Zscaler Internet Access (ZIA) and Skybox Deployment Guide

November 2019

Version 1.1
Table of Contents

1 Document Overview ........................................................................................................4
  1.1 Document Audience ..................................................................................................4
  1.2 Software Revisions ..................................................................................................4
  1.3 Request for Comments ..............................................................................................4
  1.4 Document Prerequisites ...........................................................................................5
  1.5 Document Revision Control .....................................................................................6

2 Configuring ZIA for Skybox .........................................................................................7
  2.1 Logging into ZIA ........................................................................................................7
  2.2 Obtain ZIA API Key ..................................................................................................8
    2.2.1 Navigate to API Key Management ......................................................................8
    2.2.2 Add API Key ......................................................................................................8
    2.2.3 Verify API Key ..................................................................................................9
  2.3 Create ZIA Administrator for Skybox ......................................................................10
    2.3.1 Add Administrator Role ..................................................................................10
    2.3.2 Add Administrator for Skybox ........................................................................12
  2.4 Activate ..................................................................................................................13

3 Configuring Skybox .......................................................................................................14
  3.1 Log into Skybox Firewall Assurance .........................................................................15
  3.2 Open Operational Console ......................................................................................16
  3.3 Create New Task – Python 2.7 Installation ..............................................................17
    3.3.1 Install Python ....................................................................................................18
    3.3.2 Validate Python Install ....................................................................................19
  3.4 Create New Task – Zscaler Collector .........................................................................21
    3.4.1 Validate Zscaler Collector Install .....................................................................22
    3.4.2 Zscaler Firewall in the Skybox network map ..................................................23

4 Requesting Zscaler Support ..........................................................................................24
  4.1 Gather Support Information ......................................................................................24
    4.1.1 Obtain Company ID .........................................................................................24
    4.1.2 Save Company ID .............................................................................................25
    4.1.3 Enter Support Section .......................................................................................26

5 Appendix A: Zscaler Resources ...................................................................................27

6 Appendix B: Skybox Resources ....................................................................................28
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (<em>RFC 3706</em>)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (<em>RFC 2890</em>)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (<em>RFC 2409</em>)</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security (<em>RFC 2411</em>)</td>
</tr>
<tr>
<td>OAM</td>
<td>Operation, Administration, and Management</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (<em>RFC 6101</em>)</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security (<em>RFC 5246</em>)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (<em>RFC 7239</em>)</td>
</tr>
<tr>
<td>ZAPP</td>
<td>Zscaler End-point Client Application</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
1 Document Overview

This Deployment Guide document will provide GUI examples for configuring Zscaler Internet Access (ZIA) and Skybox Firewall Assurance. This guide is intended for standing up proof-on-concept topologies and demos, for evaluating interoperability, and joint integration. This guide should not be used to configure either vendor platform for production use. For production deployments, please contact Zscaler or Skybox for post-sale deployment assistance.

1.1 Document Audience

This document was designed for Network Security Engineers and Network Security Architects. All examples in this guide presume the reader has a basic comprehension of IP Networking. For additional product and company resources, please refer to the Appendix section.

1.2 Software Revisions

This document was written using Zscaler Internet Access v5.7 and Skybox 10.0.304 (Build 109).

1.3 Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact partner-doc-support@zscaler.com.
1.4 Document Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 5.7 (or newer)
- Administrator login credentials to ZIA

Skybox

- Administrator login credentials to Skybox
- License for Skybox Firewall Assurance
- Enable SkyBox to use NTP (please refer to Appendix Section)
### 1.5 Document Revision Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Change Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>September 2019</td>
<td>Initial document created by Zscaler and Skybox</td>
</tr>
<tr>
<td>1.1</td>
<td>November 2019</td>
<td>Incorporated edits from Skybox</td>
</tr>
</tbody>
</table>
2 Configuring ZIA for Skybox

2.1 Logging into ZIA

First, we will setup the Zscaler side of this service. The required steps for this section are:

- Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, please contact support: [https://help.zscaler.com/submit-ticket](https://help.zscaler.com/submit-ticket).
2.2 Obtain ZIA API Key

2.2.1 Navigate to API Key Management

To create an API key, navigate to: Administration -> API Key Management.

![Figure 2: Obtain ZIA API Key](image)

2.2.2 Add API Key

Next select “Add API Key”, as show below.

![Figure 3: Obtain ZIA API Key](image)
2.2.3 Verify API Key

After selecting “Add API Key”, an API key will be generated. Your screen should match what is show below.

Figure 4: Obtain ZIA API Key
2.3 Create ZIA Administrator for Skybox

2.3.1 Add Administrator Role

Next we need to create an Administrator Role, so navigate to: Administration -> Role Management -> Add Administrator Role. The Administrator Role settings we need to enable for Skybox should match what is shown below. Note: the screen capture below only shows the top portion of this web form. You will have to scroll down to see all the settings, which are shown in the next section of this document.

Figure 5: Obtain ZIA API Key
Below are the lower-half of the web form. One you have completed configuring your settings to match the settings below, click “Save”.

Figure 6: Obtain ZIA API Key
2.3.2 Add Administrator for Skybox

Now that we have our Administrator Role, we will configure a new Administrator account, and apply this role to it. Please navigate to: Administration -> Administrator Management -> Add Administrator.

![Add Administrator](image)

Figure 7: Add Administrator
2.4 **Activate**

You are now ready to activate all pending changes. Once you have completed this set, you will be ready to configure Skybox.

![Figure 8: Activate Pending Configuration Changes](image)

Figure 8: Activate Pending Configuration Changes
3 Configuring Skybox

Skybox integration with Zscaler (ZIA) allows Skybox users to collect information from the Zscaler web firewall to be used in the Skybox SPM (Security Policy Management) platform.

The information collected from the ZIA service can be used in Skybox in a variety of use cases:

- **Access Policy Compliance:** Administrators can create an access policy in Skybox and run access checks against the Zscaler firewall to ensure policy compliance.
- **Access Analysis:** Skybox users can create access queries to analyze the traffic that can traverse the Zscaler firewall solution.
- **Easy Review:** Users and firewall administrators can review their entire firewall policy from all vendors in a single pane of glass.
- **Rule Policies:** Users can define an access rule policy that details how the rules are created in the organizational firewalls.
- **Visualize the cloud firewall with all connections (VPN/GRE tunnels) to on-premises equipment. (Network Map)**

Collecting the Zscaler secure web gateway information into Skybox can be achieved by the out-of-box collection task which can be launched in a regular schedule to ensure the Skybox platform is updated with the latest information from the Zscaler solution.
3.1 Log into Skybox Firewall Assurance

Figure 9: Log Into Skybox
3.2 **Open Operational Console**

Once you have your Skybox Appliance, or Skybox Virtual Appliance, installed and licensed, you can now start configuring the Skybox software and adding the tasks needed to collect your Zscaler instances. You will need to open the operational console. The operation console is where can begin to create the tasks necessary to collect the various devices on your network. Please click on the Operational Console at the top and in the middle of the Firewall Assurance window.

![Figure 10: Open Operational Console](image)
3.3 Create New Task – Python 2.7 Installation

Skybox is a task driven solution. Script installations, necessary software installation, Analytics, Zscaler collection and more are all driven by creating a task. Zscaler uses a python script to collect from the Zscaler instance. As a result, we will need to install python to proceed with collecting Zscaler into the Skybox Model. In the Operation Console click on “New Task” this will open the New Task window to configure the task needed to install python on the Skybox Server.

![Figure 11: Install Python 2.7](image)
3.3.1 Install Python

The Python installation task needs run only once. After successfully installing Python with this task you will no longer need to re-run the task.

Once the New Task window opens, where you will insert the task configurations necessary to install Python, please do the following:

1. Insert a “Name” in the corresponding field. A name that briefly describes what you are doing with this task will be beneficial for future organization. Example – Python Install Tool
2. In the “Task Type” field, select the “Install Python Tools for Skybox Appliance”. If you type the first 2 letters of the word “Python” the task selection will automatically narrow down to tasks with the letters “Py”.
3. Choose the collector you will use to collect the Zscaler instances. If you have only one Skybox Server, you are, more than likely, running both the Skybox Server and the Skybox Collector. In larger environments, that use both a standalone Skybox Server and a standalone Skybox Collector, each will appear in this field. Select the collector you would like to use to collect the Zscalers.
4. Leave the “Timeout” and “Enable Auto Launch” as their defaults.
   a. The timeout is the amount of time you need to the task to run before it times out. This may be increased for environments with high latency. Leave this as the default for the purposes of this collection.
   b. Enable Auto Launch with allow this task to launch on its own. You can schedule a specific time that this task will launch under the “Schedule” tab at the top of the task window. Leave this as default; it will default to the time that it was created. If you want to change the time, click on the schedule tab and change the schedule to your preference.
5. Choose whether the device, that is running Skybox, is a collector or a server. If you have only one device, choose collector, as the Skybox server is, more than likely, running both collector and server.
6. Select the Python version you would like to run on the Skybox Server. Your options are Python 2.7 and Python 3.7.
   a. Zscaler requires Python 2.7 installation.
7. Click on “Launch”.
   a. Note: The “Alerts”, “Comments” and “Schedule” tabs at the top of the task are for the following additional configurations:
      i. Alerts – You can configure email and error level preferences in this tab.
      ii. Comments – Insert comments regarding this task
      iii. Schedule – You can specify, down to the minute, when you would like to “Auto Launch” this task.
Figure 12: Install Python
3.3.2 Validate Python Install

The Install Python Tools task is only needed for Virtual Machine instances of the Skybox Server. If you would like to install Zscaler and Python tools on a Windows Machine, or various Linux Machines, you will need to install Python at the OS Level, not in the Skybox Software.

After you have launched the Install Python Tools task, it will run for about 5-10 minutes depending on the resources allocated for this VM.

Figure 13: Validate Python Install
3.4 **Create New Task – Zscaler Collector**

Open the Operation Console and open a new task by clicking on the “New Task” button. Then, please insert the following:

1. Name – This is the name of the task you’re creating. Ex. – “Zscaler collection”.
2. Task Type – select Zscaler. If you type the first two letters of the task type, such as “zs”, the Zscaler task will appear in the task type pull down menu. The Zscaler task is located in the “general” folder and has the name “Secure Web Gateway – Zscaler”. Select the Secure Web Gateway – Zscaler task.
3. Leave “Timeout”, “Enable Auto Launch” as their defaults.
4. Choose “Server” or “Collector”. If you have only 1 Skybox Server, choose “Collector” as you are typically running both on a single instance of Skybox, unless you specify otherwise.
5. Choose the Zscaler “Cloud” (provided by Zscaler and indicated as the host of the URL from your Zscaler UI)
6. Insert “Username”
7. Insert “Password” (Click on the ellipsis ‘…’ to insert in secure DB)
8. Insert “API Key” (located in Zscaler UI under Administration > API Key Management)
9. Click Launch

![Figure 14: Install Zscaler Collector](image)
3.4.1 Validate Zscaler Collector Install

A check mark in the “running” column will indicate that the Zscaler task is still running and collecting data from your Zscaler instance. Once the check mark disappears from the column, the Zscaler collection is complete. You can watch the progress of the collection by bringing focus to the message tab located in the bottom half of the screen. In the messages window a line will appear with “Success” indicating that the collection was successful and is now being incorporated into your Skybox Model. You have now successfully ingested your Zscaler instances into the Skybox Model. Adding Zscaler will allow you to run analytics on Access policy compliance, Access rule Compliance, Change Tracking and much more.

Figure 15: Validate Zscaler Collector Install
3.4.2 Zscaler Firewall in the Skybox network map

This is what your Skybox network map should look like.

Figure 16: Skybox Network Map
4 Requesting Zscaler Support

4.1 Gather Support Information

Zscaler support is required to provision new locations for GRE or IPsec service. Zscaler support is also available to help troubleshoot configuration and service issues, and is available 24/7 hours a day, all year.

4.1.1 Obtain Company ID

First, let’s grab our Company ID, which is how Zscaler uniquely identifies a given customer. The navigation is: Administration -> Settings -> and then click Company profile.

![Obtaining Company ID](image)

Figure 17: Obtaining Company ID
4.1.2 Save Company ID

Your company ID can be found in the red box below. Please copy this ID somewhere convenient as we will need it in subsequent screens.

Figure 18: Save Company ID
4.1.3 Enter Support Section

Now that we have our company ID, we are ready to open a support ticket. The navigation is: “?” -> Support -> and then click Submit a Ticket.

Figure 19: Enter Support Section
5 Appendix A: Zscaler Resources

Zscaler: Getting Started
https://help.zscaler.com/zia/getting-started

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/
Appendix B: Skybox Resources

Skybox’s Website
https://www.skyboxsecurity.com/

Skybox Support
https://www.skyboxsecurity.com/support/portal