



FIREMON

# ZSCALER AND FIREMON DEPLOYMENT GUIDE

# Contents

<b>Terms and Acronyms</b>	<b>3</b>
<b>About This Document</b>	<b>5</b>
Zscaler Overview	5
FireMon Overview	5
Audience	5
Software Versions	5
Request for Comments	5
<b>Zscaler and FireMon Introduction</b>	<b>6</b>
ZIA Overview	6
FireMon Security Intelligence Platform Overview	7
FireMon Resources	7
<b>Overview for Zscaler and FireMon SIP Integration</b>	<b>8</b>
<b>Setup the ZIA Account</b>	<b>9</b>
Configure ZIA	9
Role Management Permission Settings	10
API URL and Key	10
Policy Normalization	10
<b>Add Zscaler Management Station to FireMon SIP</b>	<b>11</b>
Configure SIP Administration Module	11
<b>Verify Normalization</b>	<b>13</b>
View Zscaler in the SIP Administration Module	13
View Zscaler in the SIP Security Manager Module	13
<b>Appendix A: Requesting Zscaler Support</b>	<b>14</b>

## Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SIP	Security Intelligence Platform
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

## Trademark Notice

© 2024 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at [zscaler.com/legal/trademarks](https://zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

## About This Document

The following sections describe the organizations and requirements of this deployment guide.

### 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. Its flagship 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. To learn more, see [Zscaler's website](#).

### FireMon Overview

FireMon, LLC has been at the forefront of the security management category, delivering first-ever functionality such as firewall behavior testing, workflow integration, traffic flow analysis, and rule recertification. The Security Intelligence Platform has helped more than 1,700 organizations around the world gain visibility into and control over their complex network security infrastructures. To learn more, refer to [FireMon's website](#).

### 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, see:

- [Zscaler Resources](#)
- [FireMon Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

### Software Versions

This document was authored using the latest version of Zscaler software.

### Request for Comments

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

# Zscaler and FireMon Introduction

Overviews of the Zscaler and FireMon applications are described in this section.



If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

## ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—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, and 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
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	Zscaler Support portal for submitting requests and issues.

## FireMon Security Intelligence Platform Overview

FireMon Policy Manager is a purpose-built network security policy management (NSPM) platform that automates the management of firewall and cloud security policies to increase the visibility, eliminate policy-related risk, accurately and quickly change rules, and meet internal and external compliance requirements.

- Increase visibility: Eliminate blind spots with a complete view of all firewall policies across the entire environment.
- Reduce risk: Remediate policy-related vulnerabilities with real-time visibility and control.
- Manage change: Avoid misconfigurations, accelerate business, and improve security.
- Enforce and maintain compliance: Avoid violations, avoid risk, and avoid fines.

## FireMon Resources

The following table contains links to FireMon support resources.

Name	Definition
<a href="#">FireMon User Center</a>	Online help and support for FireMon customers.

## Overview for Zscaler and FireMon SIP Integration

This guide explains the integration process for connecting the FireMon Security Intelligence Platform (SIP) and Zscaler.

An active SIP license is required for integration with Zscaler.



# Setup the ZIA Account

The following sections describe how to configure ZIA.

## Configure ZIA

To configure the ZIA:

1. Log in to your ZIA Admin Portal.
2. In the left-side navigation, go to **Administration > Authentication > Administration Management**.
3. Click **Administration Management**.
4. Click **Add Administrator**. The **Add Administrator** window is displayed.
5. In the **Add Administrator** window:
  - a. Enter an email for the Login ID. This is used for credentials in SIP.
  - b. Enter the email address for the user for **Email**.
  - c. Enter the name of the user for **Name**.
  - d. For **Role**, select **ReadOnly-adminRole** from the drop-down menu. (The permission settings for the ReadOnly-adminRole are in **Authentication > Role Management**.)
  - e. For **Scope**, select **Organization**.
  - f. Do not enable any **Update** settings.
  - g. Enter a **Password** for the account.
  - h. Click **Save**.
6. In the **Resources** section, click **Location Management**. This is where you'll set discovery for child devices. Child devices are listed as a sublocation.
7. Click **Add Location**:
  - a. Enter the server **Location** information.
    - Disable **Exclude from Manual Location Groups** and **Exclude from Dynamic Location Groups**.
  - b. For **Addressing**, select the **Static IP Addresses** and any **VPN Credentials**.
  - c. For **Gateway Options**, enable:
    - **Enforce Authentication**
    - **Enable SSL Inspection**
    - **Enforce Zscaler Client Connector SSL Setting**
    - **Enforce Firewall Control**
    - Disable **Enforce Bandwidth Control**.
8. Click **Save**.

## Role Management Permission Settings

If you want to add a role specifically for SIP, the following are the recommended permission settings for use with the ReadOnly-adminRole account.

1. In the ZIA Admin Portal, select **Administration > Role Management > Add Administrator Role**.
2. Enter a **Name** for this role (e.g., FM-readonly).
3. Disable **Enable Permissions for Executive Insights**.
4. Configure the following **Permissions** settings:
  - **Logs Limit (Days)**: Unrestricted
  - **Dashboard Access**: View Only
  - **Reporting Access**: Full
  - **Insights Access**: View Only
  - **Policy Access**: View Only
  - **Administrative Access**: None
  - **User Names**: Visible
5. Enable all the **Functional Scope** options.
6. Click **Save**.

## API URL and Key

You need the API URL and Key when adding Zscaler to SIP. To locate the API URL and Key, go to **Administration > API Key Management**.

## Policy Normalization

You can view the policies that are normalized by Security Manager.

1. On the left-side navigation, go to **Policy**.
2. Click **Firewall Control** and/or **URL & Cloud App Control**.

## Add Zscaler Management Station to FireMon SIP

The following sections describe adding ZIA management stations to FireMon SIP.

### Configure SIP Administration Module

To configure the SIP Administration Module:

1. Open the **SIP Administration** module.
2. On the toolbar, go to **Device > Management Stations**.
3. Select **Create > Zscaler > ZIA**.

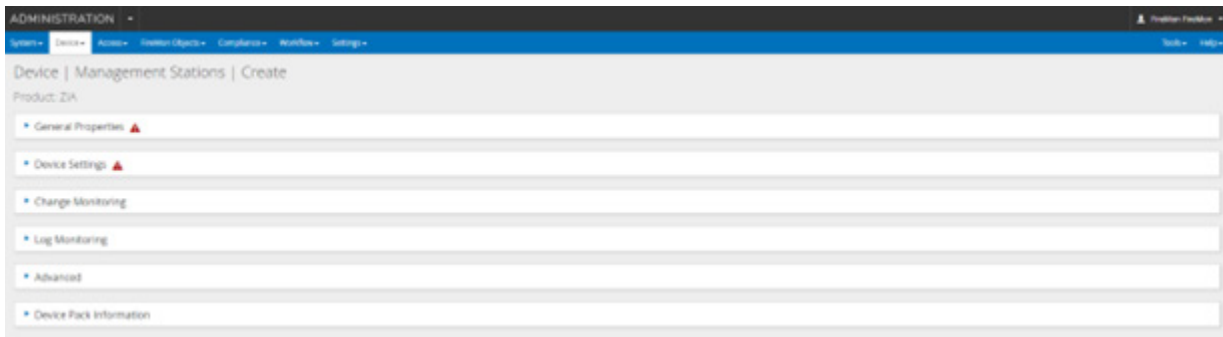


Figure 1. Device management stations



To prevent errors in device group-level device maps and incorrect reporting data, all devices added in Administration must have unique IP addresses. If devices with duplicate IP addresses must be added within a domain, it is strongly recommended that you separate those devices into discrete device groups, where no duplicate IP addresses are included in the same device group. Devices with duplicate IP addresses cause errors in the All Devices device map, and might cause incorrect data in reports, even if they are in discrete device groups.

4. In the **General Properties** section:
  - a. In **Name**, enter the name of the device as you want to see it in SIP.
  - b. In **Description**, type an optional description of the device being added.
  - c. Leave the **Management IP Address** field blank.



A Management IP Address is not needed, however Zscaler recommends assigning an arbitrary, but unique, IP. For example, 0.0.0.0 or 1.1.1.1 with an incremental increase for each similar vendor management station used (0.0.0.0, 0.0.0.1, 0.0.0.2, etc.). If you don't enter an IP address, device logs are sent to a specific directory that is named after the device ID. If you have the IP address in the system, it is used to name the directory, which makes it easier for support to find. For example, a non-IP address device would have a directory with domain\_deviceID (e.g., 1\_61).

- d. In **Data Collector Group**, select the IP address of the data collector group that collects data from this device.
- e. (Optional) In **Central Syslog Server**, select the syslog server from the list.



You must create a syslog server before assigning it to a device.

- f. (Optional) In **Syslog Match Name**, enter the syslog match name.
  - g. By default, **Automatically Retrieve Configuration** is selected.
  - h. In **External ID**, enter a unique identifier to be used when the device identifier is different than what is displayed in SIP.
  - i. For **Collection Configuration**, enable **Update Rule Documentation on Member Devices** to allow Rule Documentation fields on member devices to inherit a value from the management station. Any management stations' Rule Documentation field updates override updates on the member device. A rule marked for removal is not updated.
5. In the **Device Settings** section:
- a. **API URL**: Enter the URL of the API version.
  - b. **API Key**: Enter the API key that was generated for API access.
  - c. For **Re-enter API Key**, enter the key entered earlier.



You can find the API URL and Key in the ZIA Admin Portal (**Administration > API Key Management**).

- d. For **User Name**, enter the **Login ID** used for the ReadOnly-adminRole account.
  - e. For **Password**, enter the password used for the ReadOnly-adminRole account.
  - f. For **Re-enter Password**, re-enter the password.
6. In the **Change Monitoring** section.
- a. By default, **Enable Scheduled Retrieval** is selected. Clear the checkbox to disable it.
    - The default **Check for Change Interval** time is 1440.
    - Set an optional time in the **Check for Change Start Time** field.
7. In the **Advanced** section.
- a. **File Retrieval Options**: Select **Use Batch Config Retrieval** only if you are manually sending configurations for this device via your data collector's batchconfig directory. While this option is enabled, online retrievals are disabled.
  - b. **SSH Key Options**: Select **Automatically Update SSH Keys** if you want the data collector to automatically update the SSH key for a device when a conflict occurs.
8. Click **Save**.
9. After configuring the SIP Administration Module, you can view a list of discovered devices. Open the SIP Administration Module and go to the **Discovered Devices** section to see a list of the discovered devices.

## Verify Normalization

After you have added the device in SIP, you can verify successful normalization. You can view the health of the Zscaler in the Administration module and the rules that were normalized in the Security Manager module.

### View Zscaler in the SIP Administration Module

To view Zscaler in the SIP Administration Module:

1. In the SIP Administration module toolbar, select **Device > Management Stations**.
2. Find the **Zscaler ZIA** in the **All Management Stations** list.
3. Click the device **Health** icon to view the health check results.

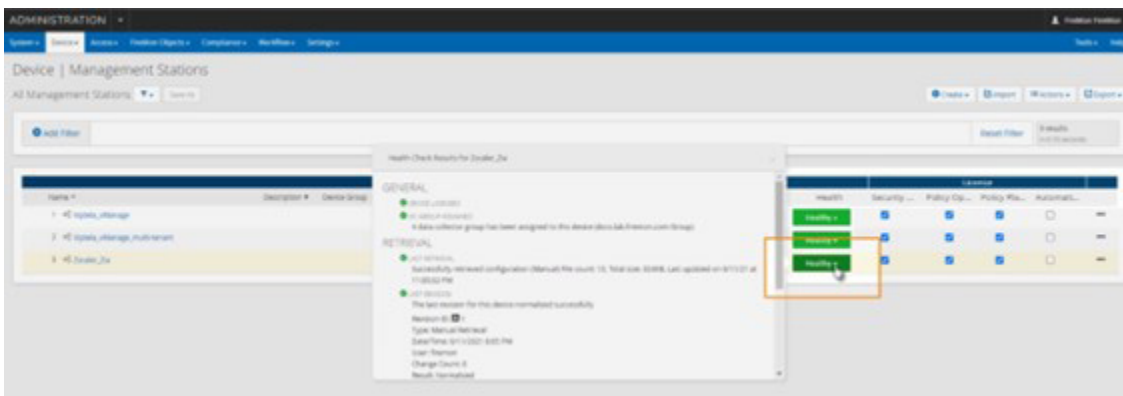


Figure 2. Health check results

### View Zscaler in the SIP Security Manager Module

To view Zscaler in the SIP Security Manager Module:

1. Open the Security Manager module.
2. On the toolbar, click the **Domain Home** arrow and select **Go to All Devices List**.

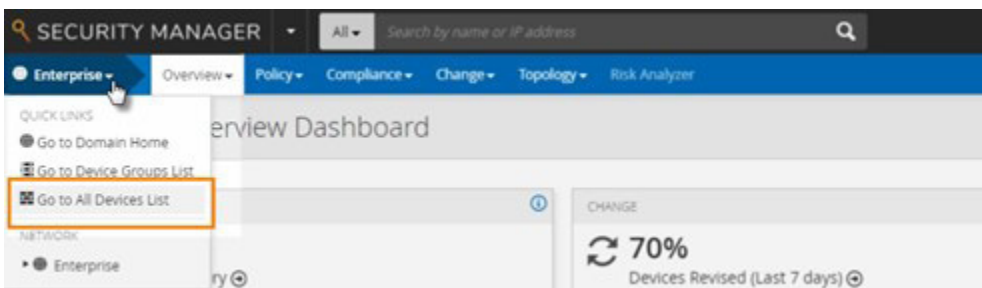


Figure 3. Go to All Devices list

3. Select the Zscaler ZIA device from the list to open the **Overview Dashboard**.
4. On the toolbar, select **Policy > Policy View**.
5. In the **Security Rules** tab, in the **Policy** field, click the arrow to select a policy to view.
  - **Firewall** is a list of the policies in Zscaler's Firewall Control.
  - **URL Control** is a list of the policies in Zscaler's URL & Cloud App Control.

## Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration > Settings > Company Profile**.

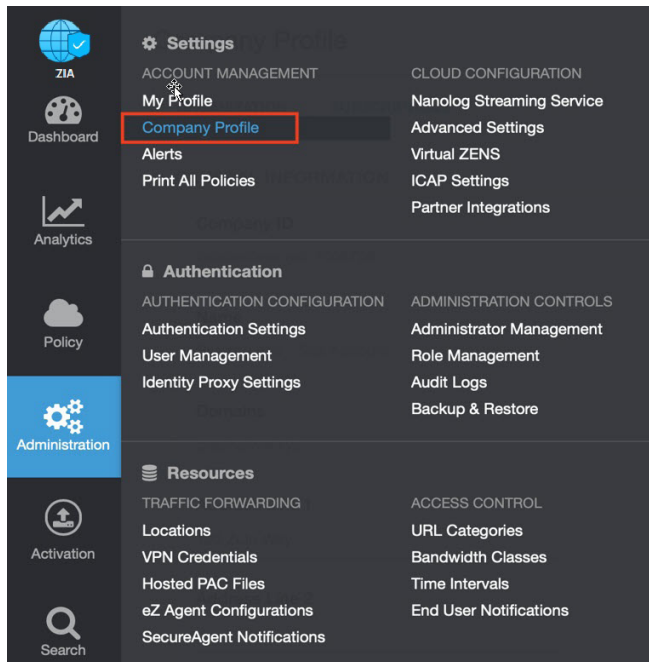


Figure 4. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

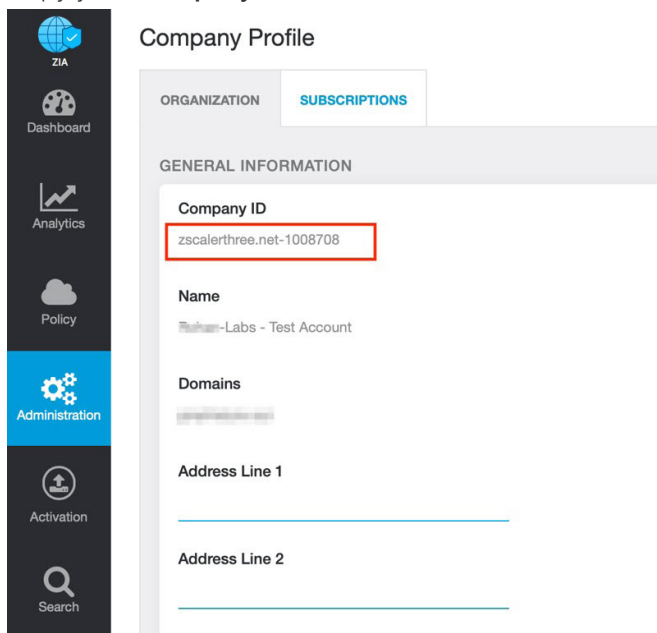


Figure 5. Company ID

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

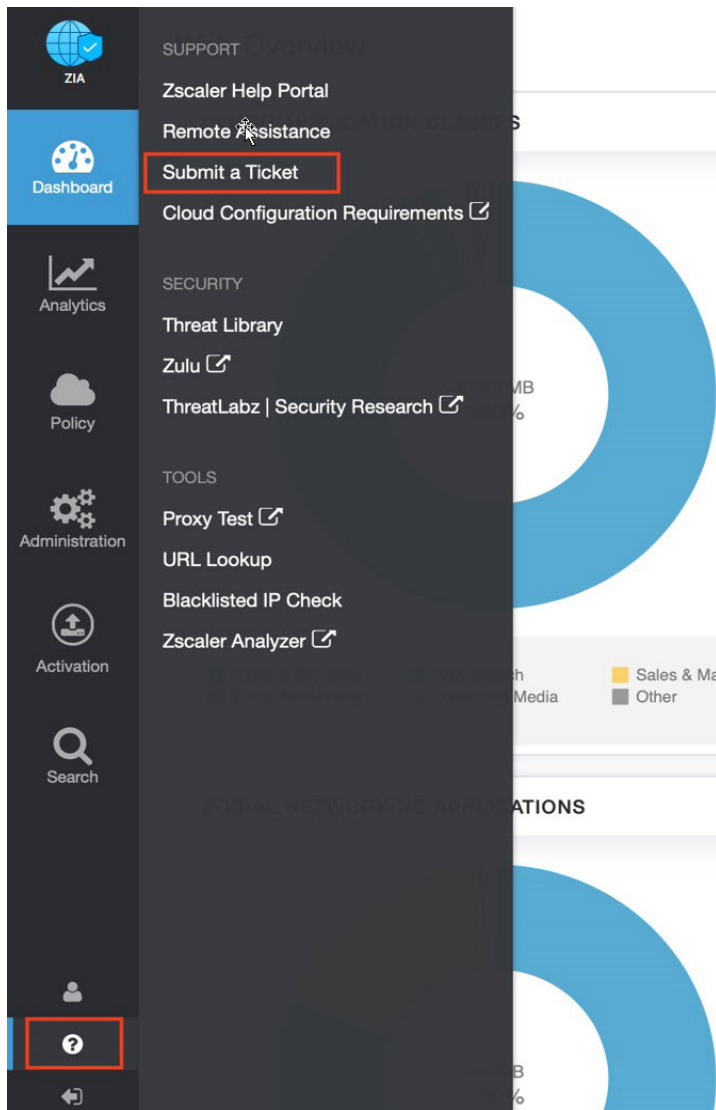


Figure 6. Submit a ticket