Contents

Change Log ........................................................................................................................................... 3
Preface .................................................................................................................................................. 4
Reports for Device Type ...................................................................................................................... 4
Licensing ............................................................................................................................................... 4
Download ............................................................................................................................................ 5
Deploying a Virtual or Software Appliance .......................................................................................... 8
Virtual Appliances ............................................................................................................................... 8
Software Appliances (ISO File) ........................................................................................................... 8
Creating an Installer ............................................................................................................................ 8

Installation process .................................................................................................................................. 9

Booting .................................................................................................................................................. 10

First-Time Device setup ....................................................................................................................... 11
Basic Setup ........................................................................................................................................... 11
Device Activation ..................................................................................................................................... 12
Device Registration ............................................................................................................................... 14
Synchronize License ............................................................................................................................... 15

Configure Sophos iView – Network and System Settings ...................................................................... 16

Start using iView ................................................................................................................................... 17
Configure UTM /Firewall to connect to iView ...................................................................................... 17
Add devices in iView ............................................................................................................................. 17
Selecting Device type to view reports ................................................................................................. 17
Create Device Groups .......................................................................................................................... 18
Start viewing reports ............................................................................................................................ 18
Set Log Retention Period ..................................................................................................................... 18
Export and Schedule reports ............................................................................................................... 18
## Change Log

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 April, 2016</td>
<td>Updated: The IP address is updated from <a href="http://172.16.16.18:4444">http://172.16.16.18:4444</a> to <a href="http://172.16.16.80">http://172.16.16.80</a> or <a href="https://172.16.16.443">https://172.16.16.443</a> under First-Time Device setup</td>
</tr>
</tbody>
</table>
Preface

This guide is intended to help you install and get up and running with Sophos iView v3.

Reports for Device Type

iView v3 provides reports for following device types:

- Sophos Firewall OS
- Sophos UTM 9
- CyberoamOS

Licensing

Sophos iView licenses are available in multiple tiers based on storage requirements and support terms offering great value for any size organization.

A limited capacity (100GB) version is available at no charge for evaluation, or for small customers who don’t need to store data for extended periods. Paid licenses are available for 500 GB, 1TB, 4 TB, 8TB, and unlimited storage requirements.

After Device Registration and License Activation, the Storage Subscriptions in iView are perpetual while the Support Subscriptions need to be renewed periodically.

<table>
<thead>
<tr>
<th>Sophos iView Licenses</th>
<th>Storage limit</th>
<th>Recommended CPU*</th>
<th>Recommended Memory (vRAM)</th>
<th>Network Interface support (Minimum / Maximum)</th>
<th>Approximate event capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>iView Light*</td>
<td>100 GB</td>
<td>Dual core</td>
<td>4 GB</td>
<td>1 / 4</td>
<td>Short-term evaluation only</td>
</tr>
<tr>
<td>iView 500 GB</td>
<td>500 GB</td>
<td>Dual core</td>
<td>4 GB</td>
<td>1 / 4</td>
<td>Up to 300 events per second</td>
</tr>
<tr>
<td>iView 1 TB</td>
<td>1 TB</td>
<td>Dual core</td>
<td>4 GB</td>
<td>1 / 4</td>
<td>Up to 300 events per second</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>--------</td>
<td>---------</td>
<td>-----</td>
<td>--------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>4 TB</td>
<td>Quad core</td>
<td>4 GB</td>
<td>1/4</td>
<td>Up to 600 events per second</td>
</tr>
<tr>
<td>iView 4 TB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 TB</td>
<td>Quad core</td>
<td>4 GB</td>
<td>1/4</td>
<td>Up to 600 events per second</td>
</tr>
<tr>
<td>iView 8 TB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unlimited (16 TB recommended)</td>
<td>Quad core#</td>
<td>8 GB</td>
<td>1/4</td>
<td>Up to 2000 events per second</td>
</tr>
<tr>
<td>iView Unlimited</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Event capacity varies with CPU family and hardware specs

* Free for evaluation purpose
** CPU frequency 2.7 GHz or equivalent
# CPU frequency 3.1 GHz or equivalent

**Download**

iView v3 is available as Virtual Appliance or as Software Appliance [on custom hardware].


2. To register for MySophos Account, fill in the required details as highlighted in the image below and click Submit.
Note:

After clicking submit, you will receive an email at the Email Address specified in the step above asking you to activate your account. For now, skip activating your account and proceed directly to step number 3.

3. Fill-in your organization details and click Submit.

4. Download the virtual image for your iView appliance, as highlighted in the image below:
5. Clicking Download takes you to the End User License Agreement page. Select the checkbox against ‘I accept the terms and conditions’ and click Submit to initiate the download process of a ZIP file containing the virtual image for iView v2.

In addition, you will receive an email with subject line ‘Your Sophos Serial Number’ containing the serial number to activate and register your Sophos product. For now, just save the serial number and proceed to step number 6 since you will need the serial number for Device Activation and Registration.

6. Activate your MySophos account
While your virtual image is being downloaded, open the mail you received in step 2 asking you to activate your account. Click the link provided in the mail to activate your account. You should see the image below.

![MySophos Account Activated]

**Deploying a Virtual or Software Appliance**

**Virtual Appliances**

A. VMware Virtual Machine (VMware Workstation, ESXi_Server)
B. Xen Virtual Machine
C. Hyper-V Virtual Machine
D. KVM Virtual Machine

Import the VM file into your hypervisor of choice, and set the hardware specs for your Sophos iView VM.

**Software Appliances (ISO File)**

The downloaded ISO file can be installed on the custom hardware using an Installer. To create the Installer, refer the next section.

**Creating an Installer**

For Software installs, you’ll start with an ISO. Write the ISO to a standard USB thumb drive to start the installation.

**On Windows:**

1. Download and run the Win32 Disk Imager utility [http://sourceforge.net/projects/win32diskimager/]
2. Run the utility, and browse for the downloaded ISO file. The application will default to looking for .IMG files. Be sure to change the file filter to [*.*], then locate and select the iView ISO file.
3. Select the USB thumb drive you wish to install the ISO on. The thumb drive should be at least 1GB in size, and writing the ISO to it will erase any data it currently contains.
4. Once the process is complete, your thumb drive is ready to use.

**On OSX:**
1. Open the Disk Utility included on OSX.
2. Locate the thumb drive in the list of disks.
3. On the partitions tab, change the volume scheme to “1 partition”, and the format to “Free Space”, then click **apply**.
4. You’ll need to convert the downloaded ISO file into a new format. Open a terminal window, and navigate to the path where the ISO is stored.
5. Run the command:
   ```bash
   hdiutil convert -format UDRW -o VI-SIVOS_02.00.0-092.iso
   The converted ISO will be /can be named iView.img.dmg
   ```
6. Next, locate the device path of the USB device, by running **diskutil list**.
   For example, let’s say your USB thumb drive’s path is **/dev/disk9** but be sure to use the actual path of your thumb drive.
7. Next, write the converted ISO to your thumb drive, with the following command:
   ```bash
   dd if=./iView.img.dmg of=/dev/rdisk9 bs=1m
   **Note:**
   - The of= path adds an “r” in front of the device path name. This is deliberate, and enables RAW disk access. You may leave the r out, but the process will go much more slowly.
   - You may need to run “sudo dd <rest of command>” for the imaging to work on your system.
8. Wait a few minutes for the process to complete. When you return to a command prompt, the thumb drive will be ready, and can be ejected.
9. If you run into problems, see [http://borgstrom.ca/2010/10/14/os-x-bootable-usb.html](http://borgstrom.ca/2010/10/14/os-x-bootable-usb.html) for more detailed instructions.

**Installation process**

Since this is a Software Appliance, you may need to change BIOS settings for the thumb drive to boot, if you are installing on your own hardware. You will also need to connect a monitor and keyboard, or a serial cable to the system to complete. You will need to respond to two prompts to begin the installation.
**Booting**

When prompted, press **y<enter>** to start the install. The install progress will be shown on the screen, as it continues.

Once the install is complete, remove the thumb drive, and reboot the device. Give it a couple minutes for the first boot to complete, and the system to be ready and running iView.

At this point, the system is now running iView.
First-Time Device setup

Basic Setup

1. Open the Web Admin UI from https://172.16.16.18:80 or https://172.16.16.18:443 using initial credentials admin /admin. The End User License Agreement is displayed, carefully read the agreement and click I Accept to continue.

2. Click Basic Setup and complete the device’s Basic Setup so that device will be able to connect to the Internet for Activation.
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"

Serial Number: 

Activate Appliance

Basic Setup

Device basic setup settings updated successfully.

Note: To activate device successfully, make sure the WAN, DNS, and Default Gateway are configured correctly to reach to the internet connection.

Device Activation

You should have received an email with the Serial Number on the email address provided while downloading the iView v3 Partner Beta image.

After Basic Setup is done, enter the Serial Number and click Activate Appliance. Your device will be activated successfully.
Device Registration

After Activation, click Register Device to register your device.

As highlighted in the image below, under ‘I have an account already’ section, provide the login credentials you configured while registering for MySophos Account

Click Continue and your device will be registered.
**Synchronize License**

After Registration, click **Initiate License Synchronization** to start license synchronization on the device.
Configure Sophos iView – Network and System Settings

After License Synchronization, you will see below screen.
Clicking on ‘Click Here’ will take you to the Home Dashboard. You can configure basic setup of iView using the iView settings.

1. Network Settings
   - Go to System -> Network -> Interface to configure Port A IP address and configure Gateway settings
2. Configure DNS [System -> Network -> DNS]
3. Configure System Time from System -> Configuration -> Time & Date
4. For Report Notifications, configure Mail Server [System -> Configuration -> Mail Server]
5. Change the default administrator password from System -> Administration -> Users
Start using iView

Configure UTM /Firewall to connect to iView

1. Sophos Firewall OS devices
   b. Add and configure Syslog server:
      i. Configure Port, IP address
      ii. Change severity level to debug
      iii. Select modules for which logs need to be sent via Syslog to iView

2. Sophos UTM 9 devices
   b. Configure IP and Port of iView.
   c. Select modules for which logs are to be sent via Syslog.

3. CyberoamOS devices
   a. Go to Logs and Reports > Configuration
   b. Add and configure Syslog server:
      i. Configure Port, IP address
      ii. Change severity level to debug
      iii. Select modules for which logs need to be sent via Syslog to iView

Add devices in iView

Upon login to iView, you can add devices from Add device pop-up

OR

Visit System -> Configuration -> Devices

Selecting Device type to view reports

You can view reports for Sophos Firewall OS devices, Sophos UTM 9.x and CyberoamOS devices in iView. Also, there is an option to view reports of All Device Types.

1. Viewing reports for each device type separately

   The number of reports supported and displayed across these device types varies. Selecting the device type in the dropdown displays reports and menu items relevant and supported for that device type.

2. View reports for all device types together
If you have more than one device type, you can choose the All Devices option that reports for all supported device types.

**Create Device Groups**

You can group devices based on your need

For example:

As an Enterprise, you may want to group devices based on location

OR

As an MSP, you may want to group devices based on customers

**Start viewing reports**

As the devices added in iView send logs to iView, you can view dashboards and reports to analyze security and productivity risks, analyze usage patterns and create custom views and bookmark reports.

**Set Log Retention Period**

iView allows you to customize the retention period of sections of reports after which those reports are automatically purged. Depending on your Licensed Capacity, change the Log Retention Period of your required report sections.

**Export and Schedule reports**

You can export or schedule reports for your analysis or share with your management or customers.