

Zscaler Internet Access (ZIA) and Cloudi-Fi Deployment Guide

October 2022

Version 1.0

Table of Contents

1	Document Overview	3
1.1	Document Audience	3
1.2	Software revisions	3
1.3	Request for comments	3
1.4	Document Prerequisites	3
1.5	Document Revision Control	3
2	Solution overview	4
3	Zscaler deployment into an existing Zscaler tenant	7
3.1	Introduction	7
3.2	Prerequisites for Eligibility	7
3.2.1	Authentication	7
3.2.2	URL Policies for Unauthenticated traffic	8
3.3	Synchronization	8
3.4	Service activation	11
3.5	Firewall and SSL Inspection	13
3.5.1	Firewall configuration	13
3.5.2	SSL Inspection policies	13
3.6	Adding newly created Guest profiles	13
4	Free Cloudi-Fi trial	13
5	Requesting Zscaler Support	14
6	Appendix A: Zscaler resources	15
7	Appendix B: Cloudi-Fi resources	16



1 Document Overview

This Deployment Guide document will provide GUI examples for configuring Zscaler Internet Access (ZIA) and Cloudi-Fi. This guide is intended for standing up proof-of-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 Cloudi-Fi for 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 v6.2 and Cloudi-Fi Summer 2022 Release.

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 v6.2 (or newer)
Administrator login credentials to ZIA

Cloudi-Fi

Cloudi-Fi Summer 2022 Release
Administrator login credentials to Cloudi-Fi

1.5 Document Revision Control

Revision	Date	Change Log
1.0	October 2022	Initial document created by Zscaler and Cloudi-Fi

2 Solution overview

This document describes how to manage guest network with Zscaler ZIA and Cloudi-Fi.

The rise of cloud adoption by enterprises has **democratized distributed networks** in Enterprise. As Internet is eating corporate networks, local Internet breakouts with SD-WAN and Wi-Fi are becoming essential (and often sufficient) to users' connectivity and productivity.

Distributed networks by nature are promoting **cloud-based services**, gradually replacing central infrastructure.

Zscaler **authenticates and secures employees and their managed devices.**

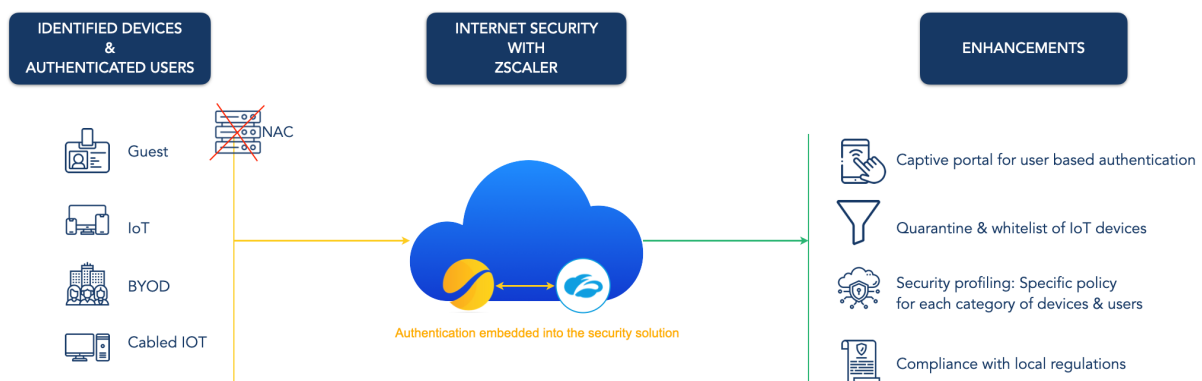
However, guests, BYOD and IoTs cannot be authenticated and identified in Zscaler. They continue to be authenticated on the central infrastructure (controller, anchor controller, NAC...) or locally on the network. Consequently, security policies cannot be defined on a per-device or per-user basis, making it impossible to enforce a least-access security policy.

Cloudi-Fi is **extending the authentication capability** of Zscaler to authenticate (and secure accordingly) all users and devices, including BYOD and IoT.

This is particularly relevant to existing Zscaler ZIA customers who are one click away of this capability.

Enabling Cloudi-Fi into Zscaler provides multiple advantages:

- Total visibility of all guest's and IoT traffic
- Unmanaged users' authentication and devices categorization
- Security profiling with specific policies for each category of devices and users
- Compliance with local regulations (Data privacy and Internet provider regulations)

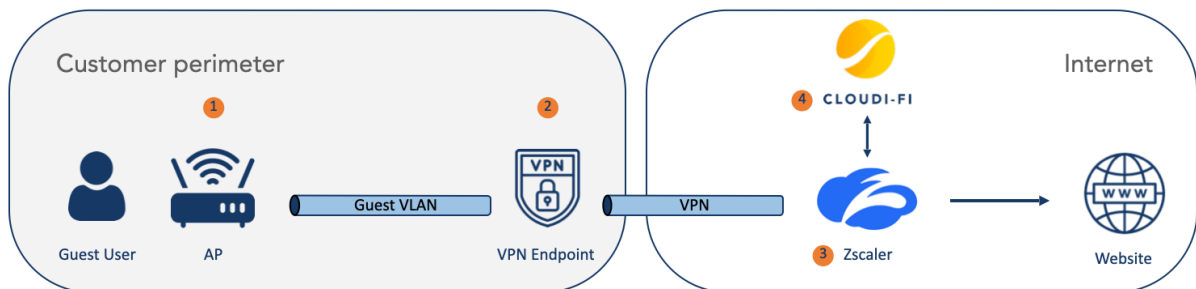


To leverage Zscaler ZIA, GRE/IPSEC redundant tunnels should be configured on the router/firewall/SD-WAN device. Zscaler allows different setup depending on your existing infrastructure. This has been developed [in this article](#).

Solution tested

The diagram below shows the Cloudi-Fi integration.

- **1** Configure an open SSID on the AP and assign it to the Guest VLAN.
- **2** On the VPN Endpoint (Internet Router or Firewall), configure Source/Policy-based routing to forward only Guest and BYOD traffic into the VPN
- **3** While Guests and BYOD device IP is not authenticated, Zscaler redirects to Cloudi-Fi portal.
- **4** Cloudi-Fi hosts the captive portal and handles guest's and BYOD authentication thanks to its directory service



This document covers the Cloudi-Fi integration into an existing Zscaler tenant: guest traffic and employees share the same tenant.

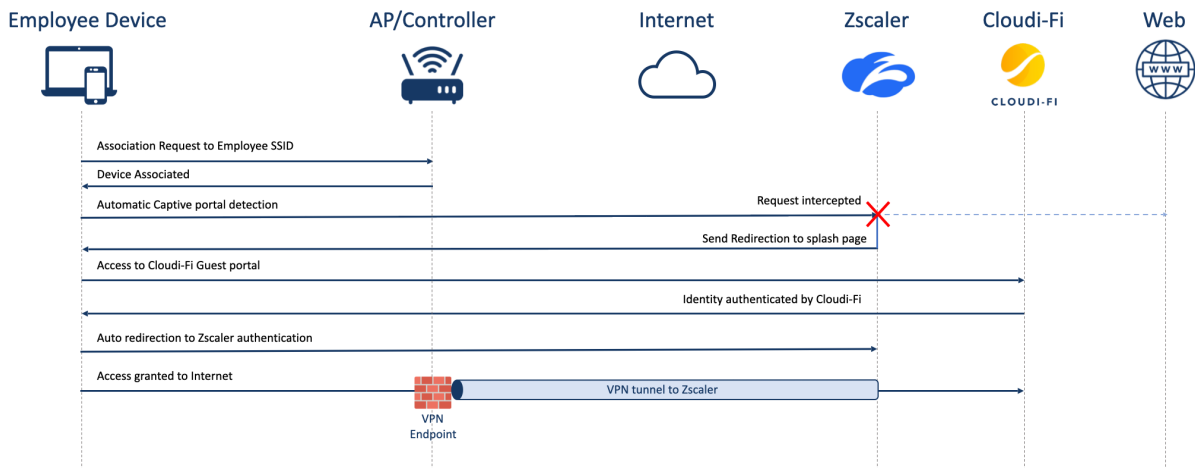
Please be aware we support other types of configurations, more information here.
<https://help.cloudi-fi.net/en/articles/3385684-zscaler-deployment-general>

The option described in this document is the option 2, WAN solution with Zscaler shared tenant).

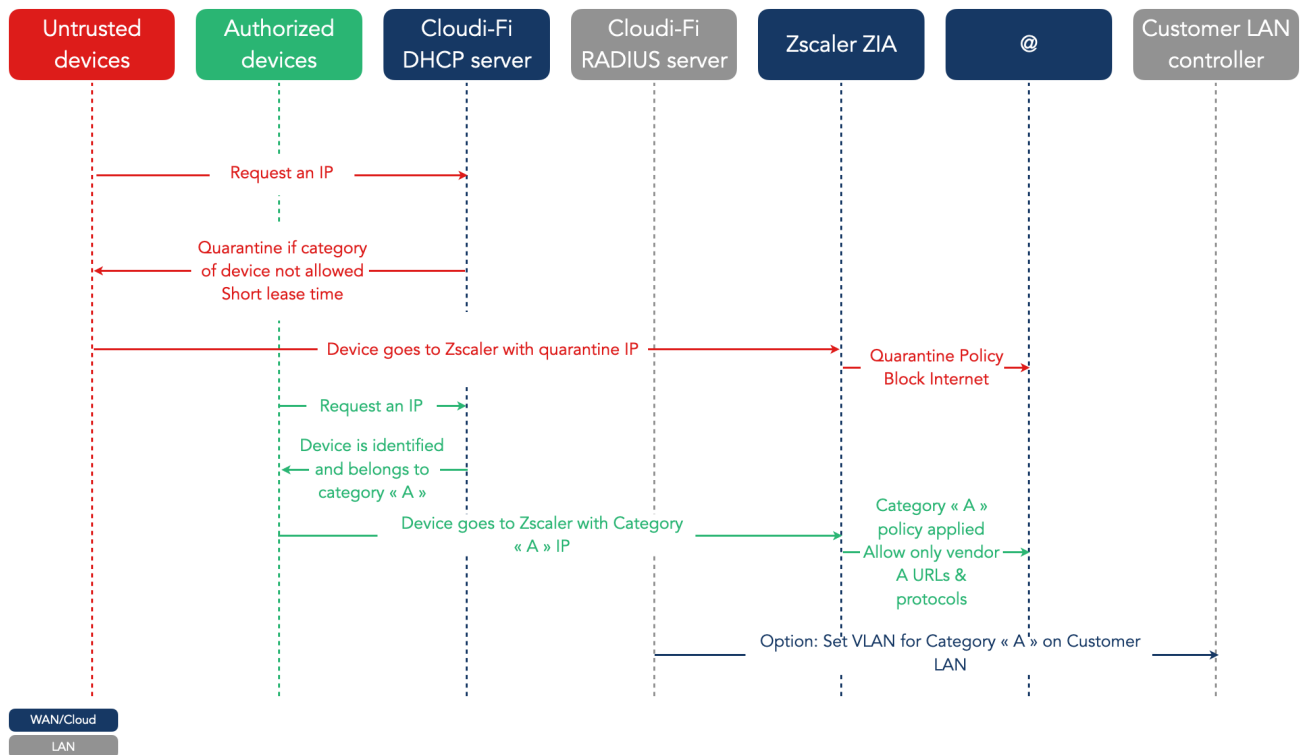
For any questions, please send an email to sales@cloudi-fi.com for qualification

Cloudi-Fi extends the authentication capability of Zscaler to authenticate (and secure accordingly) all users and devices, including BYOD and IoT

Guest authentication flow



IoT identification flow



3 Zscaler deployment into an existing Zscaler tenant

3.1 Introduction

- **Deployment for user-based authentication:** Cloudi-Fi Captive portal is configured into an existing Zscaler tenant, leveraging existing GRE/IPSEC tunnels. The source guest network(s) are routed into the tunnels.
- **Deployment for IoT identification:** Cloudi-Fi DHCP servers are available on the Internet through IPSEC tunnels. Any existing DHCP relay can request Cloudi-Fi's DHCP servers to get their IP addresses. Cloudi-Fi uses DHCP fingerprinting to identify and classify IoT.
- **Security:** Guests can be profiled based on how they authenticate in the captive portal. Daily guests, consultants, employees can have specific security policies in Zscaler. Quota, time, and duration can also be defined for each profile. Finally, categories of IoT can be profiled based on the network, matching a sublocation specific to the category of IoT.
- **Compliance:** In many countries Internet logs should be kept for a specific duration and matched with the user. To process the government request, the authentication logs and Internet logs should be correlated. All logs are hosted in the cloud. Authentication logs (in Cloudi-Fi) and pseudonymized Internet logs (in Zscaler) can be correlated in Cloudi-Fi administration interface, menu Visits. Access to this menu should be restricted to few administrators with administration profile.

3.2 Prerequisites for Eligibility

Some parameters may conflict with Cloudi-Fi integration, especially regarding the capability to Multiple Authentication Domains.

Below the settings to be verified.

3.2.1 Authentication

Go to **Administration > Authentication Settings:**

- **User Repository Type:** Must be Hosted DB
- **User Authentication Type:** Must be SAML

Login Attribute of your existing IdP:

The login attribute returned by your existing Identity Provider (IdP) **must be unique and in the form of an email address.**

Example: user@my-company.com

If it returns only a **username without any domain, Zscaler cannot perform authentications on multiple domains.**

Example: The ADFS Attribute sAMAccountName only returns a username, without domain.

3.2.2 URL Policies for Unauthenticated traffic

Go to **Administration > Advanced Settings**

Make sure the "Apply URL Policies for Unauthenticated Traffic" is checked.

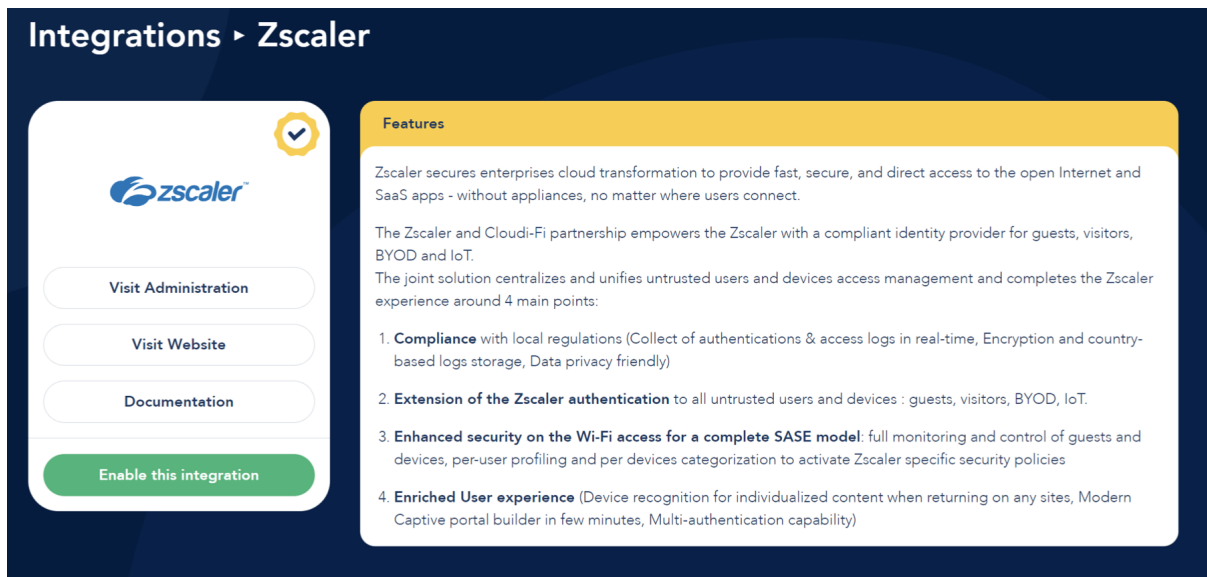
This option allows Cloudi-Fi to redirect any unauthenticated Guest to the appropriate captive portal page and recognize the Guest location.

With this option enable, you will have a better control on your traffic by allowing or blocking unauthenticated traffic.



3.3 Synchronization

To enable Cloudi-Fi into Zscaler, connect to your Cloudi-Fi Administration and go to Settings > Integration > Zscaler > Learn More

Click on "Enable this integration" button



Integrations > Zscaler

Visit Administration

Visit Website

Documentation

Enable this integration

Features

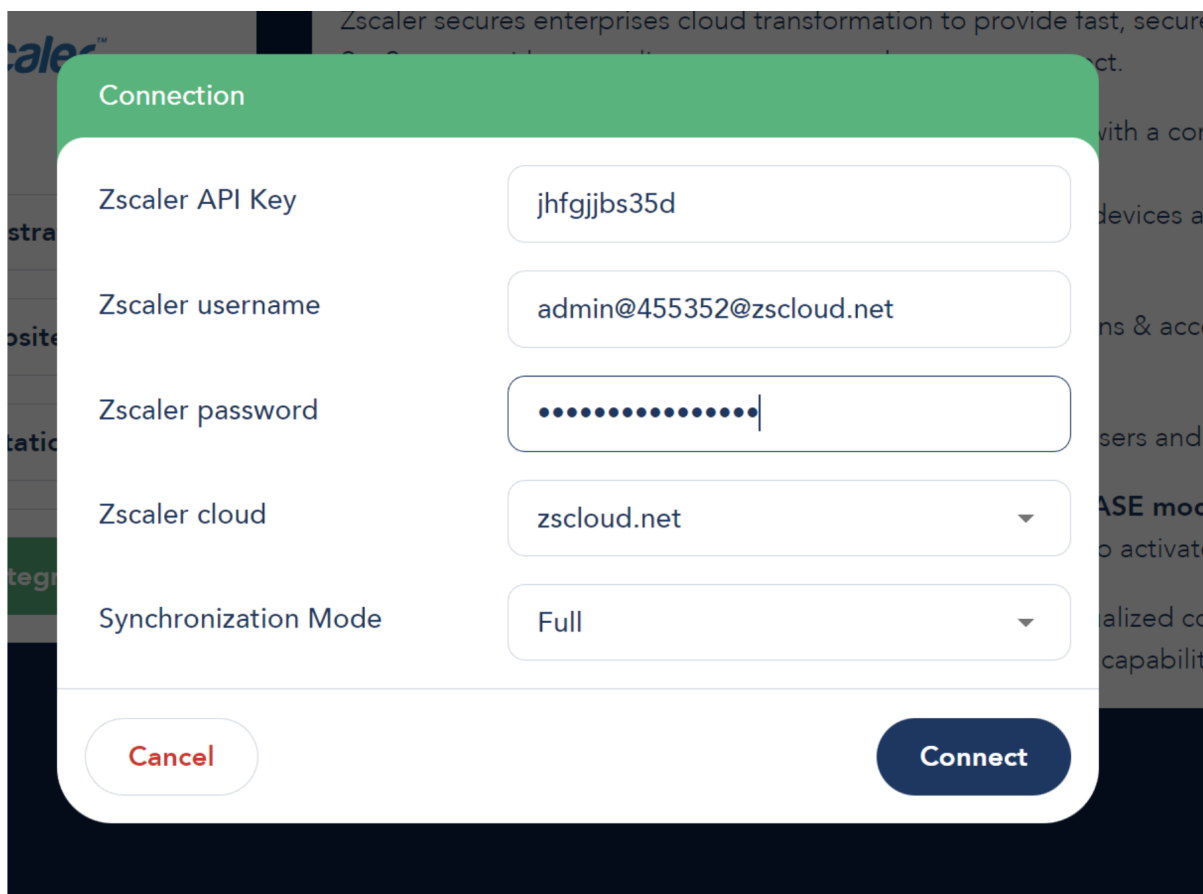
Zscaler secures enterprises cloud transformation to provide fast, secure, and direct access to the open Internet and SaaS apps - without appliances, no matter where users connect.

The Zscaler and Cloudi-Fi partnership empowers the Zscaler with a compliant identity provider for guests, visitors, BYOD and IoT.

The joint solution centralizes and unifies untrusted users and devices access management and completes the Zscaler experience around 4 main points:

1. **Compliance** with local regulations (Collect of authentications & access logs in real-time, Encryption and country-based logs storage, Data privacy friendly)
2. **Extension of the Zscaler authentication** to all untrusted users and devices : guests, visitors, BYOD, IoT.
3. **Enhanced security on the Wi-Fi access for a complete SASE model**: full monitoring and control of guests and devices, per-user profiling and per devices categorization to activate Zscaler specific security policies
4. **Enriched User experience** (Device recognition for individualized content when returning on any sites, Modern Captive portal builder in few minutes, Multi-authentication capability)

Once done, you will be requested to provide Zscaler connection details.



Connection

Zscaler API Key: jhfgjjbs35d

Zscaler username: admin@455352@zscloud.net

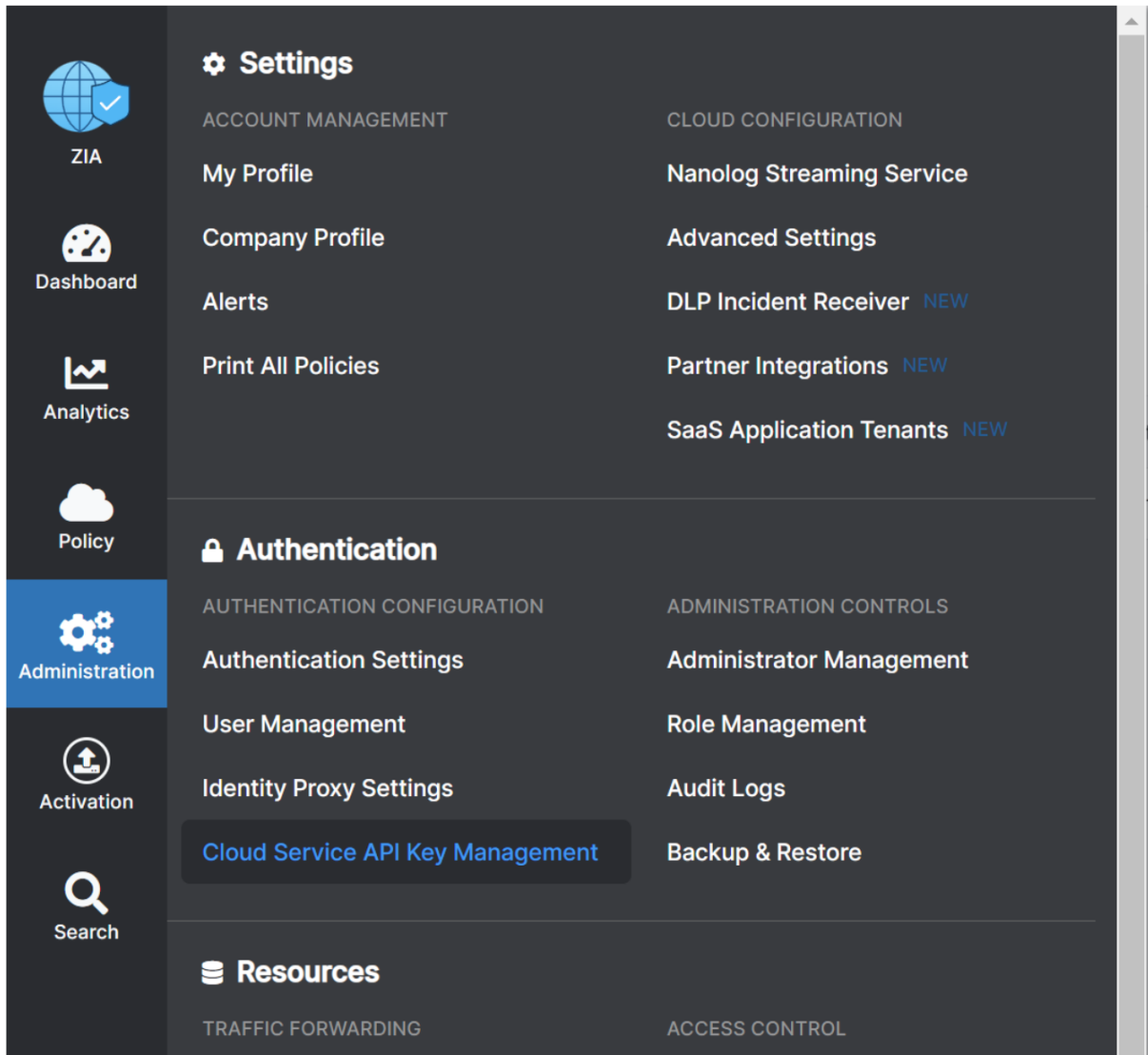
Zscaler password:

Zscaler cloud: zscloud.net

Synchronization Mode: Full

Cancel Connect

Zscaler API Key can be found under "Administration > Cloud Service API Key Management" under your Zscaler administration console.



Click "Connect" to continue.

During the activation process, the following actions are performed on your Zscaler tenant:

1. Adding a new IDP configuration dedicated to Guests (refers to Cloudi-Fi IDP configuration)
2. Creation of multiple custom Categories
3. Customization of Advanced Settings (URL Bypass Category list)
4. Add a Location Group "Cloudi-Fi" which will contain all location and sublocation when Cloudi-Fi portal must be enabled.
5. Add base URL Filtering rules. These rules only apply on "Cloudi-Fi" location group to make sure Cloudi-Fi configuration does not interfere with existing Employee ruleset.

If you need to know exactly what configuration is changed by this Activation, [follow this link](#).

3.4 Service activation

You have the choice to create location (dedicated VPN tunnel for Guest traffic) or sub-locations (reuse an existing location and define the Guest private IP range).

Cloudi-Fi captive portal will be automatically enabled on your location by changing your location name and prefix it by "CLOUDIFI-". If you want to enable Cloudi-Fi on a subset of your Location, you will have to create a sublocation as described below.

Go to **Administration > Location Management**

- For new location: Create a new Location
- For sub-location: Select an existing location and click on this icon on the right

How to configure your Guest location:

- **Name:** Must start with "CLOUDIFI-" to match the Dynamic location Group configuration
- **Enforce Authentication:** ON
- **Enable IP Surrogate (both options):** Timers should be equal to Cloudi-Fi lifetime session
- **Enforce Firewall control:** ON

Edit Location ✕

Name CLOUDIFI-acheres	Country Vietnam
City/State/Province Enter Text	Time Zone Asia/Vientiane
Manual Location Groups None	Dynamic Location Groups Corporate User Traffic Group,CLOUDIFI
Exclude from Manual Location Groups <input type="checkbox"/>	Exclude from Dynamic Location Groups <input type="checkbox"/>
Location Type Corporate user traffic	
Description <div style="border: 1px solid #ccc; height: 60px;"></div>	

ADDRESSING

Static IP Addresses and GRE Tunnels
None

VPN Credentials
acheres@nrb.cloudi-fi.net

GATEWAY OPTIONS

Use XFF from Client Request <input type="checkbox"/>	Enforce Authentication <input checked="" type="checkbox"/>
Enable IP Surrogate <input checked="" type="checkbox"/>	Idle Time to Disassociation 4 Hours
Enforce Surrogate IP for Known Browsers <input checked="" type="checkbox"/>	Refresh Time for re-validation of Surrogacy 3 Hours
Enforce Firewall Control <input checked="" type="checkbox"/>	

BANDWIDTH CONTROL

Enforce Bandwidth Control
Enable Disable

Save Cancel Delete

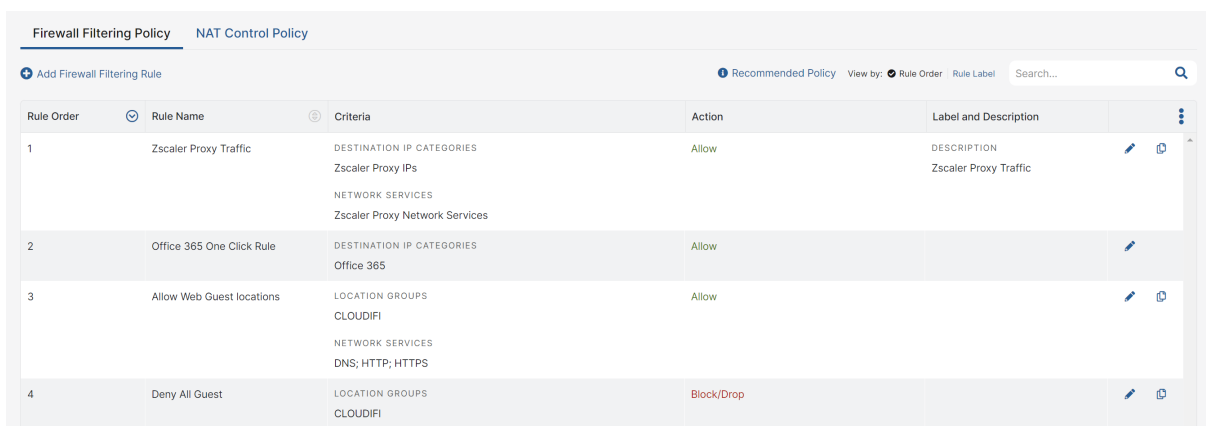
3.5 Firewall and SSL Inspection

In addition to the base Cloudi-Fi ruleset, Firewall and SSL Inspection Zscaler' settings need to be adjusted to ensure access to Internet for your Guests.

3.5.1 Firewall configuration

We recommend configuring these rules at the beginning of your Firewall Policy.

Go to Policy > Firewall control



The screenshot shows the 'Firewall Filtering Policy' configuration page. It features a table with four rules. The first rule, 'Zscaler Proxy Traffic', is highlighted. The table columns are: Rule Order, Rule Name, Criteria, Action, and Label and Description. The 'Criteria' column for the first rule lists 'DESTINATION IP CATEGORIES' (Zscaler Proxy IPs), 'NETWORK SERVICES' (Zscaler Proxy Network Services), and 'Action' is 'Allow'. The 'Label and Description' column shows 'DESCRIPTION' (Zscaler Proxy Traffic). The second rule is 'Office 365 One Click Rule' with criteria 'DESTINATION IP CATEGORIES' (Office 365) and action 'Allow'. The third rule is 'Allow Web Guest locations' with criteria 'LOCATION GROUPS' (CLOUDIFI), 'NETWORK SERVICES' (DNS, HTTP, HTTPS), and action 'Allow'. The fourth rule is 'Deny All Guest' with criteria 'LOCATION GROUPS' (CLOUDIFI) and action 'Block/Drop'.

Rule Order	Rule Name	Criteria	Action	Label and Description
1	Zscaler Proxy Traffic	DESTINATION IP CATEGORIES Zscaler Proxy IPs NETWORK SERVICES Zscaler Proxy Network Services	Allow	DESCRIPTION Zscaler Proxy Traffic
2	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow	
3	Allow Web Guest locations	LOCATION GROUPS CLOUDIFI NETWORK SERVICES DNS, HTTP, HTTPS	Allow	
4	Deny All Guest	LOCATION GROUPS CLOUDIFI	Block/Drop	

3.5.2 SSL Inspection policies

If you have SSL Inspection enabled, you will have to check your existing policies and create a dedicated SSL Policy for Guest traffic.

Go to "Policy > SSL Inspection"

3.6 Adding newly created Guest profiles

Your Guest can have different profiles. These profiles are shared by Cloudi-Fi to Zscaler through SAML AutoProvisioning.

You may have to add any newly created profile into the Zscaler Allow URL policy.

Departments created through Cloudi-Fi SAML Auto-provisioning are all suffixed by "{Cloudi-Fi}" in their name.

4 Free Cloudi-Fi trial

You can ask for a free Cloudi-Fi trial by activating your evaluation account here:

<https://get.cloudi-fi.net>



5 Requesting Zscaler Support

Please check the article on our knowledge base describing the troubleshooting procedure <https://help.cloudi-fi.net/en/articles/6632077-cloudi-fi-and-zscaler-troubleshooting-guide>



6 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

<https://ip.zscaler.com/>

7 Appendix B: Cloudi-Fi resources

Cloudi-Fi Knowledge Base

<https://help.cloudi-fi.net/en/>

Zscaler Deployment with Cloudi-Fi - General principles

<https://help.cloudi-fi.net/en/articles/3385684-zscaler-deployment-general>

Zscaler activation with Cloudi-Fi

<https://help.cloudi-fi.net/en/articles/6640467-zscaler-activation>

Zscaler deployment into an existing Zscaler tenant

<https://help.cloudi-fi.net/en/articles/4655086-zscaler-deployment-into-an-existing-zscaler-tenant>

Zscaler - Modifying GRE Tunnels destination datacenters

<https://help.cloudi-fi.net/en/articles/6505024-zscaler-modifying-gre-tunnels-destination-datacenters>

Zscaler and Cloudi-Fi troubleshooting guide

<https://help.cloudi-fi.net/en/articles/6632077-cloudi-fi-and-zscaler-troubleshooting-guide>

Zscaler Technology Partner webpage (Solution Brief, Deployment Guide, Troubleshooting Guide, Video)

<https://www.cloudi-fi.com/technological-partners/zscaler>

Cloudi-Fi support

support@cloudi-fi.com