Proprietary and Confidential to Skybox Security. © 2021 Skybox Security, Inc. All rights reserved.

Due to continued product development, the information contained in this document may change without notice. The information and intellectual property contained herein are confidential and remain the exclusive intellectual property of Skybox Security. If you find any problems in the documentation, please report them to us in writing. Skybox Security does not warrant that this document is error-free.

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—without the prior written permission of Skybox Security.

Skybox®, Skybox® Security, Skybox Firewall Assurance, Skybox Network Assurance, Skybox Vulnerability Control, Skybox Threat Manager, Skybox Change Manager, Skybox Appliance 5500/6000/7000/8000/8050, and the Skybox Security logo are either registered trademarks or trademarks of Skybox Security, Inc., in the United States and/or other countries. All other trademarks are the property of their respective owners.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>About Skybox Security</td>
<td>4</td>
</tr>
<tr>
<td>Installing Skybox Security Suite on Azure</td>
<td>5</td>
</tr>
<tr>
<td>Deploy Skybox on Azure from the Microsoft Azure Marketplace</td>
<td>6</td>
</tr>
<tr>
<td>Create a Virtual Machine</td>
<td>8</td>
</tr>
<tr>
<td>Connect to the VM</td>
<td>13</td>
</tr>
<tr>
<td>Install Skybox Manager</td>
<td>16</td>
</tr>
<tr>
<td>Add Storage to a VM</td>
<td>18</td>
</tr>
<tr>
<td>License Skybox Security Suite</td>
<td>20</td>
</tr>
</tbody>
</table>
Overview

This *Quick Start Guide* describes the steps required to install Skybox™ Security Suite on Azure. This guide walks you through the process from the first access of the marketplace until Skybox is successfully deployed. This installation provides the full feature set of Skybox Security Suite; however, you require a license to use each module. If you already have a Skybox license for one or more modules it can be used with this installation. If not, contact Skybox Security via one of:

- Phone: 1-408-441-8060
- Email: info@skyboxsecurity.com
- Website: [https://www.skyboxsecurity.com](https://www.skyboxsecurity.com)

About Skybox Security

Skybox provides a holistic cybersecurity management platform that gives enterprise organizations the ability to gain full context and understanding of their attack surface so they can make informed decisions that solve security issues better and faster. The platform unifies vulnerability management and security policy management with an aggregation of data sets from over 150 security and network technologies, and allows enterprise teams to analyze and validate network and security configurations together so they can most effectively close vulnerabilities while making policy and rule changes that truly optimize overall security. The Skybox Platform helps enterprise teams reduce systemic across their entire organization with a mature and tightly connected security management framework that ensures planning, implementation, and ongoing change management can collectively attain the best overall security posture. The Skybox Platform includes four software modules that can be licensed for vulnerability and threat management and security policy management: Firewall Assurance, Network Assurance, Vulnerability Management, Change Management and a daily threat feed for a detailed picture of the attack surface. The product is updated regularly with new features and capabilities. Successive updates can be downloaded from within the product and require moderate interaction with the operating system.

**Note:** For security reasons, we strongly recommend that you take great care when opening ports to internal hardware devices over public networks such as the Internet.
Chapter 1

Installing Skybox Security Suite on Azure

Skybox Security is installed from within the Azure Marketplace.

The onboarding process assumes that you have an Azure account and that you are familiar with deploying applications in the cloud.

The process for onboarding Skybox in Azure includes the following steps:

1. **Deploy Skybox on Azure from the Microsoft Azure Marketplace**
2. **Create a Virtual Machine**
3. **Connect to the VM**
4. **Install Skybox Manager**
Deploy Skybox on Azure from the Microsoft Azure Marketplace

Skybox is installed from within the Azure Marketplace.


2. On the search results page, select Skybox Security Version 11

3. On the product description page, click GET IT NOW
4. Click **Continue** to agree to the terms of use and privacy policy.

5. On the Skybox Security portal page, click **Create**.

This opens a set of VM creation dialog boxes.

Continue with **Create a Virtual Machine**.
Create a Virtual Machine

The process to create a VM on Azure is done via a series of dialog boxes that are presented in sequence.

The following steps guide you through this process and indicate the basic required parameters, optional parameters, and when to use the default values.

The parameter values can be changed based upon your deployment architecture and your business needs.

During the process you can click Previous to go to the preceding dialog box.

The Create a Virtual Machine process starts with the Basics dialog box.
1. In the Basics dialog box, fill in these fields:

![Create a virtual machine dialog box]

<table>
<thead>
<tr>
<th>FIELD</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource group</td>
<td>Enter the name of an existing resource group or create a new one.</td>
</tr>
<tr>
<td>Virtual machine name</td>
<td>Enter a unique name.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select <strong>SSH public key</strong>.</td>
</tr>
</tbody>
</table>

**FIELD** | **VALUE**
---|---
Resource group | Enter the name of an existing resource group or create a new one.
Virtual machine name | Enter a unique name.
Authentication type | Select **SSH public key**.
2. Click **Next : Disks**.

3. In the Disks dialog box:

   ![](image)

   **Create a virtual machine**

   Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more ](link)

   **Disk options**

   - **OS disk type** *(Default)*
     - Standard SSD
   - **Encryption type** *(Default)*
     - Encryption at rest with a platform-managed key
   - **Enable Ultra Disk compatibility** *(Optional)*
     - Ultra disk is not supported for Availability Zone 1 in eastus.

   **Data disks**

   You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

<table>
<thead>
<tr>
<th>LUN</th>
<th>Name</th>
<th>Size (GiB)</th>
<th>Disk type</th>
<th>Host caching</th>
</tr>
</thead>
</table>

   **Create and attach a new disk**  **Attach an existing disk**

   ![Next: Networking button]

   Click **Review + create**
Chapter 1  Installing Skybox Security Suite on Azure

a. We recommend that you set **OS disk type** to **Premium SSD**.

   **Note:** The default size of the disk is 500 GB.

b. To add additional disk space, see Add Storage to a VM.

c. Click **Next**: **Networking**.

4. In the Networking dialog box:

   a. For Network security group, the default ports are 22, 444, 8443.

   **Note:** If the node is intended to run a remote collector (non-reverse), port 9443 must be opened instead of port 8443.

   - To accept all the default values including the Network security group, do not change these values.
   - To use an existing Network security group, select it in the drop-down list.
   - To create a new Network security group, or to change the default values of the ports, click **Create new** beneath the Network security group field.
Review the Inbound rules and, if correct, click **OK**.

b. Click **Next : Management**.

5. In the Management, Advanced, and Tags dialog boxes, click **Next** to accept the default values.

6. In the Review + create dialog box:
   a. Review the VM settings and pricing information.
   b. Click **Create** to start creating the VM.

The deployment process may take several minutes.

7. When the VM is created, click **Go to resource** to go to the Virtual machine details page.

Continue with **Connect to the VM**.
Connect to the VM

Most administration activities can be completed via your browser using Skybox Appliance Administration. The process to connect to it is described in this section.

**Note:** Some activities, including updating the operating system packages or upgrading the Skybox application, require SSH access to the machine. An SSH session can be established from the Azure Cloud Shell or from your preferred SSH client. Refer to Azure online documentation that explains how to establish an SSH session to your Skybox instance.

*To connect to the VM via your browser.*

1. If you have just created the VM, click **Go to resource**.
   This takes you to the Virtual Machine details page.

2. From the Overview page, copy the IP address of your VM.

3. In your browser, enter `https://<VM IP address>:444`, where `<VM IP address>` is the IP address that you copied, and press **Enter**.
   This connects you to the Appliance Administration port. If a security warning is displayed, proceed to the IP address.

   **Note:** This security warning is related to the default self-signed certificate created by the installation.

   You can add a CA certificate as described in *Adding your own certificate* in the *Skybox Virtual Appliance Quick Start Guide*.

   This guide can be accessed via the help of Appliance Administration after you log in to it in the next step.
4. When you are connected, log in to Skybox Appliance Administration as user `skyboxview` with the default password `skyboxview`.

5. Change the default password.
   After you change your password, Skybox Appliance Administration opens.
Skybox Appliance Administration is where you can do security and date/time setup, network configuration and other system functions, and view logs.

For additional information, click Help to access the Skybox Virtual Appliance Quick Start Guide.

Continue with Install Skybox Manager.
Install Skybox Manager

After Skybox Security is installed, you need to install Skybox Manager. It is required to configure certain admin components within the product. However, almost all user functions are done in Skybox Web Client and not in Skybox Manager.

Skybox Manager is a Java client and should be installed on a Windows PC. The Skybox Manager installer is obtained directly from the VM via the Skybox Appliance Administration Support tab.

1. Click **Support > Skybox Manager > Download Skybox Manager**

![Download Skybox Manager](image)

**Download Skybox Manager** always provides the manager compatible with the initial version included in the ISO.

2. Select the Skybox Manager executable that is displayed.

![Skybox Manager Executable](image)

3. Save and run the Installer to install Skybox Manager

   After Skybox is installed on Azure, the Manager automatically upgrades during its first connection to the Server.

4. Start Skybox and log in with the following parameters:
   - Default user: Skyboxview
   - Default password: Skyboxview
   - In the **Server** field, enter the **VM IP address**, where **VM IP address** is the IP address from
the VM Overview page.
Add Storage to a VM

Storage can be added to an existing Skybox VM as needed.
Consult with Skybox Professional Services for advice and capacity planning to determine your optimal configuration.

To add storage to a VM:
2. Select a previously deployed VM, and from the left-side menu, select Disks.
3. Click Create and attach a new disk, and fill in these fields:
4. Click **Save**.
   The disk is created. This process may take several moments.

5. **Establish an SSH session to your Skybox instance and run:**
   - `su` – to log in as the root user.
     The default password is `skyboxview`. This password must be changed on first login.
   - `lsblk` to see the disk names for this VM.
     Note the name of the last disk in the list (this is the disk you created). Replace `<device name>` in the following commands with this name.
   - `pvcreate /dev/<device name>` to create the physical volume.
   - `vgextend skyboxvg /dev/<device name>` to add the disk to the existing space.
   - `lvresize -l+100%FREE --resizefs /dev/mapper/skyboxvg-optlv`

6. **Run the command `lvs` to confirm that the disk was added to the logical volume `optlv`.
   To add the disk to a different logical volume, run the command, change the volume name in the `lvresize` command to the other volume.
Chapter 3

License Skybox Security Suite

Skybox Security Suite requires a valid license file to operate. If you are already a Skybox customer your current license will work with this installation.

If you do not possess a license or you would like to purchase one, contact Skybox Security via one of:

- Phone: 1-408-441-8060
- Email: info@skyboxsecurity.com
- Website: https://www.skyboxsecurity.com

Detailed instructions explaining how to set up Skybox Security Suite are available online at http://downloads.skyboxsecurity.com/files/Installers/Skybox_View/latestDocs/