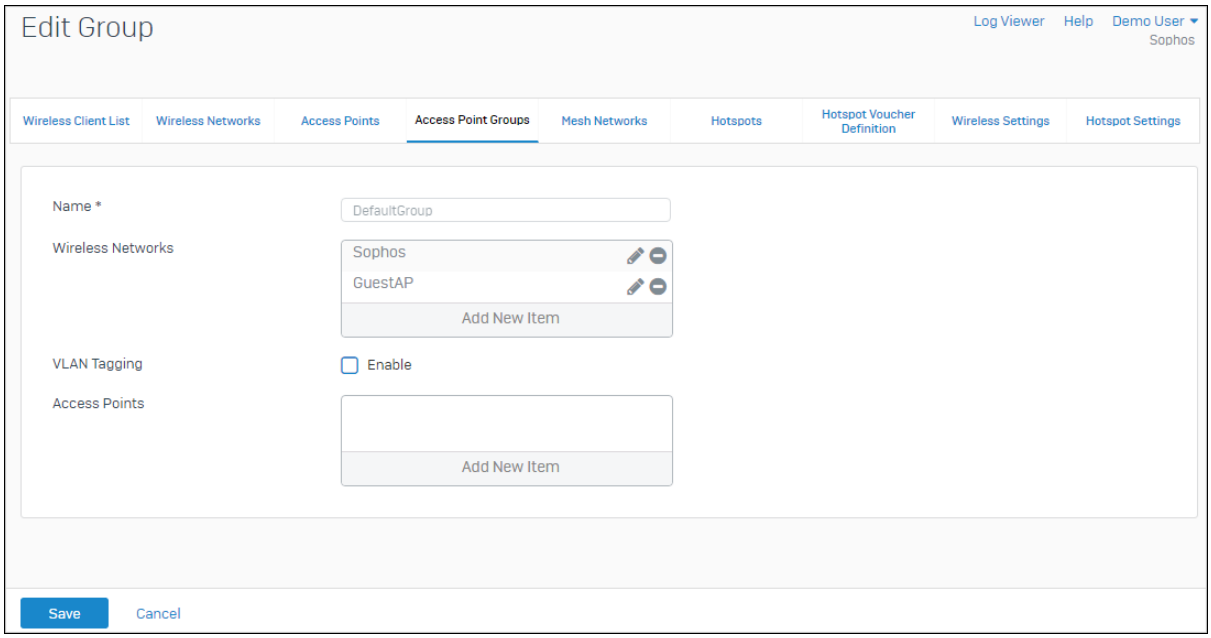
4. Add another Wireless Network for Guest Access as shown in the image below.



Both the added wireless networks can now be seen on the Wireless Network page.



5. Navigate to **Protect > Wireless > Access Point Groups**.
6. Click **Add** to add a new access point group.
7. Configure the new AP group, and add both wireless networks, and the new access point.



After some time, you can continue to discover and add APs from Control Center.

Copyright Notice

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is registered trademarks of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.