



ZSCALER AND CLOUDI-FI DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	5
Zscaler Overview	5
Cloudi-Fi Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and Cloudi-Fi Introduction	6
ZIA Overview	6
Zscaler Resources	6
Cloudi-Fi Security Overview	7
Cloudi-Fi Resources	7
Solution Overview	8
Solution Tested	9
Cloudi-Fi Deployment into an Existing Zscaler Tenant	11
Create a Cloudi-Fi Account	11
Prerequisites for Eligibility	12
Tunnels	12
Authentication Settings	12
Login Attribute for Your Existing IdP	13
URL Policies for Unauthenticated Traffic	14
Subscriptions	14
Synchronization	15
Zscaler API Key	15
Enabling Zscaler on Cloudi-Fi	16

Service Activation	18
Firewall and SSL Inspection	20
Firewall Configuration	20
SSL Inspection policies	21
Adding Newly Created Guest Profiles	21
Appendix A: Requesting Zscaler Support	22

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
AP	Access Point
BYOD	Bring Your Own Device
CA	Central Authority (Zscaler)
DHCP	Dynamic Host Configuration Protocol
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)
IoT	Internet of Things
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
NAC	Network Access Control
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSID	Service Set Identifier
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
VLAN	Virtual LAN
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

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](#).

Cloudi-Fi Overview

Cloudi-Fi is a 100% cloud-based SaaS solution that extends the authentication capability of Zscaler to all users and devices, including guests, BYOD, and IoT. Using Cloudi-Fi, organizations can define specific security policies per user profile and IoT category based on user profiling and identification and IoT identification and classification. The integration of Cloud-Fi and Zscaler is particularly suited to help SD-WAN architectures ensure high levels of local access breakout security.

To learn more, refer to [Cloudi-Fi'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, refer to:

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

Software Versions

This document was authored using:

- ZIA:
 - A working instance of ZIA v6.2 and later.
 - Administrator login credentials to ZIA.
- Cloudi-Fi:
 - Cloudi-Fi Summer 2022 Release.
 - Administrator login credentials to Cloudi-Fi.

Request for Comments

- **For prospects and customers:** Zscaler values reader opinions and experiences. Contact 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 Cloudi-Fi Introduction

Overviews of the Zscaler and Cloudi-Fi 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
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.

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

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.

Cloudi-Fi Security Overview

Cloudi-Fi is a guest Wi-Fi, BYOD, and IoT management software designed to help businesses in education, healthcare, retail, transportation, hospitality, and other sectors identify and secure their network access for unmanaged users and devices. The platform offers multiple authentication modes for users (SMS, QR code, social networks, etc.) by generating login credentials and automating onboarding processes via a guest management system. For IoT devices, Cloudi-Fi's cloud-based DHCP service provides their discovery, identification, and classification. Together with Zscaler, the solution provides specific security policies for all users and devices.

Administrators can create and manage client meetings, product launches, and other events in a centralized dashboard.

Marketing professionals gain insights into various key metrics such as total views, clicked links, and interaction rate across campaigns on a unified interface. Using Cloudi-Fi, businesses visualize behavioral analytics and retarget campaigns for preferred channels such as social networking sites, emails, and SMS.

Cloudi-Fi Resources

The following table contains links to Cloudi-Fi support resources.

Name	Definition
Cloudi-Fi Knowledge Base	Search for <code>zscaler</code> in the Cloudi-Fi Knowledge Base.
Deploying Cloudi-Fi with Zscaler	Comprehensive overview: Deploying Cloudi-Fi Captive Portal with Zscaler.
Zscaler Deployment into an Existing Zscaler Tenant	Add guest security into an existing Zscaler ZIA tenant.
Zscaler GRE Tunnels Destination Data Centers	Help on modifying Zscaler GRE tunnel destination data centers.
Cloudi-Fi and Zscaler Troubleshooting Guide	Describes the main steps to troubleshoot Cloudi-Fi captive portal solution integrated into a Zscaler environment.
Zscaler Technology Partner Webpage	Downloadable solution brief, integration guide, troubleshooting guide, and video.
Cloudi-Fi support	How to contact Cloudi-Fi support.

Solution Overview

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

The rise of cloud adoption by enterprises has democratized distributed networks in Enterprise. As the internet becomes the corporate network, local internet breakouts with SD-WAN and Wi-Fi are 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, bring your own device (BYOD), and internet of things (IoT) cannot be authenticated and identified in Zscaler. They continue to be authenticated on the central infrastructure (controller, anchor controller, network access control) or locally on the network. Consequently, you cannot define security policies on a per-device or per-user basis, making it impossible to enforce a least-access security policy.

Cloudi-Fi extends the authentication capability of Zscaler to secure accordingly all users and devices, including BYOD and IoT. This is particularly relevant to existing ZIA customers who are one click away of this capability.

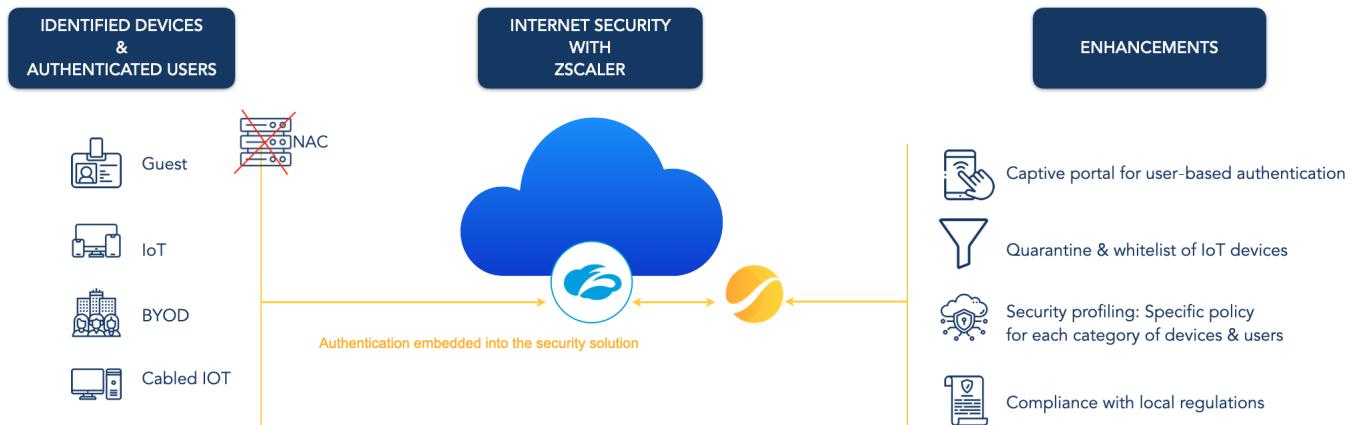


Figure 1. Cloudi-Fi and Zscaler architecture

Enabling Cloudi-Fi into Zscaler provides multiple advantages:

- Total visibility of all guests 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 ZIA, [you must deploy the Cloudi-Fi captive portal](#). Zscaler allows a different setup depending on your existing infrastructure.

Solution Tested

The following diagram shows the Cloudi-Fi integration.

1. Configure an open Service Set Identifier (SSID) on the Access Point (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 the BYOD device IP is not authenticated, Zscaler redirects to the Cloudi-Fi portal.
4. Cloudi-Fi hosts the captive portal and handles guests and BYOD authentication using its directory service.

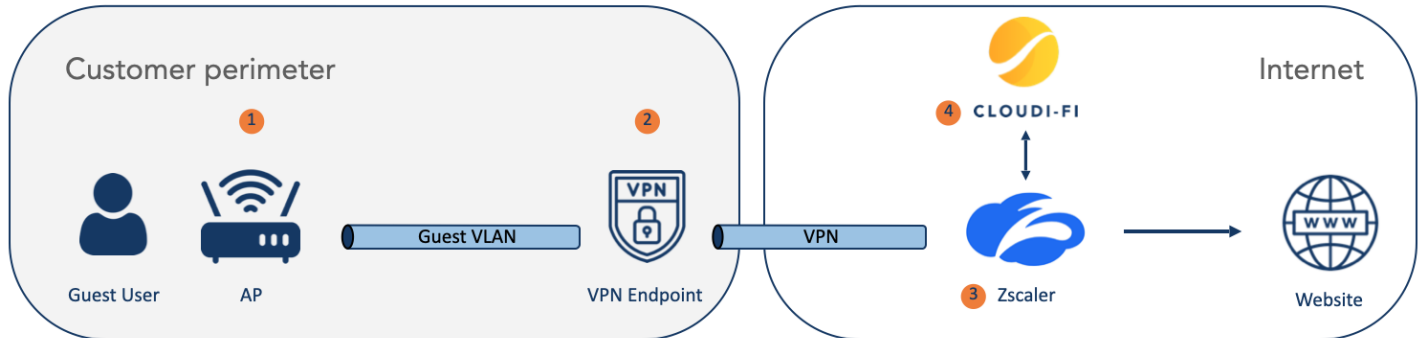


Figure 2. Cloudi-Fi integration

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

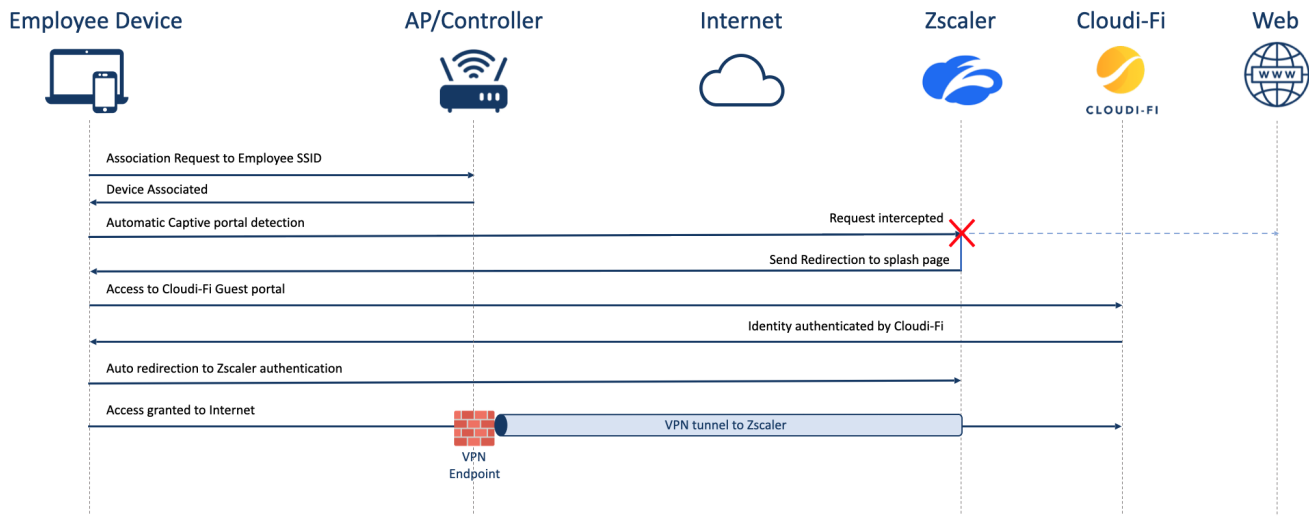


Figure 3. Guest authentication flow

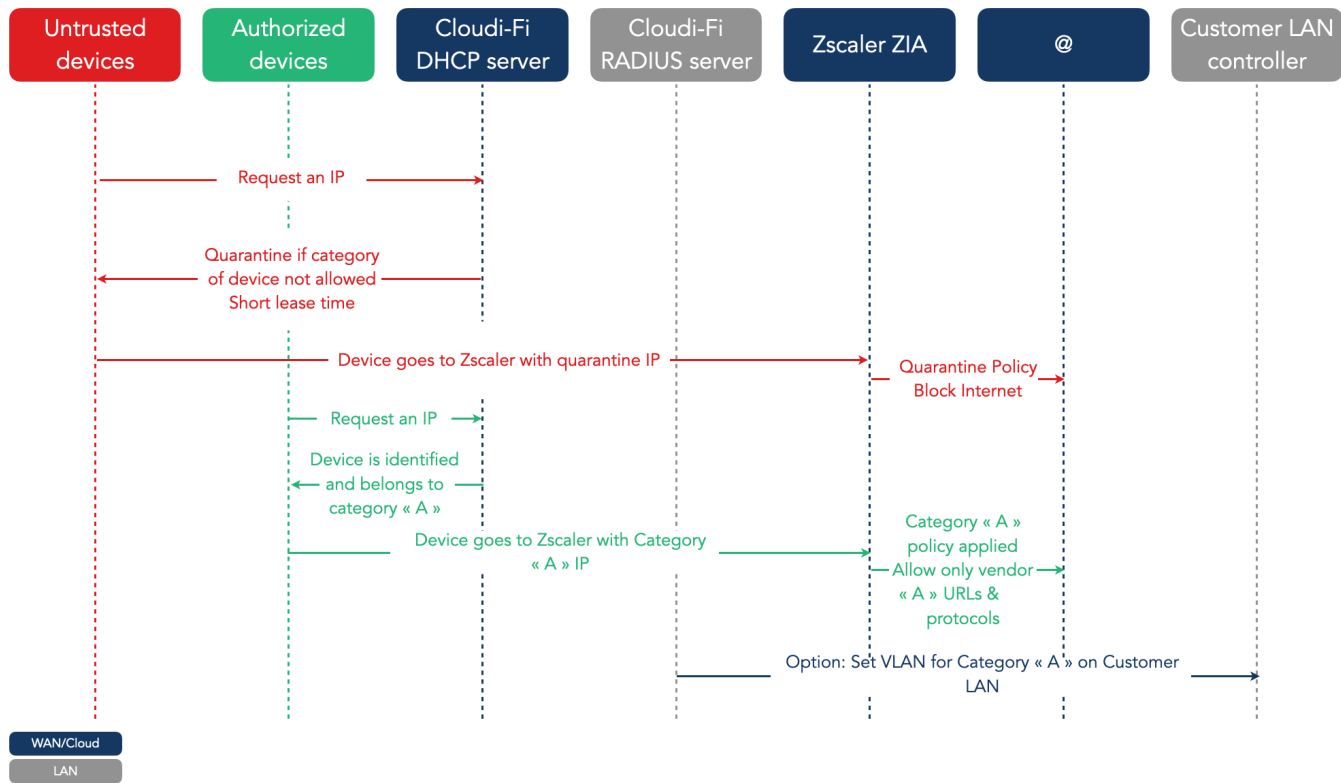


Figure 4. IoT identification flow

This document covers the Cloudi-Fi integration into an existing Zscaler tenant: guest traffic and employees share the same tenant. The option described in this document is the option called a WAN solution with Zscaler shared tenant.

Cloudi-Fi [supports other types](#) of configurations.

Cloudi-Fi Deployment into an Existing Zscaler Tenant

To integrate Cloudi-Fi with an existing Zscaler tenant:

- Deployment for user-based authentication: Cloudi-Fi Captive portal is configured into an existing Zscaler tenant, leveraging existing GRE/IPSec tunnels. The source guest networks 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 are profiled based on how they authenticate in the captive portal. Daily guests, consultants, and employees have specific security policies in Zscaler. Quota, time, and duration are defined for each profile. Categories of IoT are profiled based on the network, matching a sublocation specific to the category of IoT.
- Compliance: In many countries, internet logs are kept for a specific duration and matched with the user. To process the government request, correlate the authentication logs and internet logs. All logs are hosted in the cloud. Authentication logs (in Cloudi-Fi) and pseudonymized internet logs (in Zscaler) are correlated in the Visits menu of the Cloudi-Fi administration interface. Restrict access to this menu to few administrators with administration profiles.

Create a Cloudi-Fi Account

Before beginning, it is mandatory to have your Cloudi-Fi account and credentials with you. If not, go to <https://www.cloudi-fi.com/forms/get-cloudi-fi> and sign up.

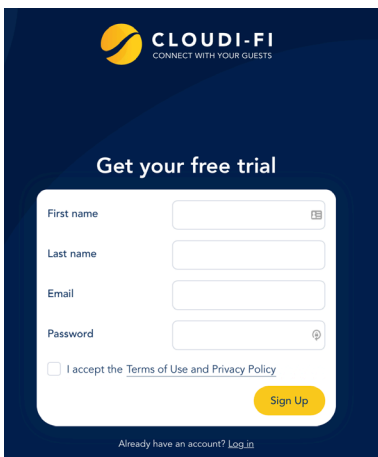


Figure 5. Cloudi-Fi free trial

This immediately activates your free trial account. Cloudi-Fi's teams will contact you to validate the definitive account with you.

If you have a Cloudi-Fi account, you can directly [connect to the Cloudi-Fi Admin UI](#) using your credentials.

Prerequisites for Eligibility

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

Verify the settings in the ZIA Admin Portal.

Tunnels

Guest traffic must go through an IPSec or GRE Tunnel to Zscaler.

The Client IP address must be visible by Zscaler.

No NAT must be applied on traffic going through Zscaler Tunnels.

Authentication Settings

Configure the following Authentication settings:

1. In the ZIA Admin Portal, go to **Administration > Authentication Settings**.
2. Set **User Repository Type** to **Hosted DB**.
3. Set **Authentication Type** to **SAML**.

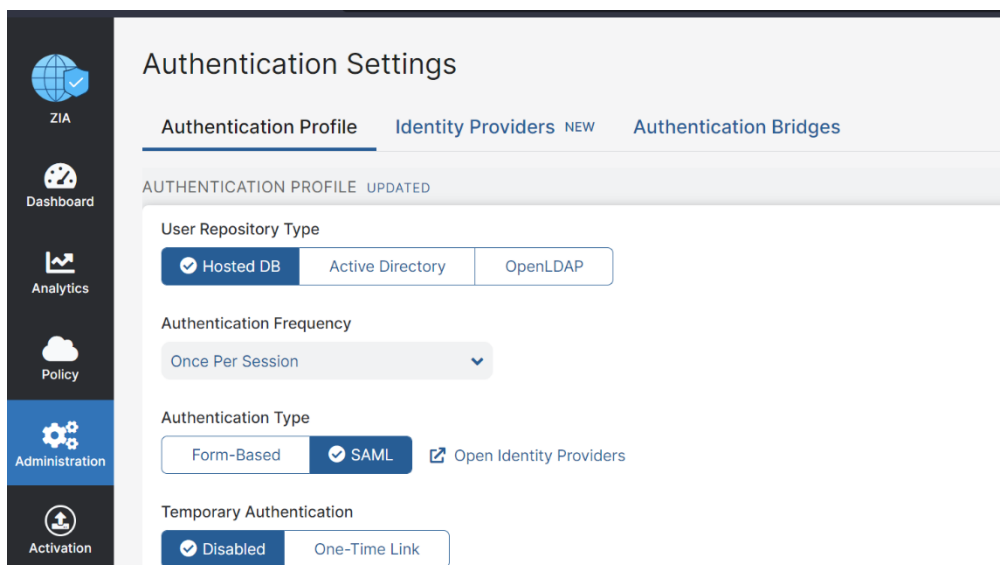


Figure 6. Authentication Settings

Login Attribute for Your Existing IdP

For an existing IdP:

1. In the ZIA Admin Portal, go to **Identity Providers > Edit IdP**. The login attribute returned by your existing Identity Provider (IdP) must be unique and in the form of an email address (e.g., user@my-company.com). If the login attribute returns only a username without any domain, Zscaler cannot perform authentications on multiple domains (e.g., the ADFS Attribute sAMAccountName returns only the username, without a domain).
2. In the ZIA Admin Portal, verify at **Administration > User Management**.
3. Check the **User ID or Name**.

User Management

Users Groups Departments

+ Add User Download Import Sample Import CSV file

User ID or Name Search...

No.	User ID or Name	User Display Name	Groups	Department	Status	Comments	
1	7babe872-b128-4db8-974c-39b8e1249cff@nrb.cl...	Hello	Service Admin	Service Admin	Enabled	Added via Cloudi-Fi	
2	admin@8286542.zsccloud.net	DEFAULT ADMIN	Service Admin	Service Admin	Enabled	---	
3	admin@nrb.cloudi-fi.net	DEFAULT ADMIN (Deprecated)	Service Admin	Service Admin	Enabled	---	
4	anil.singh@nrb.cloudi-fi.net	Anil Singh	Service Admin	Service Admin	Enabled	---	
5	provisioning.api@nrb.cloudi-fi.net	Cloudfi Api	Service Admin	Service Admin	Enabled	---	
6	user1@nrb.cloudi-fi.net	user1@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	
7	user2@nrb.cloudi-fi.net	user2@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	
8	user3@nrb.cloudi-fi.net	user3@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	
9	user4@nrb.cloudi-fi.net	user4@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	
10	user5@nrb.cloudi-fi.net	user5@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	
11	user6@nrb.cloudi-fi.net	user6@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	
12	user7@nrb.cloudi-fi.net	user7@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	
13	user8@nrb.cloudi-fi.net	user8@nrb.cloudi-fi.net	Guest	Guest	Enabled	---	

Help

Figure 7. User Management in ZIA

URL Policies for Unauthenticated Traffic

To set URL policies for unauthenticated traffic:

1. In the ZIA Admin Portal, go to **Administration > Advanced Settings**.
2. Verify that **Enable Policy for Unauthenticated Traffic** is enabled. This option allows Cloudi-Fi to redirect any unauthenticated Guest to the appropriate captive portal page and recognize the Guest location. With this option enabled, you have better control of your traffic by allowing or blocking unauthenticated traffic.

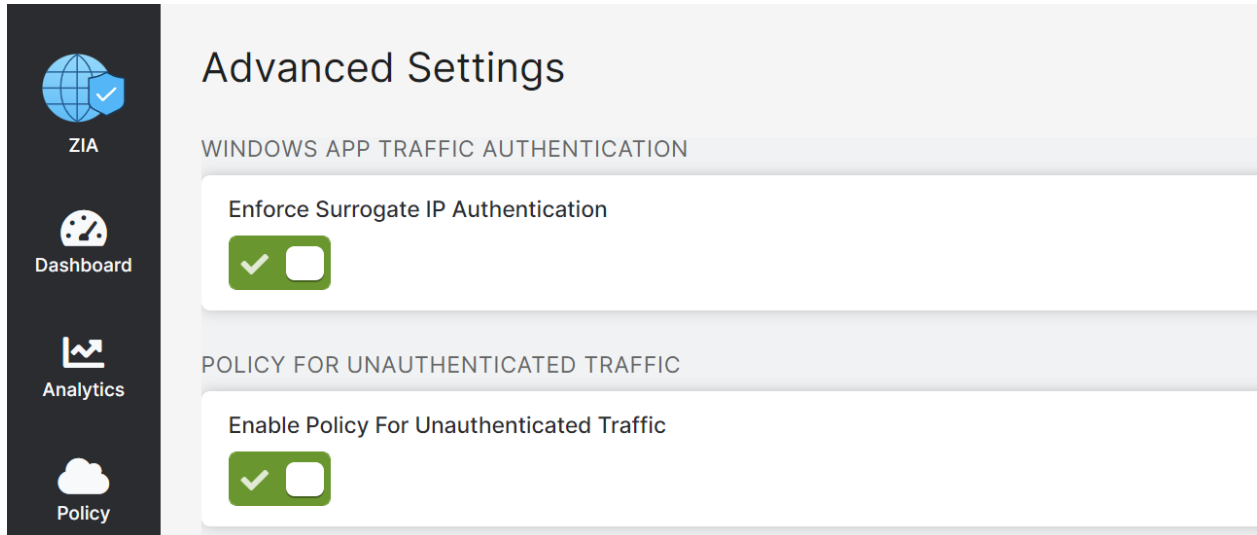


Figure 8. Advanced Settings

Subscriptions

To verify subscriptions:

1. In the ZIA Admin Portal, go to **Administration > Company Profile > Subscriptions**.
2. Verify the API license is set on the Zscaler account and valid.

No.	Name	SKU	Status	Number of Licenses	Service Start Date (PST)	Service End Date (PST)
1	API	Z_API	Subscribed	1 Users	04/29/2018	04/29/2024
2	Basic Reporting	Z_REPORTING	Subscribed	30 Users	04/29/2018	04/29/2024
3	Firewall Basic	Z_FIREWALL_BASIC	Subscribed	30 Users	04/29/2018	04/29/2024
4	URL Filter	URL_FILTER	Subscribed	30 Users	04/29/2018	04/29/2024
5	VPN - Site-to-site	Z_VPN_S2S	Subscribed	30 Users	04/29/2018	04/29/2024
6	Zscaler Client Connector	ZSCALER_CLIENT_CONNECTOR	Subscribed	30 Users	04/29/2018	04/29/2024

Figure 9. Subscriptions in ZIA

Synchronization

The following sections set up synchronization between Cloudi-Fi and ZIA.

Zscaler API Key

First, retrieve the Cloud Service API Key in the ZIA Admin Portal. Go to **Administration > Cloud Service API Key Management**.

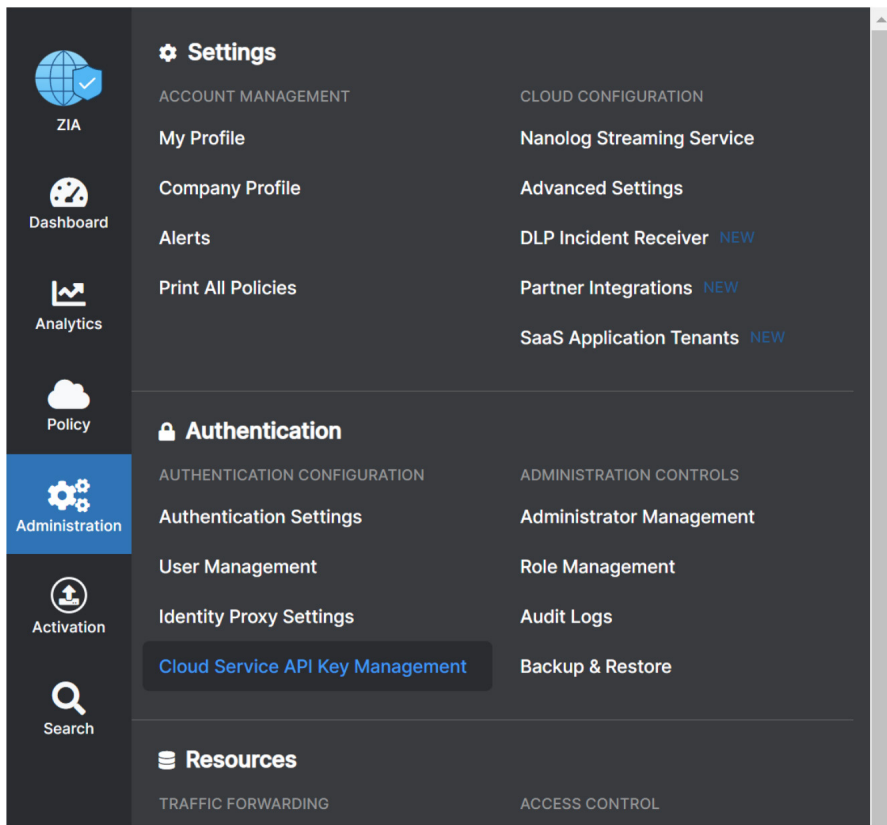


Figure 10. Cloud Service API Key Management

Enabling Zscaler on Cloudi-Fi

To enable ZIA on Cloudi-Fi:

1. Go to the **Cloudi-Fi Administration**.
2. Go to **Cloudi-Fi > Settings > Integrations > Zscaler**.
3. Click **Enable this integration**.

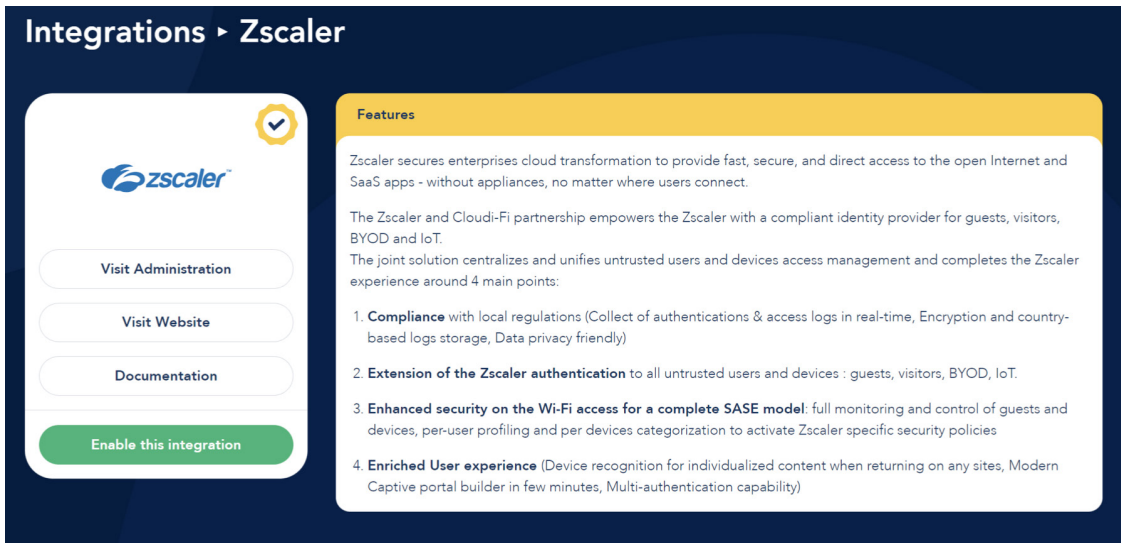


Figure 11. Cloudi-Fi integrations

4. Provide your Zscaler connection details.

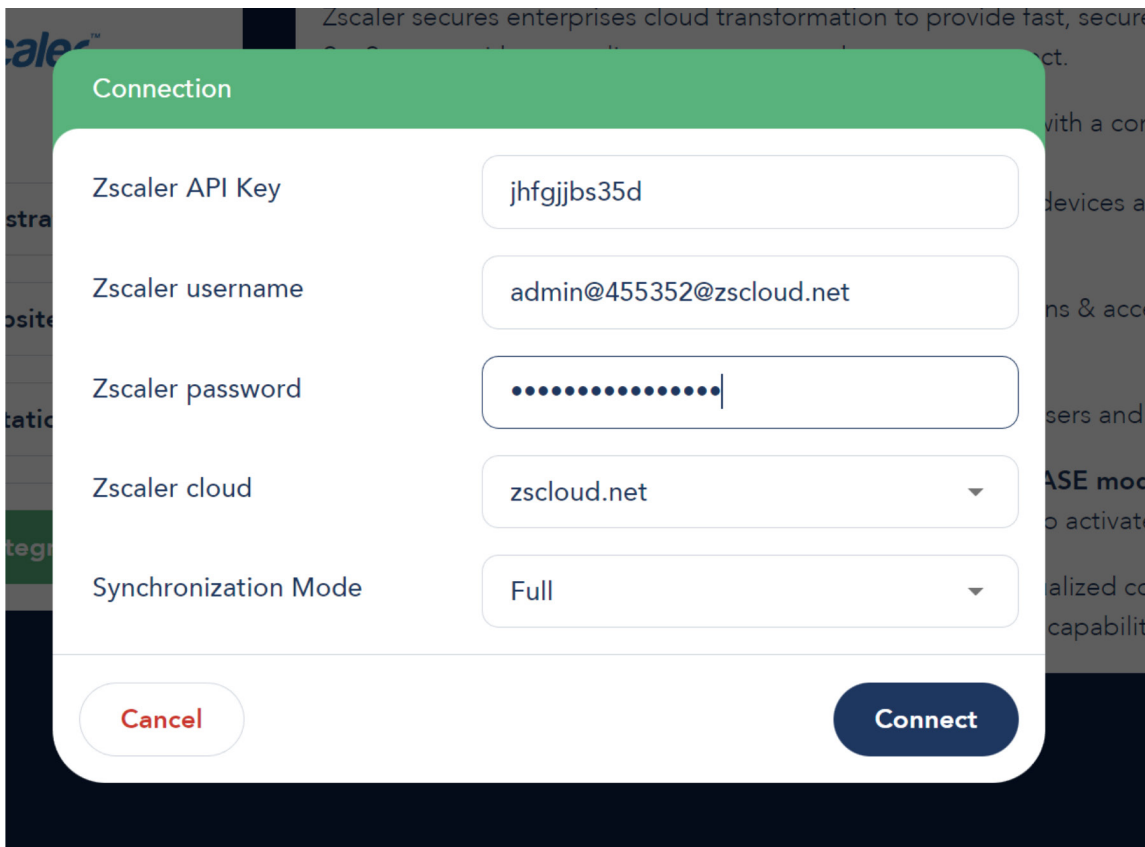


Figure 12. Connection details in Cloudi-Fi

5. Click **Connect**.
6. During the activation process, perform the following actions on your Zscaler tenant:
 - a. Add a new IdP configuration dedicated to Guests (refers to Cloudi-Fi IdP configuration).
 - b. Create multiple custom Categories.
 - c. Customize Advanced Settings (URL Bypass Category list).
 - d. Add a Location Group Cloudi-Fi that contains location and sublocation when the Cloudi-Fi portal is enabled.
 - e. Add base URL Filtering rules. These rules only apply on the Cloudi-Fi location group to make sure the Cloudi-Fi configuration does not interfere with the existing Employee ruleset.
7. See the [Cloudi-Fi documentation](#) for detailed information on the configuration. In the following image, 7 is the number of locations and 12 is the number of location identities.

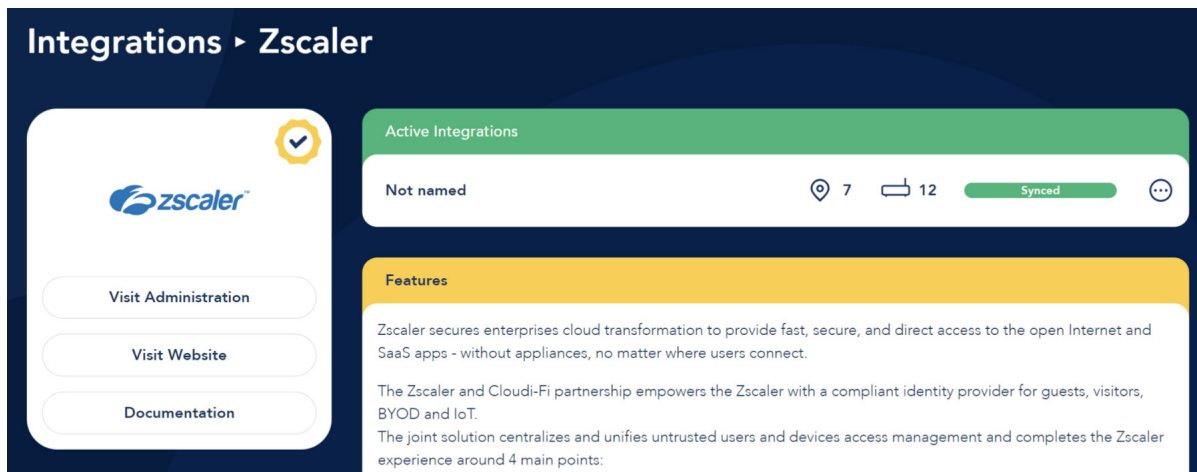


Figure 13. Cloudi-Fi Zscaler Integrations

During the first synchronization, both numbers are set to 0 because you must create locations in Zscaler before the locations are imported into Cloudi-Fi.

Service Activation

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

The Cloudi-Fi captive portal is automatically enabled on your location by changing your location name. Then prefix it with CLOUDIFI-.



To enable Cloudi-Fi on a subset of your Location, you must create a sublocation.

1. In the ZIA Admin Portal, go to **Administration > Location Management**. In the window:
 - a. Select **Create a new Location** for a new location.
 - b. Select an existing location and click the **Edit** icon on the right for a sublocation.
2. To configure your Guest location:
 - a. **Name:** Must start with CLOUDIFI- to match the Dynamic Location Group configuration.
 - b. Set **Enforce Authentication** to **ON**.
 - c. Set **Enable IP Surrogate** and **Enable Surrogate IP for Known Browsers** to **ON**.
 - d. Set **Enforce Firewall Control** to **ON**.

Edit Location

Name: CLOUDIFI-achenes

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: ☒ X

Exclude from Dynamic Location Groups: ☒ X

Location Type: Corporate user traffic

Description:

ADDRESSING

Static IP Addresses and GRE Tunnels: None

VPN Credentials: achenes@nrb.cloudi-fi.net

GATEWAY OPTIONS

Use XFF from Client Request: ☒ X

Enforce Authentication: ☒

Enable IP Surrogate: ☒

Idle Time to Disassociation: 4 Hours

Enforce Surrogate IP for Known Browsers: ☒

Refresh Time for re-validation of Surrogacy: 3 Hours

Enforce Firewall Control: ☒

BANDWIDTH CONTROL

Enforce Bandwidth Control: ☒ Disable

Save Cancel Delete

Figure 14. Edit Location in ZIA

- To check the lifetime session on the Cloudi-Fi administration, go to **Cloudi-Fi > Portals > Templates**.
- Click ... to the right of the Guest location (e.g., Cloud-Fi Base V1 - DO NOT REMOVE).

Name	Creation Date	Usage	Session lifetime	Scope	
Cloudi-Fi Base - DO NOT REMOVE	21/10/2019	-	4 hours	None	⋮
Cloudi-Fi Base V1 - DO NOT REMOVE	24/10/2019	-	4 hours	None	⋮
Cloudi-Fi Base V2 - DO NOT REMOVE	13/12/2019	1 location	4 hours	None	⋮
Cloudi-Fi Base V2 BETA - DO NOT REMOVE	07/02/2020	-	4 hours	None	⋮

Figure 15. Cloudi-Fi templates

- Set the **Session lifetime** to the number of hours required.
- Click **Save**.

Cloudi-Fi Base V1 - DO NOT REMOVE

Information

Name*

Cloudi-Fi Base V1 - DO NOT REM

Enable CDN

☐

Session lifetime*

4 hours

Redirection URL

https://www.cloudi-fi.com

Scope

None

Default Portal

☐

Files

Current package

Download

Upload new package

File upload

Delete

Save

Figure 16. Cloudi-Fi information

Firewall and SSL Inspection

You must adjust the Firewall and SSL Inspection settings in the ZIA Admin Portal to ensure access for your Guests.

The Firewall and SSL Inspection settings are in addition to the base Cloudi-Fi ruleset.

Rule Order	Rule Name	Criteria	Action	Label and Description
1	Apple Captive Portal - 71	DEPARTMENTS Unauthenticated Transactions REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER URL CATEGORIES Cloudifi Apple Check URLs	Block With Redirect Redirect URL: https://login-uat.cloudi-fi.net/auth/saml2/dp/SSO5erv	
2	Walled Garden - 71	REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER URL CATEGORIES Cloudifi Portal; Cloudifi Apple Check URLs	Allow	
3	Cloudi-Fi Redirection - 71	DEPARTMENTS Unauthenticated Transactions; WallGuard REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER	Block With Redirect Redirect URL: https://login-uat.cloudi-fi.net/auth/saml2/dp/SSO5erv	
4	Denied Categories - 71	REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER URL CATEGORIES Other Adult Material; Adult Themes; Lingerie/Bikini; Nudity; Pornography; Sexuality; Adult Sex Edu...	Block With Redirect Redirect URL: https://login-uat.cloudi-fi.net/eun.php	DESCRIPTION Default categories blocked for all users
5	Department Allow - 71	DEPARTMENTS Guest; NewProfile REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER	Allow	DESCRIPTION Default allow rule for authenticated users
6	Block Rule - 71	REQUEST METHODS OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONNECT; OTHER	Block With Redirect Redirect URL: https://login-uat.cloudi-fi.net/eun.php	

Figure 17. Cloudi-Fi ruleset

Firewall Configuration

Configure Firewall filtering policies:

1. In the ZIA Admin Portal, go to **Policy > Firewall control**.

Firewall Filtering Policy		NAT Control Policy		
Add Firewall Filtering Rule		Recommended Policy View by: Rule Order Rule Label Search...		
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	

Figure 18. Zscaler Firewall Filtering Policy

2. Allow **Web Guest Locations** (Rule 3).
3. Enable **Deny All Guest** (Rule 4).

SSL Inspection policies

If you have SSL Inspection enabled, you must check your existing policies and create a dedicated SSL policy for Guest traffic.

In the ZIA Admin Portal, go to **Policy > SSL Inspection**.

Rule Order	Rule Name	Criteria	Action	Label and Description
1	Cloudi-Fi	LOCATION GROUPS CLOUDIFI	Do Not Inspect Evaluate Other Policies Show End User Notifications Disabled Untrusted Server Certificates Allow OCSP Revocation Check Disabled Minimum TLS Version TLS 1.0	

Figure 19. Zscaler SSL Inspection

Adding Newly Created Guest Profiles

Your Guest can have different profiles. These profiles are shared by Cloudi-Fi to Zscaler through SAML Auto-Provisioning. You might need 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.

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support:

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

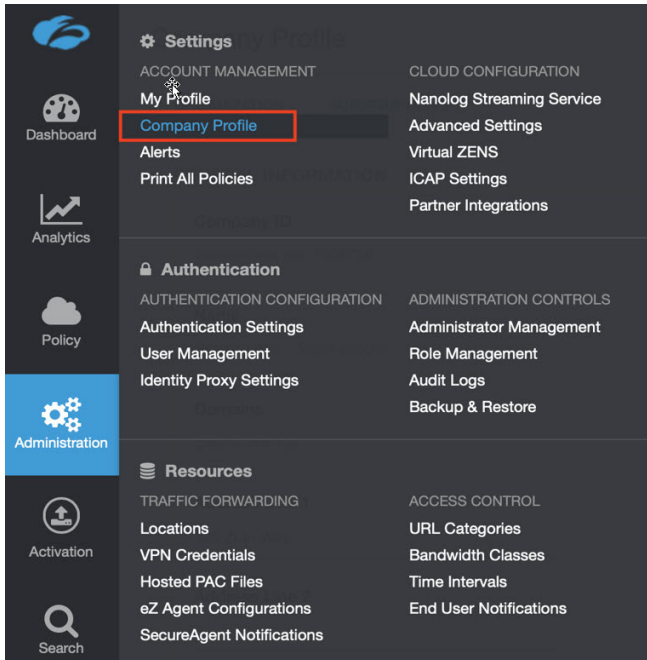


Figure 20. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

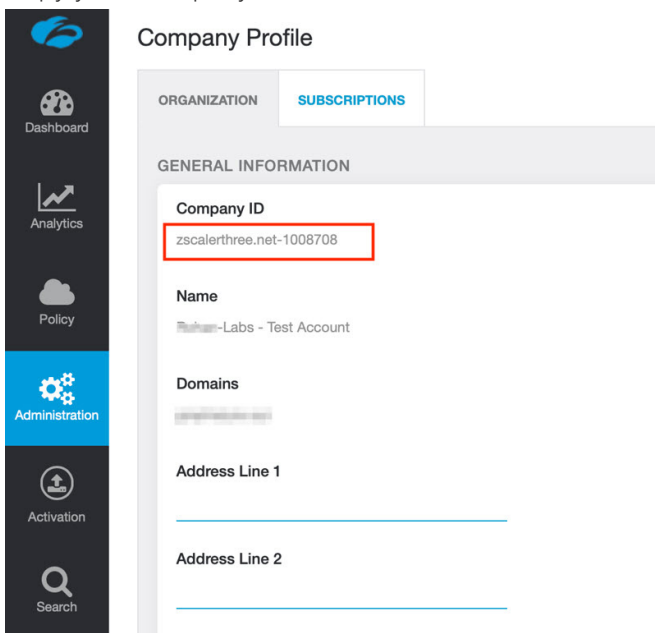


Figure 21. Company ID

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

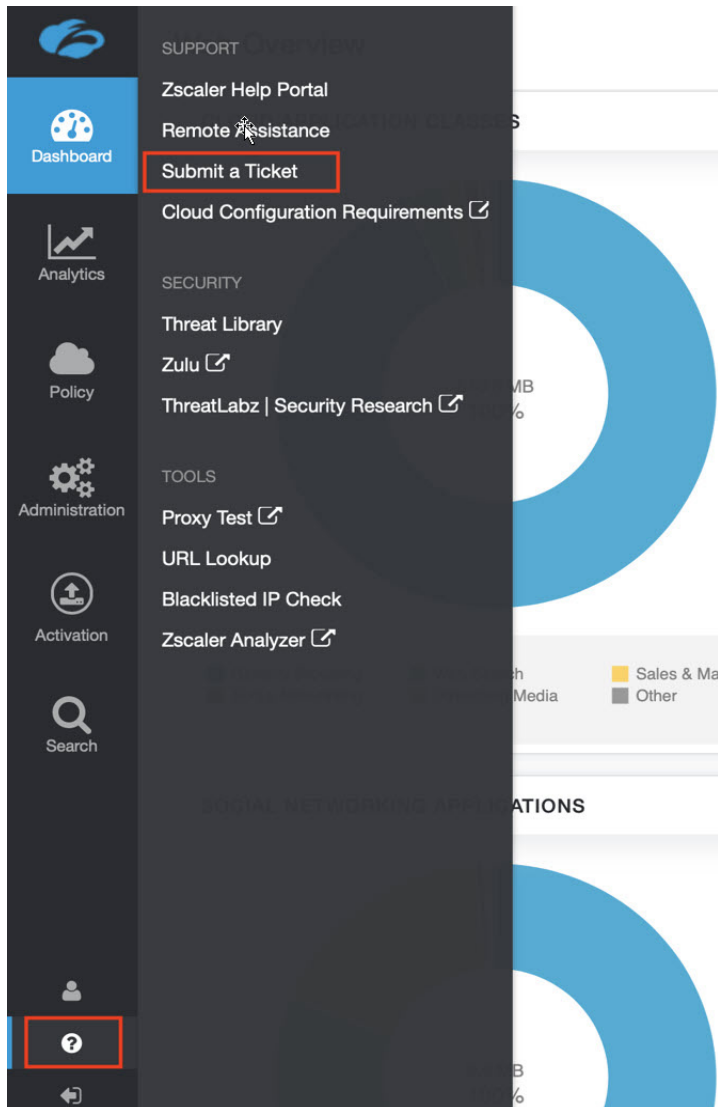


Figure 22. Submit a ticket