# ZSCALER AND SKYBOX DEPLOYMENT GUIDE

MAY 2022, VERSION 1.3

BUSINESS DEVELOPMENT GUIDE

# Contents

# Terms and Acronyms

The following terms and acronyms are used in this document.

| Acronym | Definition |
|---|---|
| CA | Central Authority (Zscaler) |
| CASB | Cloud Access Security Broker |
| CSV | Comma-Separated Values |
| DLP | Data Loss Prevention |
| DPD | Dead Peer Detection (RFC 3706) |
| GRE | Generic Routing Encapsulation (RFC2890) |
| IKE | Internet Key Exchange (RFC2409) |
| IPS | Intrusion Prevention System |
| IPSec | Internet Protocol Security (RFC2411) |
| OAM | Operation, Administration, and Management |
| PFS | Perfect Forward Secrecy |
| PSK | Pre-Shared Key |
| SCIM | System for Cross-Domain Identity Management |
| SSL | Secure Socket Layer (RFC6101) |
| TLS | Transport Layer Security (RFC5246) |
| XFF | X-Forwarded-For (RFC7239) |
| ZIA | Zscaler Internet Access (Zscaler) |
| ZPA | Zscaler Private Access (Zscaler) |

# About This Document

The following section provides an overview of the partners in this integration.

## Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, go to Zscaler's website or follow Zscaler on Twitter @zscaler.

## Skybox Overview

Skybox lets customers visualize and analyze hybrid, multi-cloud, and OT networks to gain full context and understanding of their attack surface. Skybox provides a platform that aggregates essential data from a wide range of security, cloud, and network technologies to create a network model that visualizes all security controls and network configurations. With the model, they conduct exposure analysis to determine which attack vectors or network paths could be used to gain access to vulnerable systems. Next, they calculate risk scores by factoring in CVSS severity, exploitability, asset importance, and asset exposure. Then, they offer remediation options based on risk and business impact assessments. Go to Skybox's website for more information.

## Prerequisites

### ZIA

- A working instance of ZIA 5.7 (or newer).
- Administrator login credentials to ZIA.
- ZIA API enabled (if you have not enabled API support prior, open a Zscaler support ticket requesting this be enabled).

### Skybox

- Administrator login credentials to Skybox.
- License for Skybox Firewall Assurance.
- Enable Skybox to use NTP.

## Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- Skybox Resources

## Software Versions

This document was written using ZIA v5.7 and Skybox 10.0.304 (Build 109).

## Request for Comments

- **For prospects and customers**: We value reader opinions and experiences. Contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

# Zscaler and Skybox Introduction

This deployment guide provides 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, contact Zscaler or Skybox for post-sale deployment assistance.

The next sections describe Zscaler and Skybox applications referenced in this deployment guide.

## ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet onramp— just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, CASB, and Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

### Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

| Name | Definition |
|---|---|
| ZIA Help Portal | Help articles for ZIA. |
| Zscaler Tools | Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs. |
| Zscaler Training and Certification | Training designed to help you maximize Zscaler products. |
| Submit a Zscaler Support Ticket | Zscaler support portal for submitting requests and issues. |

## Skybox Firewall Assurance Overview

Firewall Assurance improves cyber hygiene and risk management with centralized, optimized firewall management.

- **Connect and centralize**. Centrally manage traditional, next–gen, virtual, and cloud–based firewalls and secure access service edge (SASE) solutions from multiple vendors, as well as manage east–west and north–south traffic easily and effectively
- **Automate and optimize**. Automate and improve cyber hygiene tasks, including logging, configuration, and change tracking. Find and eliminate redundant, shadowed, or overly permissive firewall rules. You can conduct rule usage analysis, optimize rules, and complete faster ruleset audits, as well as automate and customize firewall reporting.
- **Improve security and reduce compliance risk**. Detect access policy violations, rule conflicts, and misconfigurations. You can ensure compliance for configurations, rules, and firewall access, as well as identify vulnerabilities within your firewalls and mitigate potential exploits leveraging Skybox Threat Intelligence.

### Skybox Resources

The following table contains links to Skybox support resources.

| Name | Definition |
|---|---|
| Skybox Website | Skybox platform and company website. |
| Skybox Support | Submit a help ticket for Skybox products. |

# Configuring ZIA for Skybox

This section documents configuring ZIA for use with Skybox.

## Logging into ZIA

First, setup the Zscaler side of this service. Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, contact support.

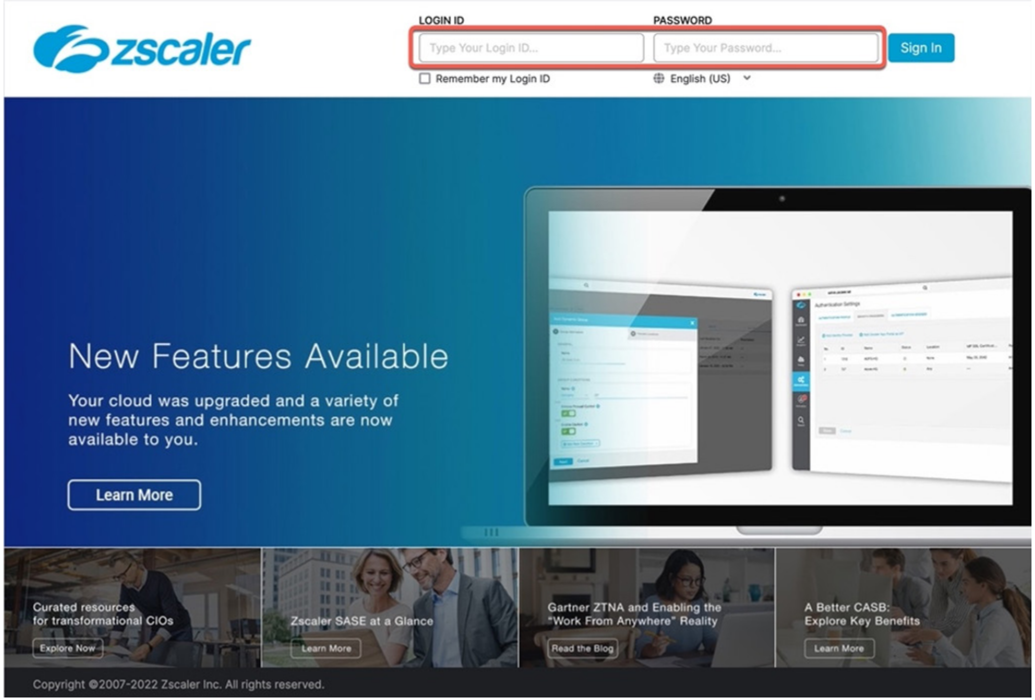

zscaler
LOGIN ID
Type Your Login ID...
PASSWORD
Type Your Password...
Sign In
Remember my Login ID
English (US)
New Features Available
Your cloud was upgraded and a variety of new features and enhancements are now available to you.
Learn More
Curated resources for transformational CIOs
Explore Now
Zscaler SASE at a Glance
Learn More
Gartner ZTNA and Enabling the "Work From Anywhere" Reality
Read the Blog
A Better CASB: Explore Key Benefits
Learn More
Copyright ©2007-2022 Zscaler Inc. All rights reserved.

*Figure 1. Logging into Zscaler*

# Obtain ZIA API Key

Next, you'll need to obtain an API key.

### Navigate to API Key Management

To create an API key, navigate to: **Administration** > **Cloud Service API Key Management**.

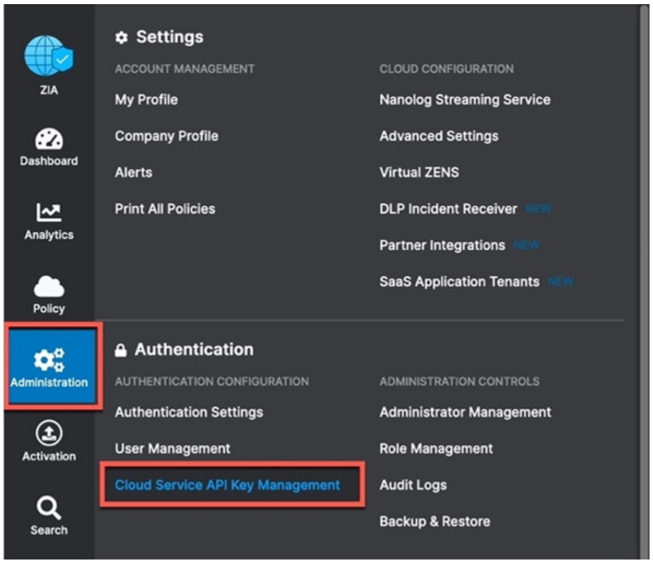
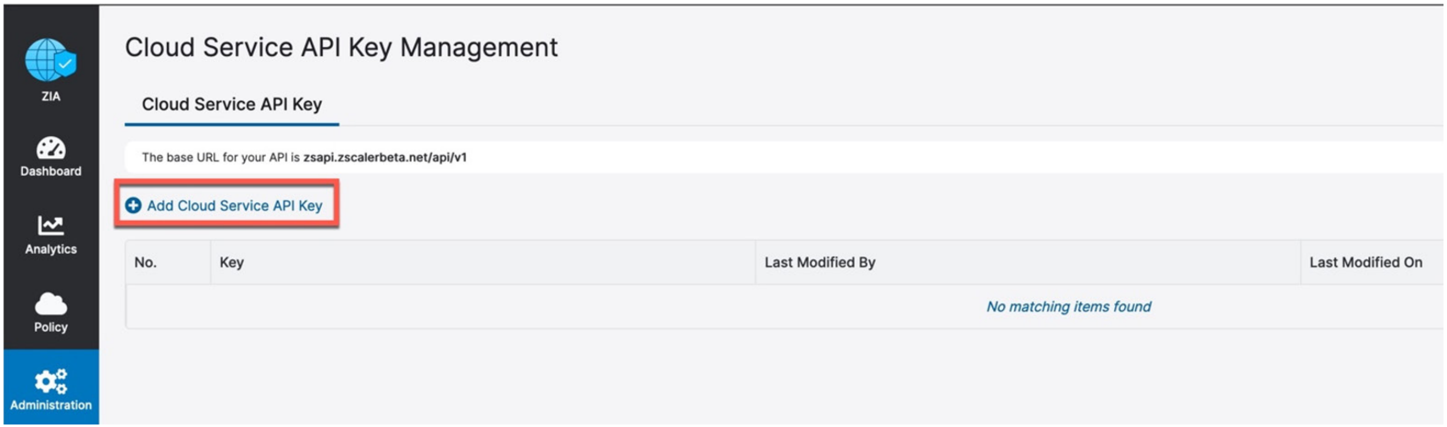


*Figure 2. Cloud Service API Key Management*

If you do not see **Cloud Service API Key Management** it means you haven't enabled ZIA API support for your ZIA instance. Open a Zscaler support ticket and request it enabled.

### Add API Key

Select **Add Cloud Service API Key**.



Cloud Service API Key Management

Cloud Service API Key

The base URL for your API is **zsapi.zscalerbeta.net/api/v1**

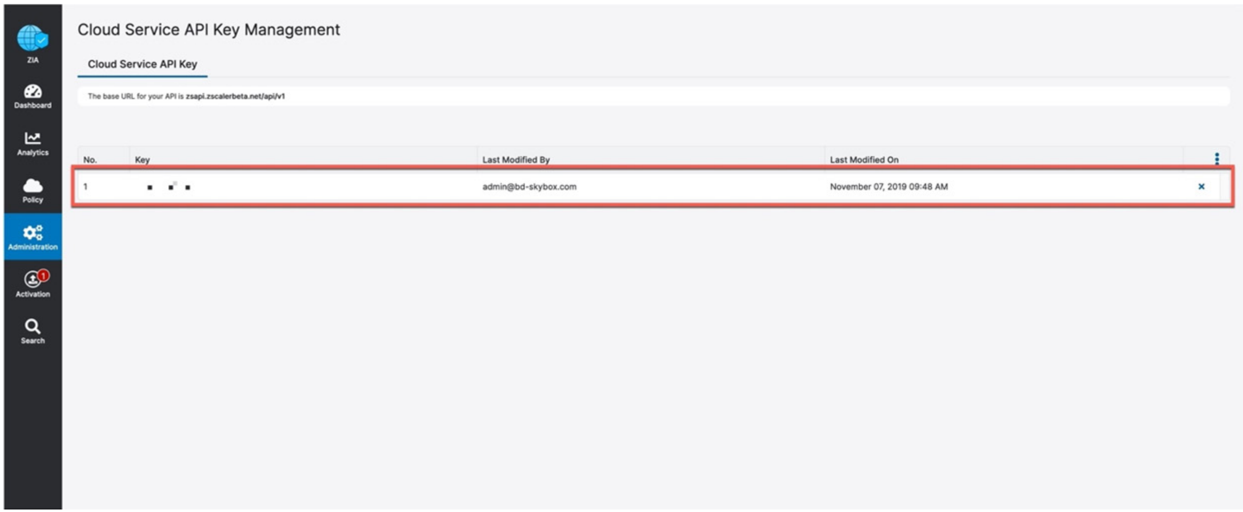
Add Cloud Service API Key

| No. | Key | Last Modified By | Last Modified On |
|---|---|---|---|
| *No matching items found* | | | |

*Figure 3. Add Cloud Service API Key*

### Verify API Key

An API key is generated after selecting Add Cloud Service API Key. Your screen should match this one.



Cloud Service API Key Management

Cloud Service API Key

The base URL for your API is **zsapi.zscalerbeta.net/api/v1**

| No. | Key | Last Modified By | Last Modified On | |
|---|---|---|---|---|
| 1 | [redacted] | admin@bd-skybox.com | November 07, 2019 09:48 AM | × |

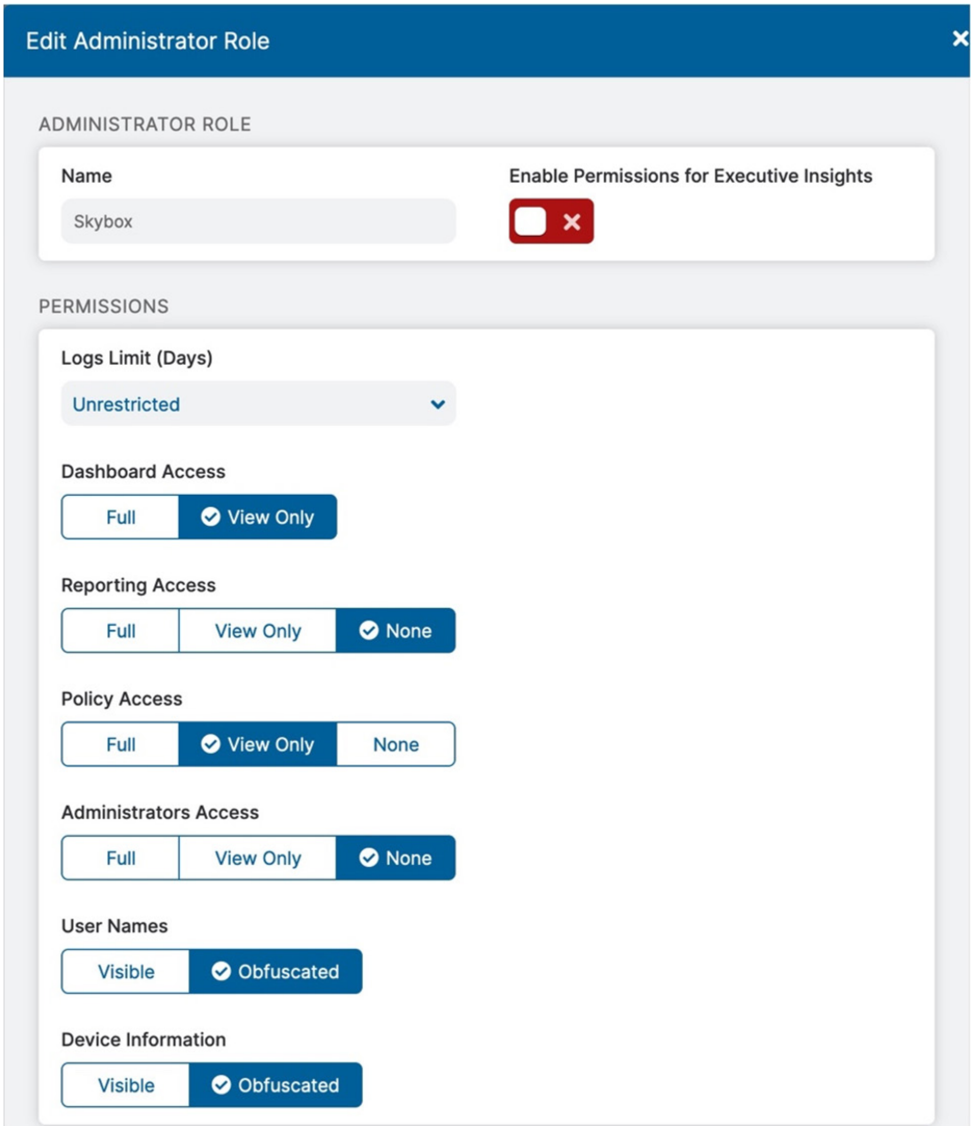
*Figure 4. Obtain ZIA API key*

## Create ZIA Administrator for Skybox

You need to create a ZIA administrator for Skybox.

### Add Administrator Role

1. Navigate to: **Administration** > **Role Management** > **Add Administrator Role**. The Administrator role settings for Skybox should match those shown in the Edit Administrator Role window.



Edit Administrator Role

ADMINISTRATOR ROLE

Name: Skybox

Enable Permissions for Executive Insights: ☒

PERMISSIONS

Logs Limit (Days): Unrestricted

Dashboard Access: Full [✓ View Only]

Reporting Access: Full View Only [✓ None]

Policy Access: Full [✓ View Only] None

Administrators Access: Full View Only [✓ None]

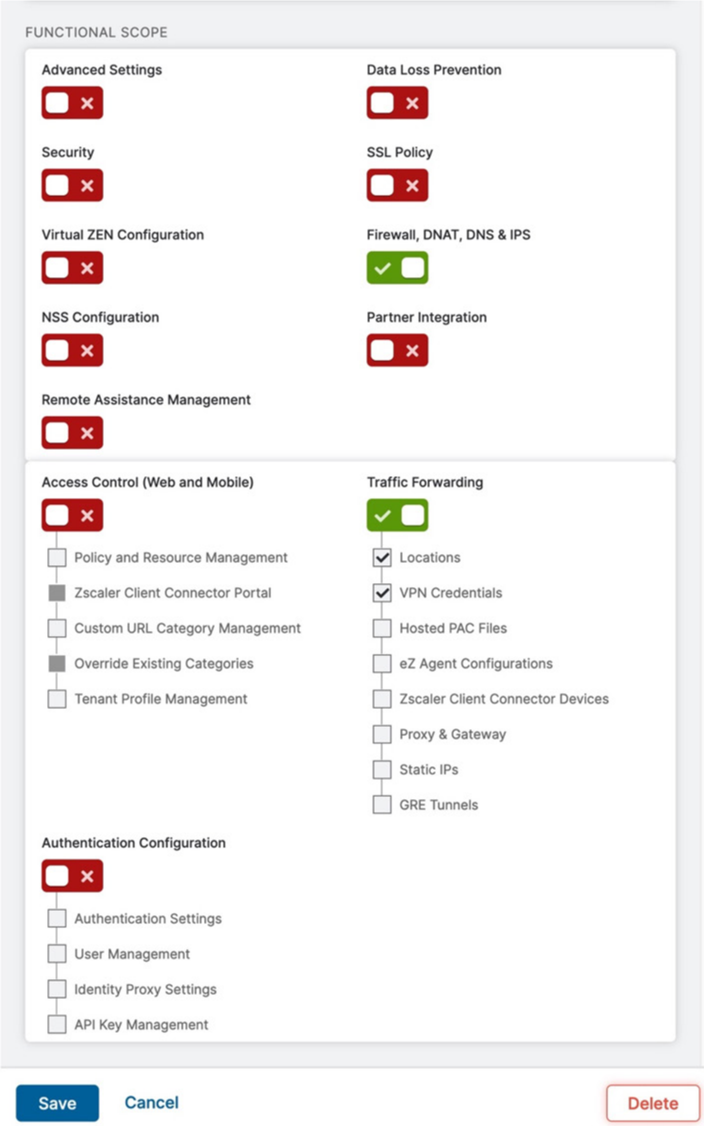
User Names: Visible [✓ Obfuscated]

Device Information: Visible [✓ Obfuscated]

*Figure 5. Configure Admin Role Permissions*

The screen capture only shows the top portion of this web form. You need to scroll down to see all the settings, which are shown in the next section of this document.

2. Match the settings shown in the Functional Scope window, and click Save.



FUNCTIONAL SCOPE

Advanced Settings ✗

Data Loss Prevention ✗

Security ✗

SSL Policy ✗

Virtual ZEN Configuration ✗

Firewall, DNAT, DNS & IPS ✓

NSS Configuration ✗

Partner Integration ✗

Remote Assistance Management ✗

Access Control (Web and Mobile) ✗

- □ Policy and Resource Management
- ■ Zscaler Client Connector Portal
- □ Custom URL Category Management
- ■ Override Existing Categories
- □ Tenant Profile Management

Traffic Forwarding ✓

- ☑ Locations
- ☑ VPN Credentials
- □ Hosted PAC Files
- □ eZ Agent Configurations
- □ Zscaler Client Connector Devices
- □ Proxy & Gateway
- □ Static IPs
- □ GRE Tunnels

Authentication Configuration ✗

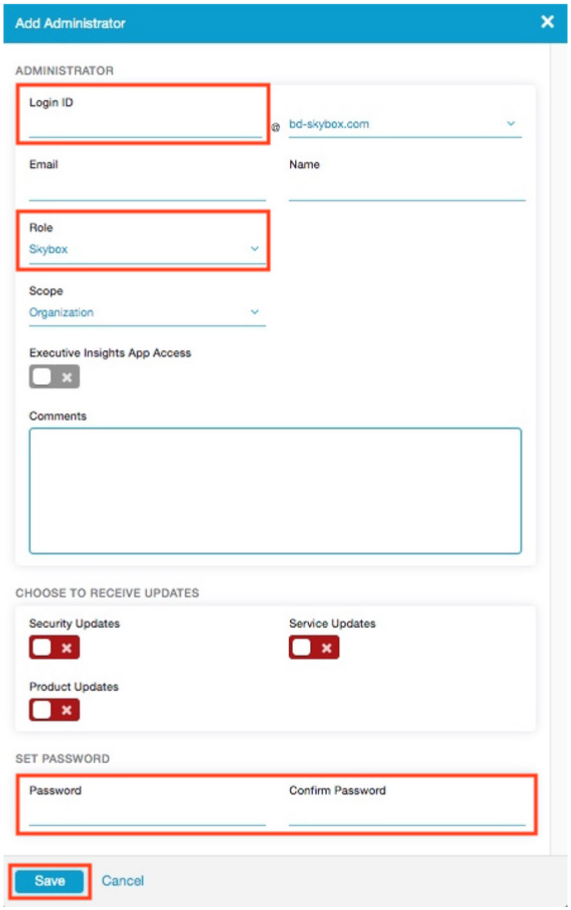
- □ Authentication Settings
- □ User Management
- □ Identity Proxy Settings
- □ API Key Management

*Figure 6. Configure Admin role functional scope*

## Add Administrator for Skybox

Now that we have our Administrator Role, configure a new Administrator account and apply this role to it.

Navigate to **Administration** > **Administrator Management** > **Add Administrator**.


Add Administrator

ADMINISTRATOR

Login ID @ bd-skybox.com

Email

Name

Role: Skybox

Scope: Organization

Executive Insights App Access ✕

Comments

CHOOSE TO RECEIVE UPDATES

Security Updates ✕

Service Updates ✕

Product Updates ✕

SET PASSWORD

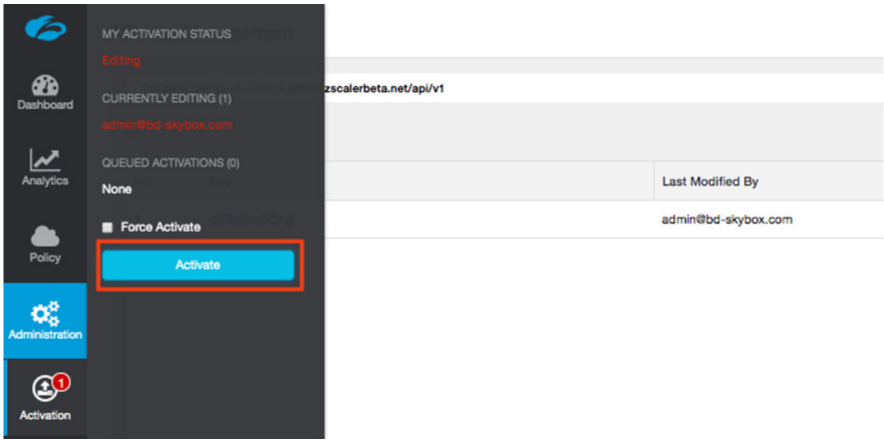
Password

Confirm Password

*Figure 7. Add Administrator*

## Activate

You should now active all pending changes. After you have completed this set, configure Skybox.


MY ACTIVATION STATUS

Editing

CURRENTLY EDITING (1)

admin@bd-skybox.com

QUEUED ACTIVATIONS (0)

None

zscalerbeta.net/api/v1

| Last Modified By |
|---|
| admin@bd-skybox.com |

*Figure 8. Activate pending configuration changes*

# Configuring Skybox

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

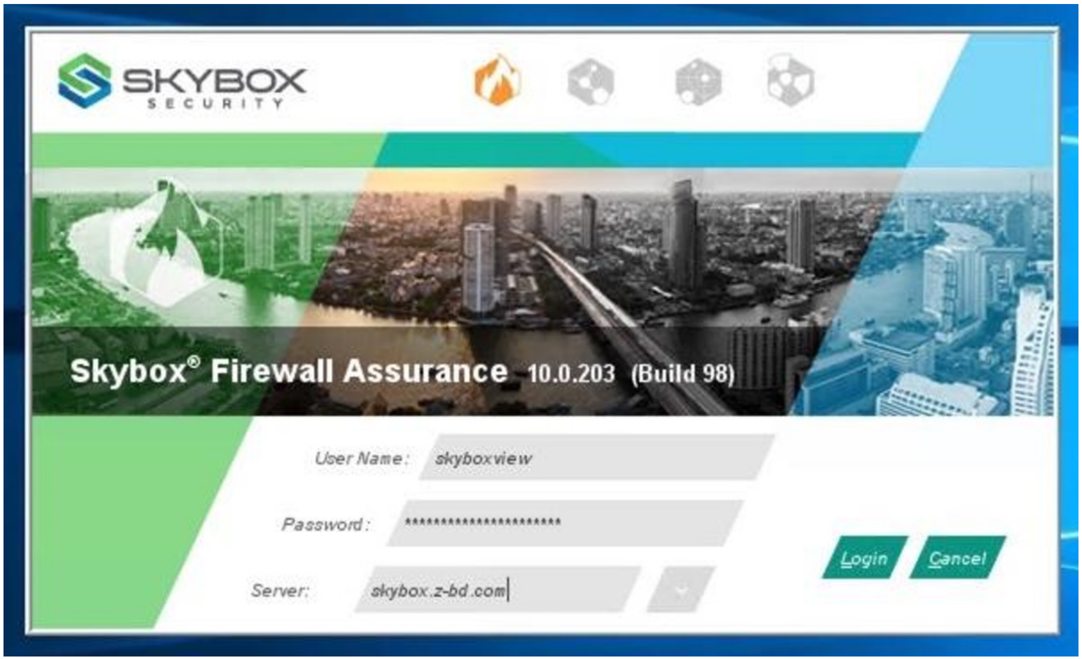
The information collected from the ZIA service can be used in Skybox in a variety of use cases:

- **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**: Users can see the firewall with all connections (VPN/GRE tunnels) to on-premises equipment. (Network Map)

Skybox collects the Zscaler secure web gateway information by the out-of-box collection task, which is launched in a regular schedule to ensure the Skybox platform is updated with the latest information from the Zscaler solution.

## Log into Skybox Firewall Assurance

Log in to Skybox Firewall Assurance with admin credentials.



User Name: skyboxview
Password: **********************
Server: skybox.z-bd.com

*Figure 9. Log into Skybox*

## Open Operational Console

After you have your Skybox Appliance or Skybox Virtual Appliance installed and licensed, you can start configuring the Skybox software and adding the tasks needed to collect your Zscaler instances.

You 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. Click on the **Operational Console** at the top and in the middle of the **Firewall Assurance** window.

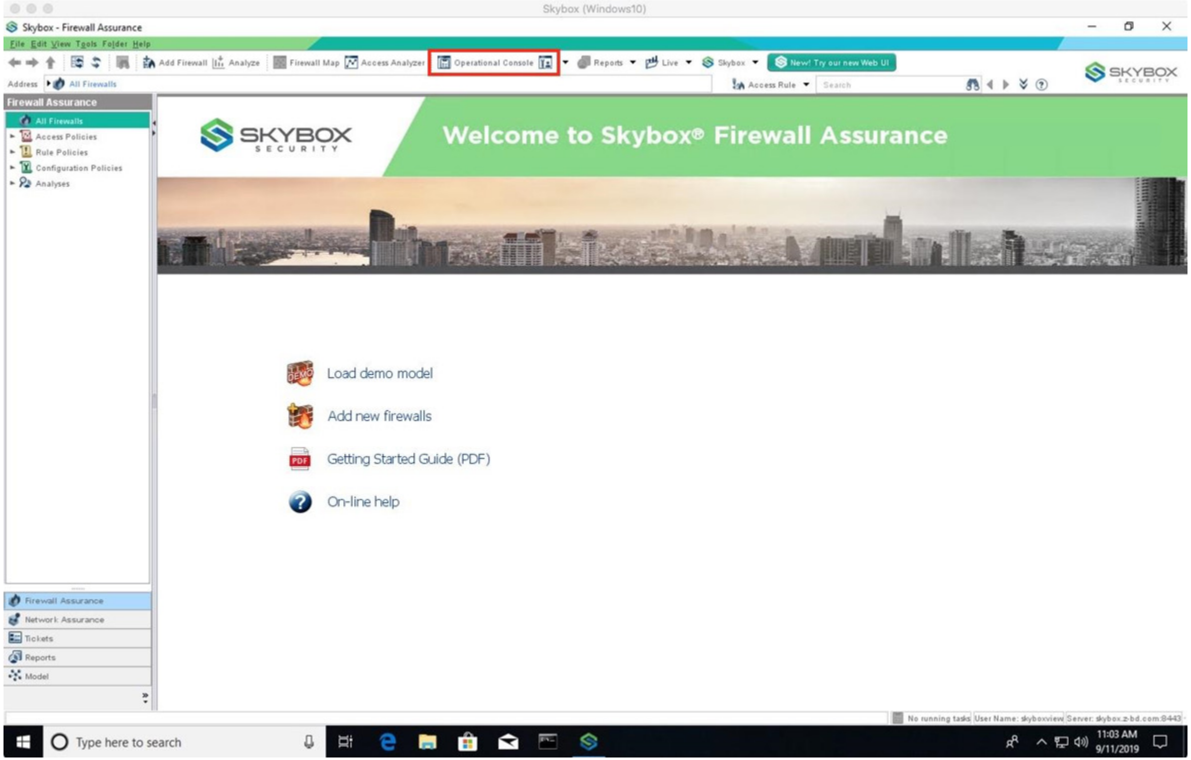
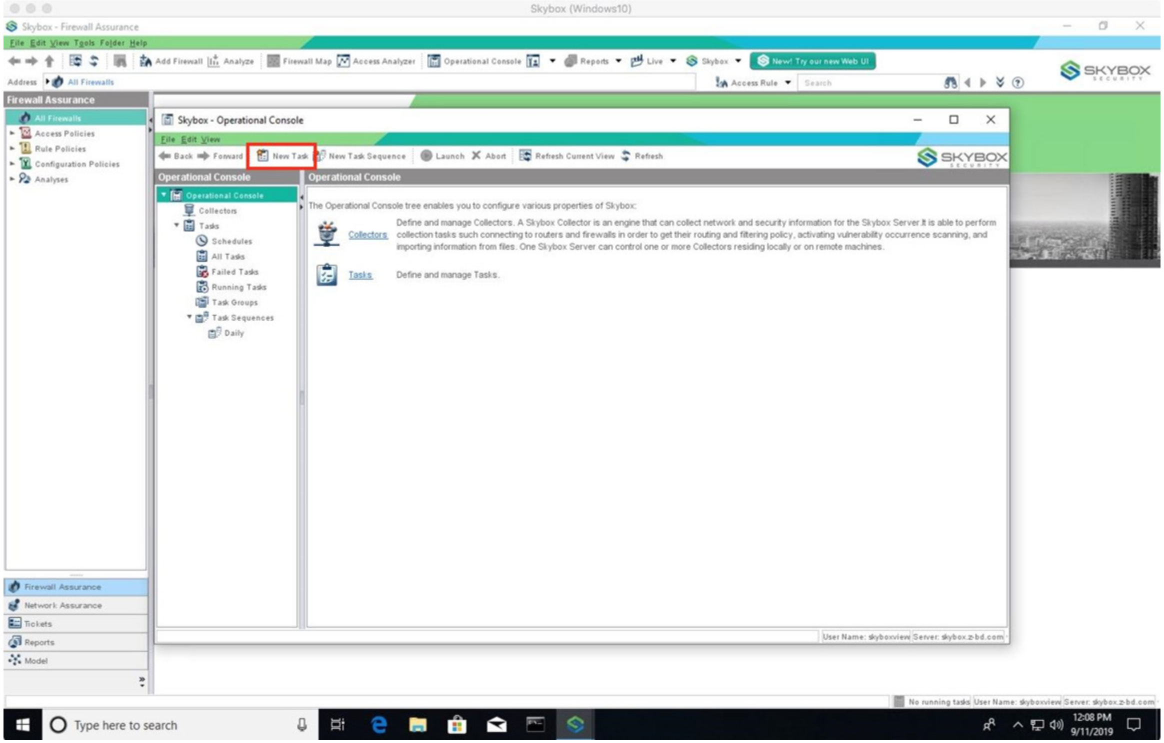


*Figure 10. Open Operational Console*

## 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 need to install python to proceed with collecting Zscaler into the Skybox Model.

In the **Operation Console** click on **New Task** to open the New Task window to configure a task that installs Python on the Skybox Server.



Operational Console

The Operational Console tree enables you to configure various properties of Skybox:

Collectors — Define and manage Collectors. A Skybox Collector is an engine that can collect network and security information for the Skybox Server.It is able to perform collection tasks such connecting to routers and firewalls in order to get their routing and filtering policy, activating vulnerability occurrence scanning, and importing information from files. One Skybox Server can control one or more Collectors residing locally or on remote machines.

Tasks — Define and manage Tasks.

User Name: skyboxview Server: skybox.z-bd.com

No running tasks User Name: skyboxview Server: skybox.z-bd.com

*Figure 11. Install Python 2.7*

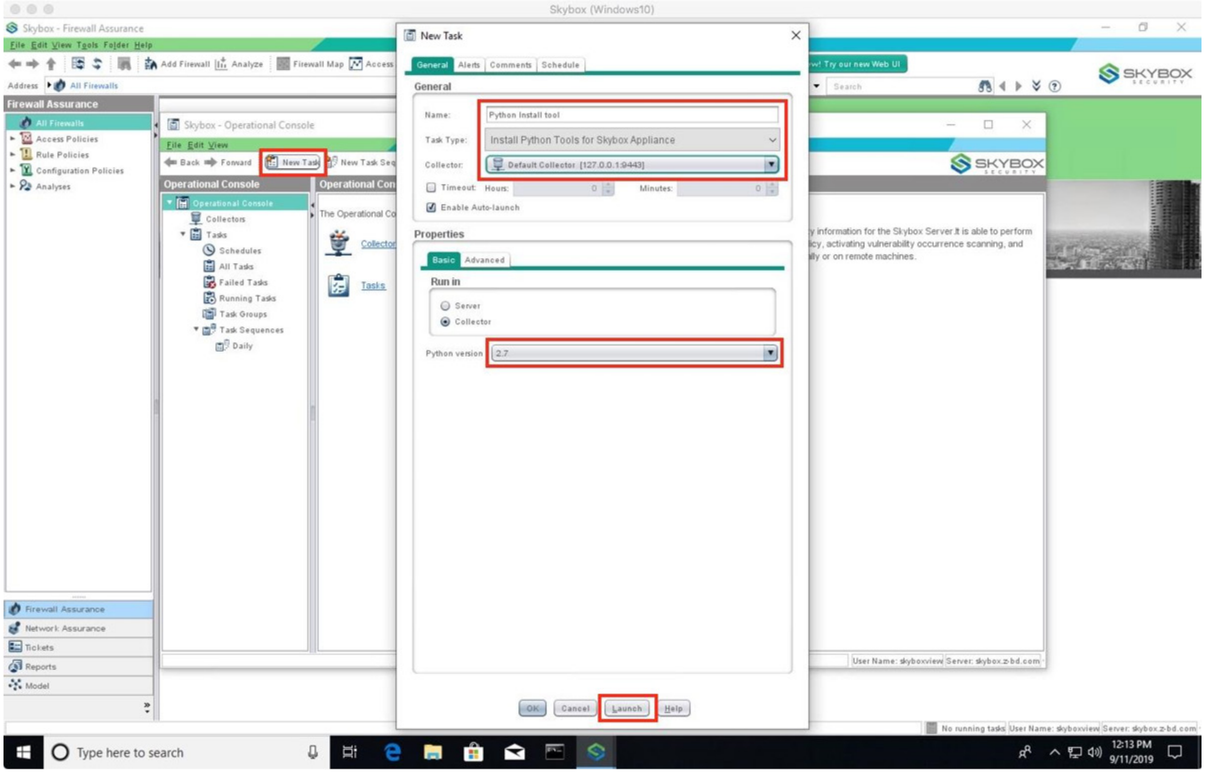
### Install Python

You should only run the Python installation task once. After successfully installing Python, you do not need to re-run the task.

Insert the necessary task configurations for installing Python into the **New Task** window. After it opens:

1. Insert a **Name** in the corresponding field. A name that briefly describes what you are doing with this task is 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 two letters of the word `Python` the task selection automatically narrows down to tasks.
3. Choose the collector that collects the Zscaler instances. If you have only one Skybox Server, more than likely you are 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 appears in this field. Select the collector you would like to use to collect Zscaler.

4. Leave the **Timeout** and **Enable Auto Launch** as their defaults:
   - The timeout is the amount of time needed for the task to run before it times out. This can be increased for environments with high latency. Leave this as the default for the purposes of this collection.
   - **Enable Auto Launch** allows this task to launch on its own. You can schedule a specific time that this task launches under the **Schedule** tab at the top of the task window. Leave this as default ( 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 probably running both the 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 (Zscaler requires Python 2.7 installation).
7. Click **Launch**. The **Alerts**, **Comments**, and **Schedule** tabs at the top of the task are for the following additional configurations:
   - **Alerts**. You can configure email and error level preferences in this tab
   - **Comments**. Insert comments regarding this task
   - **Schedule**. You can specify, down to the minute, when you would like to auto-launch this task


New Task

General

Name: Python Install tool

Task Type: Install Python Tools for Skybox Appliance

Collector: Default Collector [127.0.0.1:9443]

☐ Timeout Hours: 0 Minutes: 0

☑ Enable Auto-launch

Properties

Run in

○ Server

● Collector

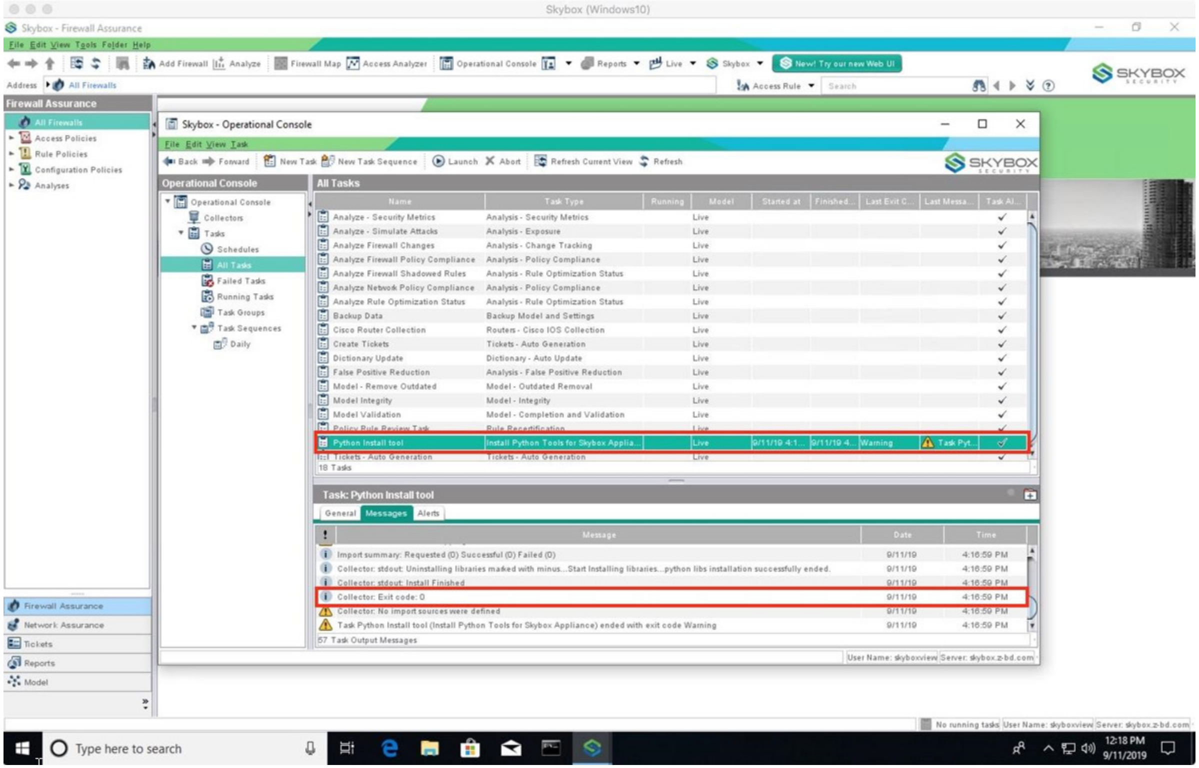
Python version 2.7

Figure 12. Install Python

### 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 need to install Python at the OS Level, not in the Skybox Software.

After you have launched the **Install Python Tools** task, it runs for about five to ten minutes (depending on the resources allocated for this VM).



All Tasks

| Name | Task Type | Running | Model | Started at | Finished... | Last Exit C... | Last Messa... | Task Al... |
|---|---|---|---|---|---|---|---|---|
| Analyze - Security Metrics | Analysis - Security Metrics | | Live | | | | | ✓ |
| Analyze - Simulate Attacks | Analysis - Exposure | | Live | | | | | ✓ |
| Analyze Firewall Changes | Analysis - Change Tracking | | Live | | | | | ✓ |
| Analyze Firewall Policy Compliance | Analysis - Policy Compliance | | Live | | | | | ✓ |
| Analyze Firewall Shadowed Rules | Analysis - Rule Optimization Status | | Live | | | | | ✓ |
| Analyze Network Policy Compliance | Analysis - Policy Compliance | | Live | | | | | ✓ |
| Analyze Rule Optimization Status | Analysis - Rule Optimization Status | | Live | | | | | ✓ |
| Backup Data | Backup Model and Settings | | Live | | | | | ✓ |
| Cisco Router Collection | Routers - Cisco IOS Collection | | Live | | | | | ✓ |
| Create Tickets | Tickets - Auto Generation | | Live | | | | | ✓ |
| Dictionary Update | Dictionary - Auto Update | | Live | | | | | ✓ |
| False Positive Reduction | Analysis - False Positive Reduction | | Live | | | | | ✓ |
| Model - Remove Outdated | Model - Outdated Removal | | Live | | | | | ✓ |
| Model Integrity | Model - Integrity | | Live | | | | | ✓ |
| Model Validation | Model - Completion and Validation | | Live | | | | | ✓ |
| Policy Rule Review Task | Rule Recertification | | Live | | | | | ✓ |
| Python Install tool | Install Python Tools for Skybox Applia... | | Live | 9/11/19 4:1... | 9/11/19 4... | Warning | ⚠ Task Pyt... | ✓ |
| Tickets - Auto Generation | Tickets - Auto Generation | | Live | | | | | ✓ |

18 Tasks

Task: Python Install tool

General | Messages | Alerts

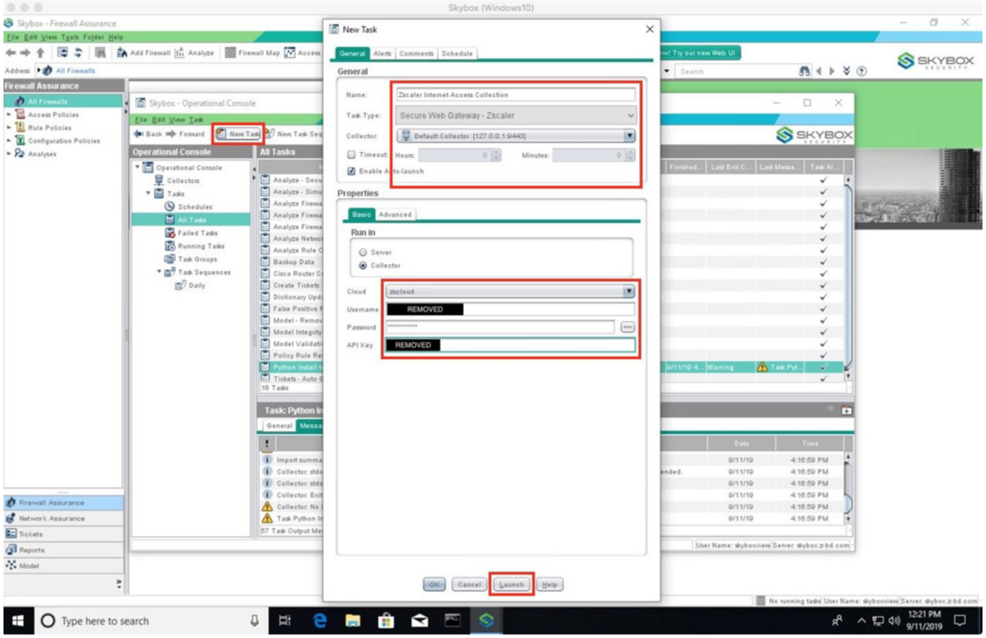
| ! | Message | Date | Time |
|---|---|---|---|
| i | Import summary: Requested (0) Successful (0) Failed (0) | 9/11/19 | 4:16:59 PM |
| i | Collector: stdout: Uninstalling libraries marked with minus...Start Installing libraries...python libs installation successfully ended. | 9/11/19 | 4:16:59 PM |
| i | Collector: stdout: Install Finished | 9/11/19 | 4:16:59 PM |
| i | Collector: Exit code: 0 | 9/11/19 | 4:16:59 PM |
| ⚠ | Collector: No import sources were defined | 9/11/19 | 4:16:59 PM |
| ⚠ | Task Python Install tool (Install Python Tools for Skybox Appliance) ended with exit code Warning | 9/11/19 | 4:16:59 PM |

57 Task Output Messages

*Figure 13. Validate Python install*

## Create New Task: Zscaler Collector

1. Open the **Operation Console**.
2. Click **New Task**.
3. Name. The name of the task you're creating (e.g., Zscaler collection).
4. Add Zscaler as the **Task Type**. If you type the first two letters of the task type (such as "zs") the Zscaler task appears in the task type drop-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.
5. Leave **Timeout** as default.
6. Leave **Enable Auto Launch** as default.
7. Choose **Server** or **Collector**. If you have only one Skybox Server, choose **Collector** as you are typically running both on a single instance of Skybox.
8. Choose Zscaler for the **Cloud** (provided by Zscaler and indicated as the host of the URL from your ZIA Admin Portal).
9. Add the admin **Username**.
10. Add the admin **Password** (click on the ellipsis **...** to insert in secure DB).
11. Add the **API Key** (located in Zscaler Admin Portal under **Administration** > **API Key Management**).
12. Click **Launch**.



Name: Zscaler Internet Access Collection

Task Type: Secure Web Gateway - Zscaler

Collector: Default Collector [127.0.0.1:9443]

☐ Timeout: Hours: 0 Minutes: 0

☑ Enable Auto-launch

Properties

Run in: ○ Server ● Collector

Cloud: zscloud

Username: REMOVED

Password: ************

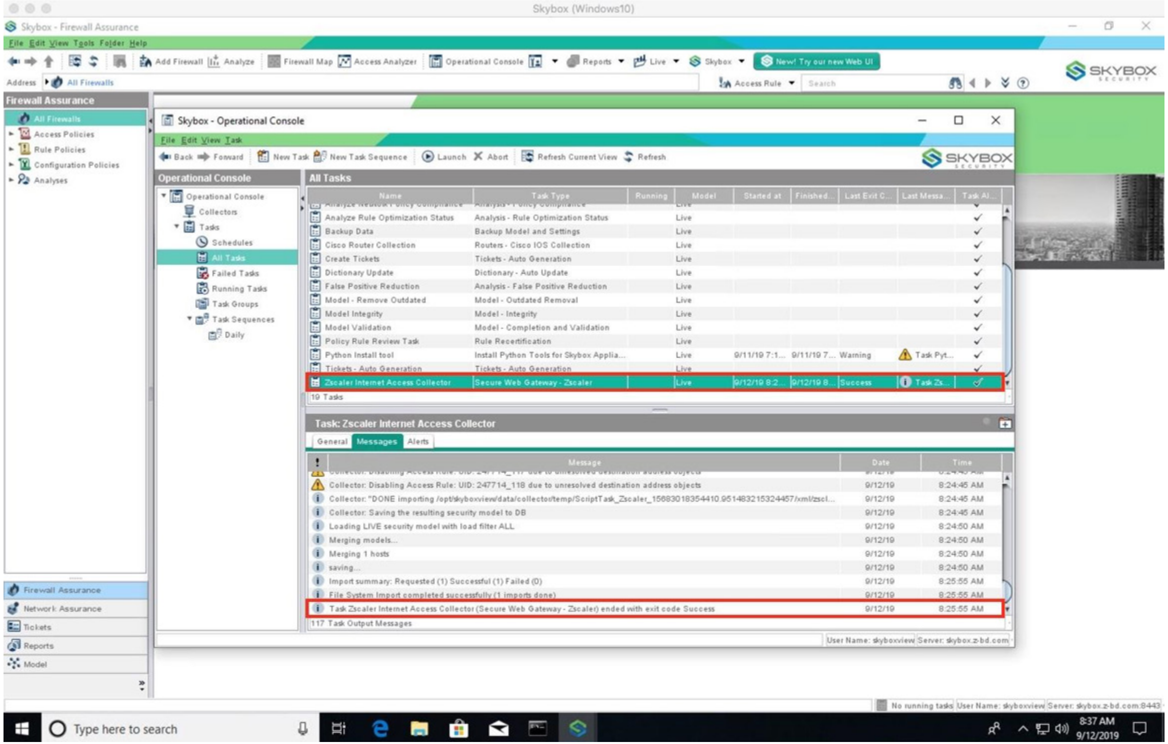
API Key: REMOVED

Figure 14. *Install Zscaler Collector*

### Validate Zscaler Collector Install

A check mark in the **Running** column indicates that the Zscaler task is still running and collecting data from your Zscaler instance. After 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 appears with **Success**, indicating that the collection was successful and is now being incorporated into your Skybox Model.

You have successfully ingested your Zscaler instances into the Skybox Model. Adding Zscaler allows you to run analytics on **Access Policy Compliance**, **Access Rule Compliance**, **Change Tracking**, and more.



All Tasks

| Name | Task Type | Running | Model | Started at | Finished... | Last Exit C... | Last Messa... | Task Al... |
|---|---|---|---|---|---|---|---|---|
| Analyze Network Policy Compliance | Analysis - Policy Compliance | | Live | | | | | ✓ |
| Analyze Rule Optimization Status | Analysis - Rule Optimization Status | | Live | | | | | ✓ |
| Backup Data | Backup Model and Settings | | Live | | | | | ✓ |
| Cisco Router Collection | Routers - Cisco IOS Collection | | Live | | | | | ✓ |
| Create Tickets | Tickets - Auto Generation | | Live | | | | | ✓ |
| Dictionary Update | Dictionary - Auto Update | | Live | | | | | ✓ |
| False Positive Reduction | Analysis - False Positive Reduction | | Live | | | | | ✓ |
| Model - Remove Outdated | Model - Outdated Removal | | Live | | | | | ✓ |
| Model Integrity | Model - Integrity | | Live | | | | | ✓ |
| Model Validation | Model - Completion and Validation | | Live | | | | | ✓ |
| Policy Rule Review Task | Rule Recertification | | Live | | | | | ✓ |
| Python Install tool | Install Python Tools for Skybox Applia... | | Live | 9/11/19 7:1... | 9/11/19 7... | Warning | ⚠ Task Pyt... | ✓ |
| Tickets - Auto Generation | Tickets - Auto Generation | | Live | | | | | ✓ |
| Zscaler Internet Access Collector | Secure Web Gateway - Zscaler | | Live | 9/12/19 8:2... | 9/12/19 8... | Success | ⓘ Task Zs... | ✓ |

19 Tasks

Task: Zscaler Internet Access Collector

General | Messages | Alerts

| ! | Message | Date | Time |
|---|---|---|---|
| ⚠ | Collector: Disabling Access Rule: UID: 247714_117 due to unresolved destination address objects | 9/12/19 | 8:24:45 AM |
| ⚠ | Collector: Disabling Access Rule: UID: 247714_118 due to unresolved destination address objects | 9/12/19 | 8:24:45 AM |
| ⓘ | Collector: "DONE importing /opt/skyboxview/data/collector/temp/ScriptTask_Zscaler_15683018354410.951483215324457/xml/zscl... | 9/12/19 | 8:24:45 AM |
| ⓘ | Collector: Saving the resulting security model to DB | 9/12/19 | 8:24:45 AM |
| ⓘ | Loading LIVE security model with load filter ALL | 9/12/19 | 8:24:50 AM |
| ⓘ | Merging models... | 9/12/19 | 8:24:50 AM |
| ⓘ | Merging 1 hosts | 9/12/19 | 8:24:50 AM |
| ⓘ | saving... | 9/12/19 | 8:24:50 AM |
| ⓘ | Import summary: Requested (1) Successful (1) Failed (0) | 9/12/19 | 8:25:55 AM |
| ⓘ | File System Import completed successfully (1 imports done) | 9/12/19 | 8:25:55 AM |
| ⓘ | Task Zscaler Internet Access Collector (Secure Web Gateway - Zscaler) ended with exit code Success | 9/12/19 | 8:25:55 AM |

117 Task Output Messages

User Name: skyboxview Server: skybox.z-bd.com

No running tasks User Name: skyboxview Server: skybox.z-bd.com:8443

*Figure 15. Validate Zscaler Collector install*

### Zscaler Firewall in the Skybox Network Map

This is what your Skybox network map should look like.

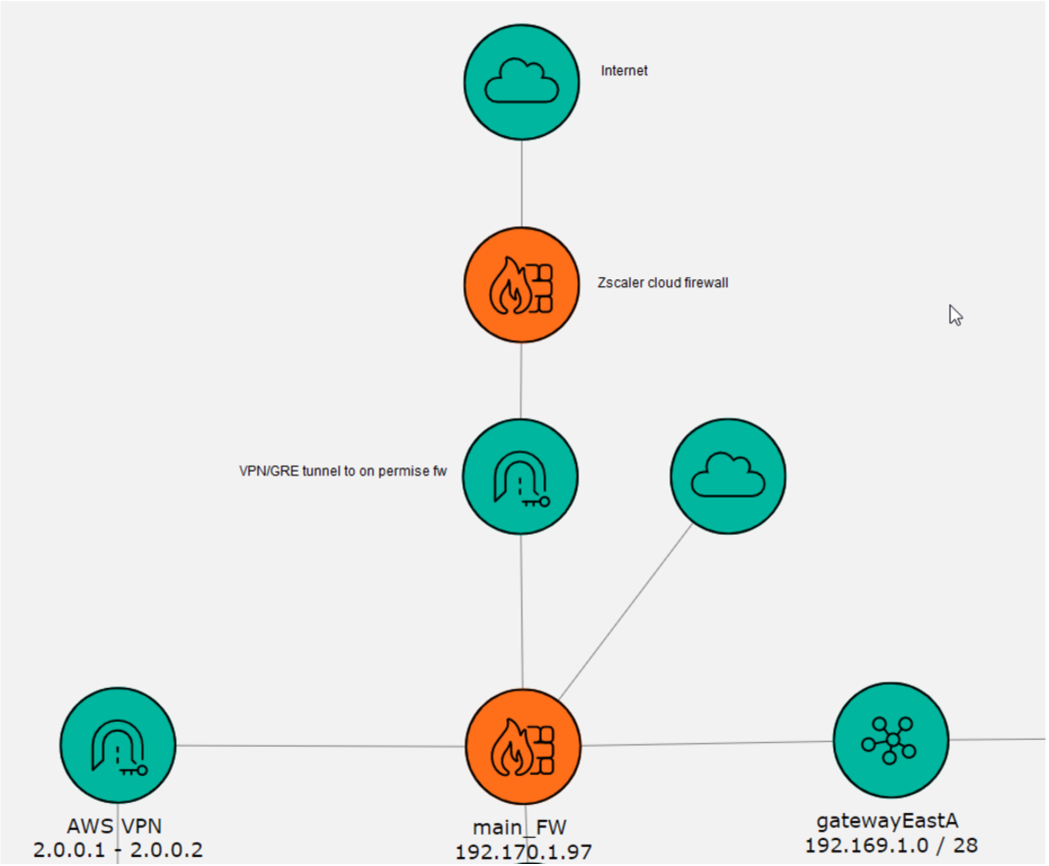


*Figure 16. Skybox Network Map*

# Appendix A: Requesting Zscaler Support

This section describes how to access your Zscaler support team.

## Gather Support Information

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round. To contact Zscaler support, select **Administration** > **Settings** > **Company profile**.

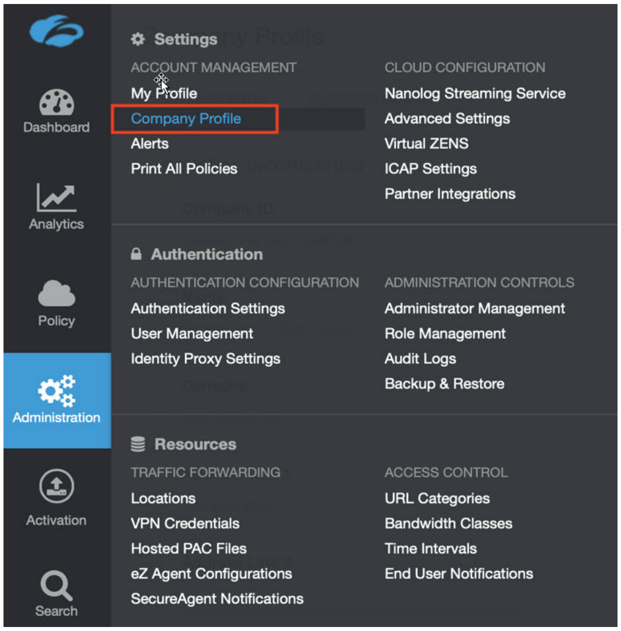
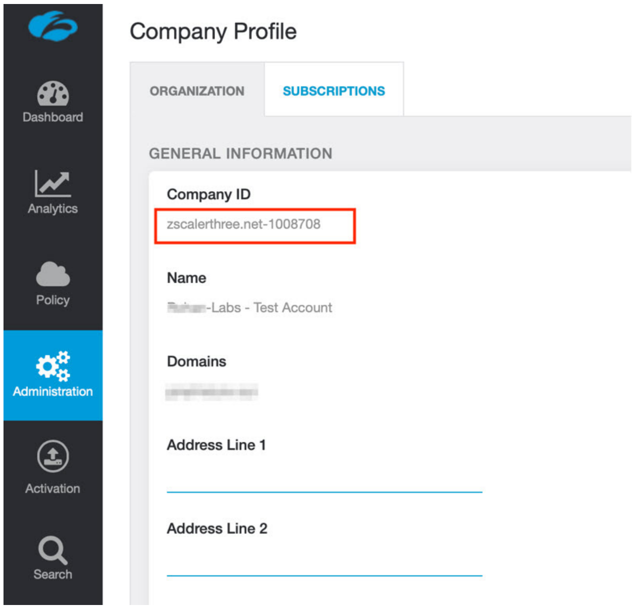


*Figure 17. Collecting details to open support case with Zscaler TAC*

### Save Company ID

Copy your Company ID.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

*Figure 18. Company ID*

### Enter Support Section

With your company ID information, you can open a support ticket. Navigate to **Dashboard** > **Support** > **Submit a Ticket**.

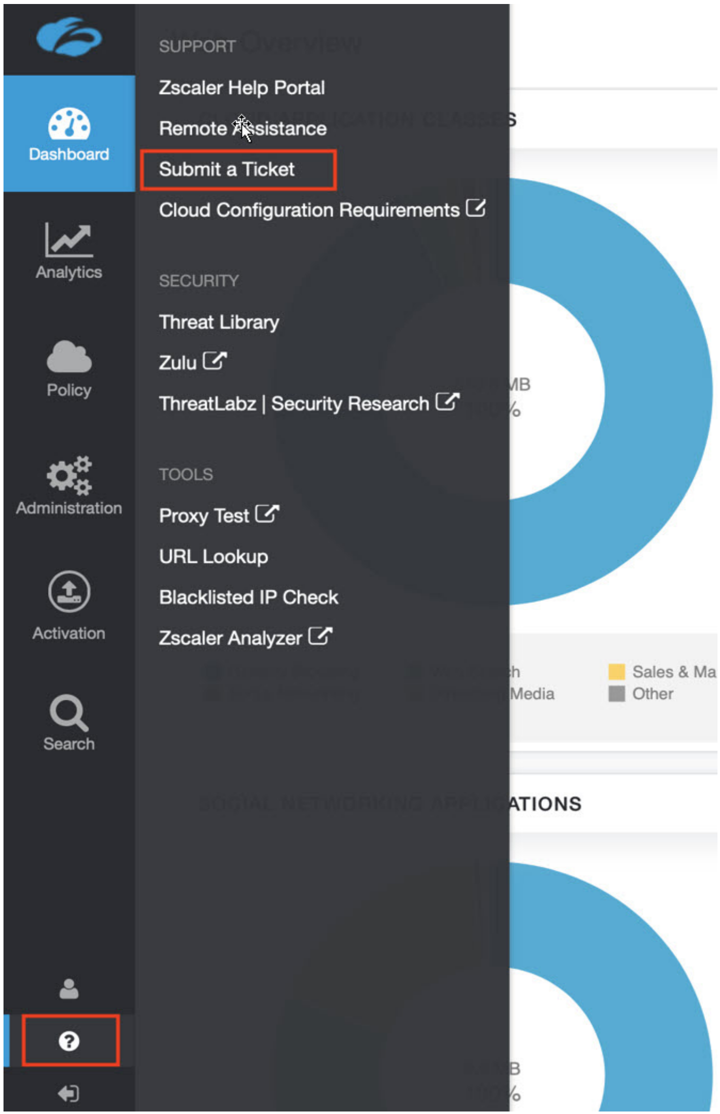


*Figure 19. Submit a Ticket*