FIREMON

Security Intelligence Platform

Zscaler Deployment Guide

July 2021

Version 1.1

Zscaler Business Development – Solutions Architecture Team

Table of Contents

Terms and Acronyms

Acronym	Definition
SIP	Security Intelligence Platform
ZIA	Zscaler Internet Access (Zscaler)

About This Document

Zscaler Overview

Zscaler (Nasdaq: ZS), **Zscaler** enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to 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, please visit www.zscaler.com or follow them on Twitter @zscaler.

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.

For more information on FireMon, LLC., please visit www.firemon.com or follow them on Twitter @FireMon.

Audience

This guide is written for Zscaler Administrators and SIP Administrators responsible for deploying, monitoring, and managing network security services in an Enterprise environment. For additional product and company resources, please refer to the Appendix section.

Document Authors

This document was authored by FireMon and Zscaler Solution Architects in the Zscaler Business Development / Technical Alliances team (aka "BD SA"). All solutions validated within this guide have been jointly reviewed by both vendors.

Software Revisions

This document was authored using Zscaler Internet Access v6.0 and SIP Release 9.3.

Request for Comments

- **For Prospects / Customers:** We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at:
    - partner-doc-support@zscaler.com
- **For Zscaler Employees:** If you are trying to reach the team that validated and authored the integrations contained within this document, please contact us at:
    - z-bd-sa@zscaler.com

1 Overview for Zscaler and FireMon SIP Integration

This guide is provided for the integration process of connecting the Security Intelligence Platform (SIP) and Zscaler.

An active SIP license is required for integration with Zscaler.

For more information, please see the resources in ***Appendix A: Zscaler Resources***.

2 Setup the Zscaler Account

2.1 Zscaler Cloud Portal

1. Log in to your Zscaler Cloud Portal.
2. On the left toolbar, go to **Administration**.
3. In the **Authentication** section, click **Administration Management**.
4. Click **Add Administrator**.
    a. **Login ID** is an email address.

    Note: The Login ID will be used for credentials in SIP.

    b. **Email** is the email address of the user.
    c. **Name** is the name of the user.
    d. For **Role**, select **ReadOnly-adminRole** from the list.

    Note: The permission settings for the ReadOnly-adminRole (a Standard Admin Type) are in Authentication > Role Management.

    e. For **Scope**, select **Organization**.
    f. There is not a need to enable any Update settings.
    g. Enter a **Password** for the account.
    h. Click **Save**.
5. In the **Resources** section, click **Location Management**. This is where you'll set discovery for child devices. Child devices will be listed as a sub-location.
6. Click **Add Location**.
    a. Enter the server **Location** information.
        - **Exclude from Manual Location Groups** and **Exclude from Dynamic Location Groups** should be disabled.
    b. For **Addressing**, select the **Static IP Addresses** and any **VPN Credentials**.
    c. For **Gateway Options**, enable (click the red X to turn the toggle green) the following:
        - **Enforce Authentication**
        - **Enable SSL Inspection**
        - **Enforce Zscaler Client Connector SSL Setting**
        - **Enforce Firewall Control**
    d. **Enforce Bandwidth Control** should remain disabled.

7. Click **Save**.

2.2 Role Management Permission Settings

If you want to add a role specifically for SIP, these are the recommended permission settings to be used for the ReadOnly-adminRole account that will be used.

1. Click **Administration > Role Management.**
2. Click **Add Administrator Role**.
3. Enter a **Name** for this role (example: FM-readonly).
4. **Enable Permissions for Executive Insights** should remain disabled.
5. **Permissions** settings to select:
    - **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**
6. **Functional Scope** settings to select:
    - All options should be enabled.
7. Click **Save**.

2.3 API URL and Key

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

2.4 Policy Normalization

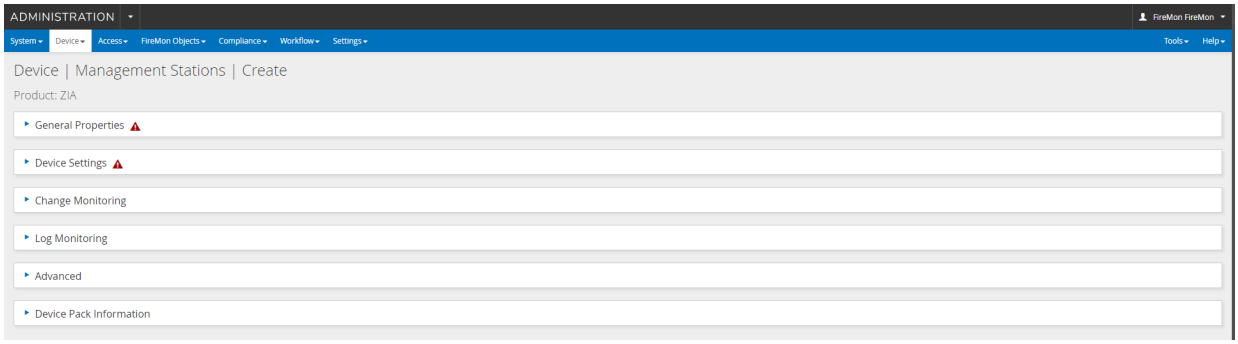
You can view the policies that will be normalized by Security Manager.

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

3 Add Zscaler Management Station to FireMon SIP

3.1 SIP Administration Module

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



4. **General Properties** section.

Caution! 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 those devices be separated into discrete device groups, where no duplicate IP addresses are included in the same device group. Devices with duplicate IP addresses will cause errors in the All Devices device map, and may cause incorrect data in reports, even if they are in discrete device groups.

- In the **Name** box, type the name of the device as you want to see it in SIP.
- In the **Description** box, type an optional description of the device being added.
- The **Management IP Address** box can be left blank.

Note: A Management IP Address is not needed, however assigning an arbitrary, but unique IP is suggested. 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, logs about the device are sent to a specific directory that is named after the device ID. If you have the IP address in the system it will be 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 (example: 1_61).

- In the **Data Collector Group** box, select the IP address of the data collector group that will collect data from this device.
- In the **Central Syslog Server** box, select the syslog server from the list (optional).

Note: A syslog server must be created before assigning to a device.

- In the **Syslog Match Name** box, type the syslog match name (optional).
- By default, the **Automatically Retrieve Configuration** check box is selected.
- In the **External ID** box, type a unique identifier to be used when the device identifier is different than what is displayed in SIP.
- 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 will override updates on the member device. A rule marked to be removed will not be updated.

5. **Device Settings** section.
   - **API URL**—this is the URL of the API version.
   - **API Key**— this is the API key that was generated for API access.
   - In the **Re-enter API Key** box, re-type the key entered above.

     Note: The API URL and Key are found in Zscaler Cloud Portal in Administration > API Key Management.

   - In the **User Name** box, type the Login ID used for the ReadOnly-adminRole account.
   - In the **Password** box, type the password used for the ReadOnly-adminRole account.
   - In the **Re-enter Password** box, re-type the password entered above.
6. **Change Monitoring** section.
   - By default, the **Enable Scheduled Retrieval** check box is selected. Clear the check box to disable.
     - The default **Check for Change Interval** time is **1440**.
     - Set an optional time in the **Check for Change Start Time** field.
7. **Advanced** section.
   - **File Retrieval Options**: Select the **Use Batch Config Retrieval** check box only if you are manually sending configurations for this device via your data collector's batch config directory. While this option is enabled, online retrievals will be disabled.

- **SSH Key Options**: Select the **Automatically Update SSH Keys** check box if you want the data collector to automatically update the SSH key for a device when a conflict occurs.

8. Click **Save**.

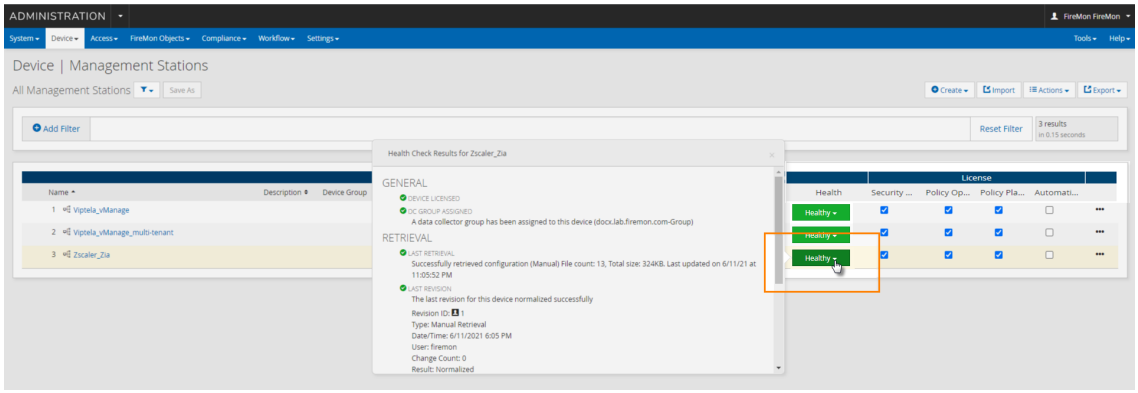
Devices being managed will be listed in the **Discovered Devices** section.

4 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.

4.1 View Zscaler in SIP Administration Module

1. In the SIP Administration module, on the toolbar, click **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.

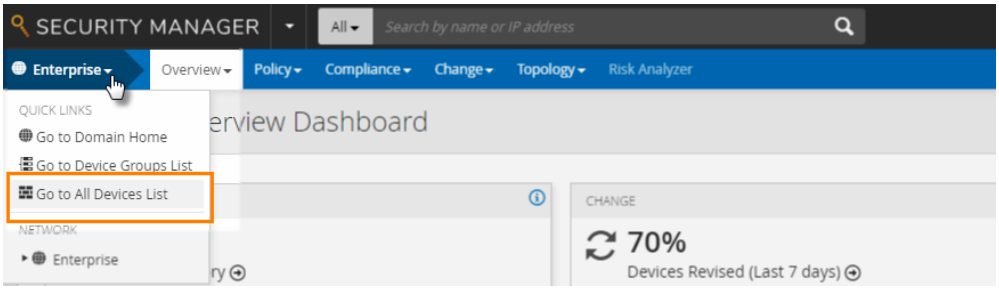


Note: More about device health checks is covered in the Device chapter of the *Administration User's Guide*.

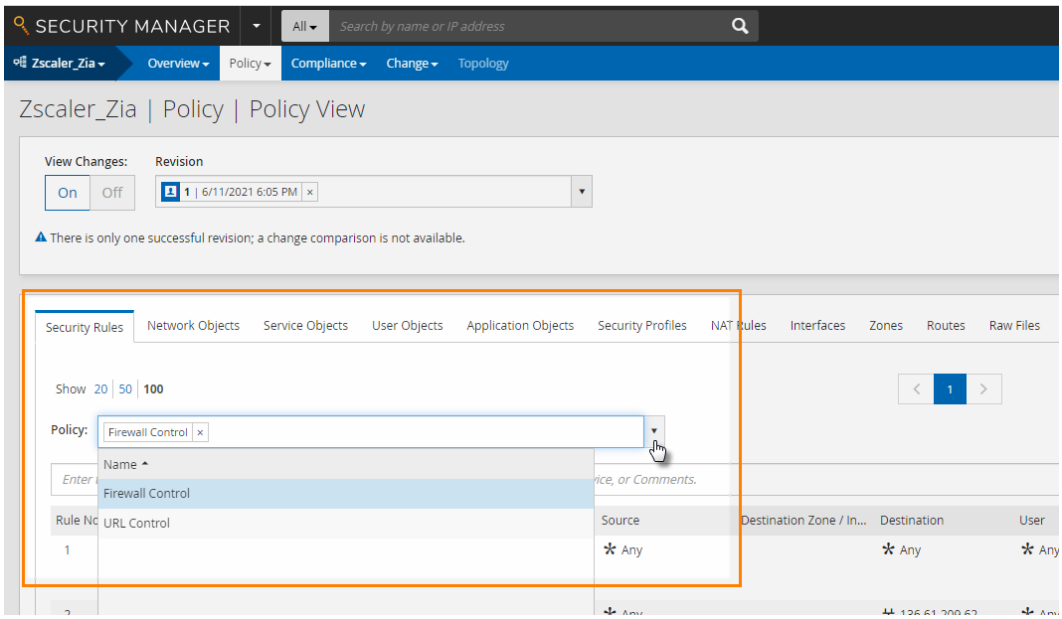
4.2 View Zscaler in SIP Security Manager Module

1. Open the Security Manger module.

2. On the toolbar, click the Domain Home arrow and select **Go to All Devices List**.



3. Select the Zscaler ZIA device from the list to open the Overview Dashboard.
4. On the toolbar, click **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



Note: A Security Profile normalized with a label of CUSTOM_## is an object type connected to a TLD Category in Zscaler. As of FireMon SIP release in September 2021, normalization for these objects will be updated to a new FireMon object type in SIP called URL Categories.

5 Appendix A: Resources

5.1 Zscaler Resources

Zscaler Internet Access (ZIA)
https://www.zscaler.com/products/zscaler-internet-access

5.2 FireMon Resources

About FireMon
https://www.firemon.com

User Center
https://usercenter.firemon.com