

Cloudi-Fi integration with Zscaler ZIA

Zscaler ZIA v6.1 & later

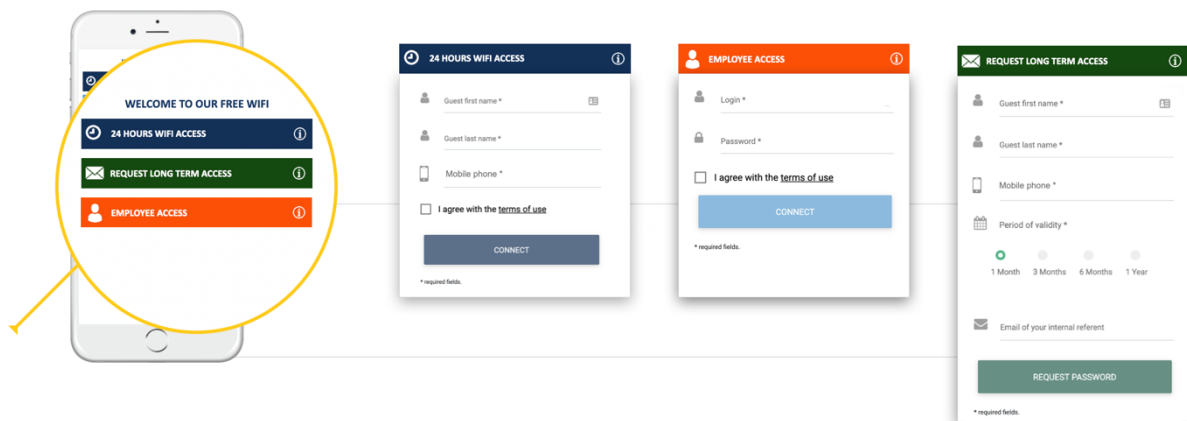
Table of Contents

1	<i>Solution overview.....</i>	<i>3</i>
2	<i>Zscaler deployment into an existing Zscaler tenant.....</i>	<i>7</i>
2.1	Prerequisites for Eligibility	7
2.2	Provide your Zscaler account information	8
2.3	Add Cloudi-Fi Guest domain to your Zscaler account.....	8
2.4	Create Cloudi-Fi Identity Provider	8
2.5	Create Cloudi-Fi Custom URL Categories	11
2.6	Create Authentication By-pass.....	11
2.7	URL filtering policies for guests	12
2.8	Dynamic group of Cloudi-Fi location(s)	13
2.9	Create your Guest location/sub-location	14
2.10	Create the Guest Firewall policy rules	16
2.11	Administration and reporting.....	16

1 Solution overview

This article describes the various architectures to manage guest network with Zscaler ZIA and Cloudi-Fi. For an existing Zscaler customer, the guest network is usually secured by the tenant, but authentication is done locally on the network. The consequence is that all guests are not identified into Zscaler and only one policy is applied to all traffic (daily guests, consultants, and BYOD). Enabling captive portal into Zscaler with Cloudi-Fi provides multiple advantages:

- Personalized guests onboarding
- Profiling of guests with security policies for each profile
- Total visibility of all guest's traffic
- Compliance with local regulations (Data privacy and Internet provider regulations)



In order 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 above diagram 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

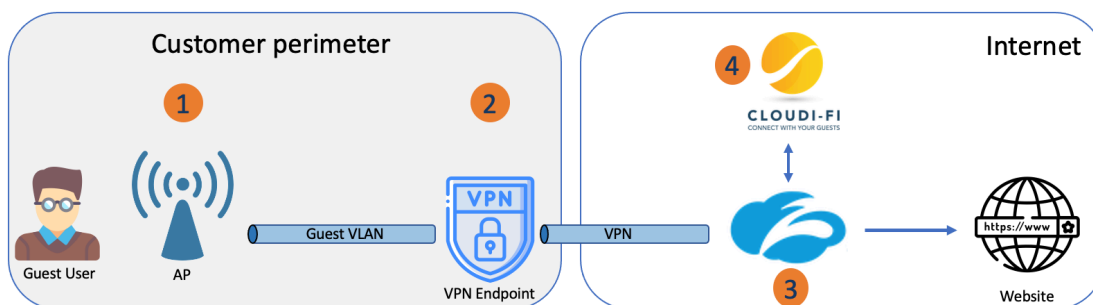


Figure - Configuration Overview

Configuration option`

3 different configurations are possible with consequences in terms of setup and licensing.

Please note that this document is subject to be enhanced as Cloudi-Fi & Zscaler may allow easier configuration for certain configurations in the future.

- 1/ **The WAN solution with Zscaler dedicated tenant** is recommended for a new customer to Zscaler or for **hotspot**
- 2/ **The WAN solution with Zscaler shared tenant** is recommended for an **existing Zscaler customer** who wants to leverage his existing tenant.
- 3/ **The LAN solution with Local Captive Portal** is recommended for a customer who cannot benefit from configuring Cloudi-Fi into Zscaler and who will proceed with **local configuration** with Cloudi-Fi.

Solutions matrix	WAN - Zscaler dedicated tenant	WAN - Zscaler shared tenant	LAN - Local captive portal
Recommended for	Hotspot or new customer to Zscaler	Existing Zscaler customer	Existing Zscaler customer
Authentication	native to Zscaler	native to Zscaler	in the WiFi
Zscaler tenant	Dedicated	Shared	Shared
Setup	Automated	Manual	Manual
Compliance	Full, tokenized	Full, tokenized	Partial, requires private IP in logs
New tunnels required	Yes	No	No
Setup complexity	Easy	Medium	High
Security	High	High	Limited, cannot profile guests
Management	One unique administration	2 administrations: Cloudi-Fi & Zscaler	Complex, different solutions to maintain
Zscaler licensing	Embedded with Cloudi-Fi Enterprise bundle based on total traffic	BYOD recognized, additional Zscaler licences for guests	BYOD/guests/servers/IOT are mixed up. transactions for unauthenticated traffic licensing

1/ Option 1 and 2: Authentication flow with WAN deployment

The captive portal is enabled into Zscaler There is no LAN configuration except the creation of open guest SSID and DNS/DHCP service.

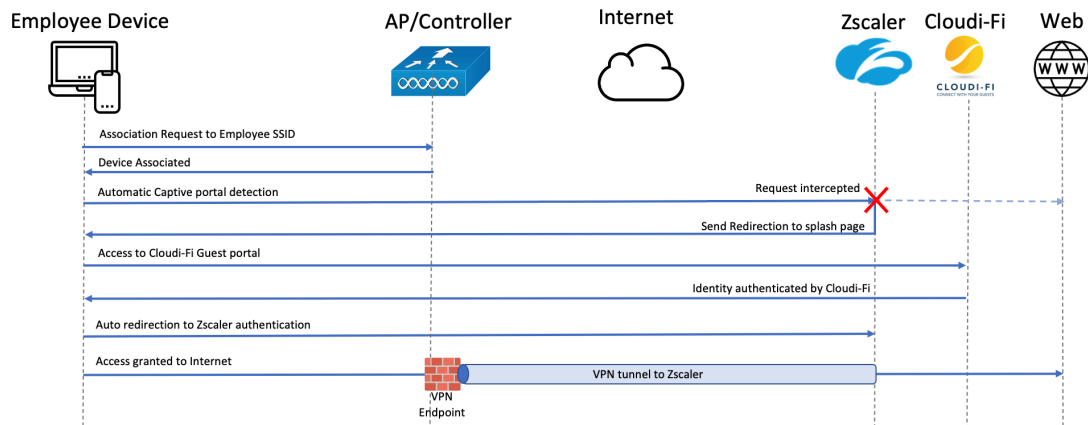


Figure - Authentication workflow - WAN deployment

The service is reusing existing Zscaler instance used for employee's protection or a new instance. The guest network should be routed into the Zscaler tunnels, new locations will be provisioned into Zscaler with authentication to Cloudi-Fi enabled. Policies, quota, QOS can be enabled per profile of guests.

2/ Option 3: Authentication flow with LAN authentication

The captive portal is configured natively on the Wi-Fi infrastructure with external authentication (URL redirect & Radius server).

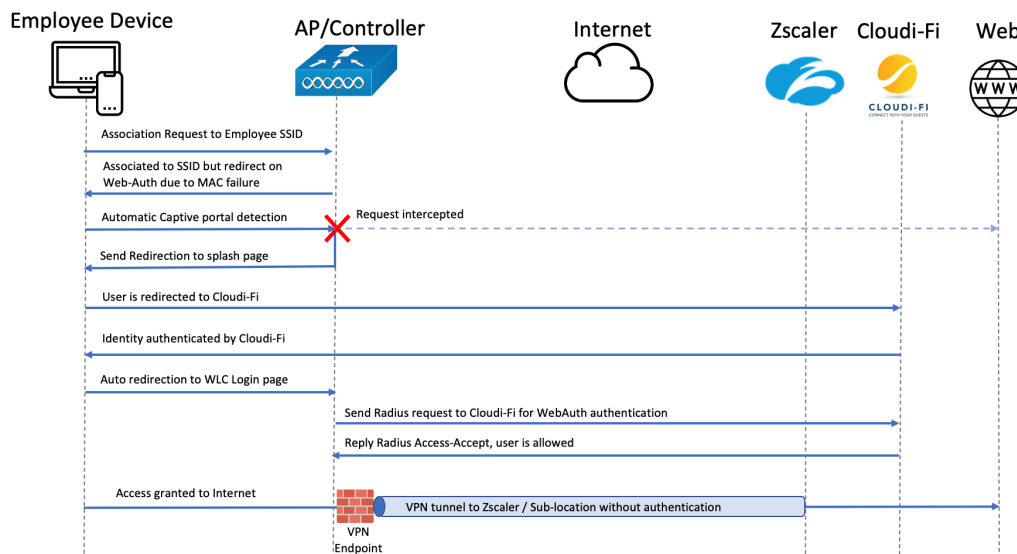


Figure - Authentication workflow in Hybrid LAN/WAN deployment

The service is reusing existing Zscaler instance used for employee's protection. The guest network should be routed into the existing Zscaler tunnel with an identified private network. This private network will belong to a Zscaler sublocation with authentication disabled.

2 Zscaler deployment into an existing Zscaler tenant

- **Deployment:** Cloudi-Fi Captive portal is configured into an existing Zscaler tenant leveraging existing GRE/IPSEC tunnels. The source guest network(s) should be routed into the tunnels.
- **Security:** Guests can be profiled based on how they authenticate in the captive portal. Daily guest, consultants, employee along with their directory group can all have different policies in Zscaler. Security policies but also quota, time and duration can be configured for each profile.
- **Compliance:** In many countries Internet logs should be kept for a specific duration and matched with the user. In order 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.
- **Configuration:** Zscaler configuration is not synchronized with Cloudi-Fi compared to a setup with a dedicated Zscaler tenant. However Zscaler configuration is done in few steps and described below.

2.1 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:

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.**

Exemple: user@my-company.com

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

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

2.2 Provide your Zscaler account information

Go to your **Zscaler Admin interface > Administration > Company Profile**

Copy/Paste the following information:

- **Company ID**
- **Name**
- **Domains**
- **Cloudi-Fi IDP ID when available**

2.3 Add Cloudi-Fi Guest domain to your Zscaler account

Submit a ticket to Zscaler support to add the Cloudi-Fi authentication domain. The domain name is provided by Cloudi-Fi team.

Example : `your-company.cloudi-fi.net`

2.4 Create Cloudi-Fi Identity Provider

Go to **Administration > Authentication Settings > Identity Provider tab >**

Add Identity Provider :

- **IDP SAML Certificate** : [Available here](#)
- **SAML Portal URL** : Provided by Cloudi-Fi team
- **Login Name Attribute** : token
- **Location**: None
- **Domain**: Cloudi-Fi dedicated domain
- **Auto-provisionning**: ON
- **User Display Name Attribute**: token
- **Group Name Attribute**: profile
- **Department Name Attribute**: profile
- **Save**

Edit IdP



GENERAL INFO

Name

Cloudi-Fi Guest|IdP

Status

☒ Enabled

☐ Disabled

SAML Portal URL

https://login-.cloudi-fi.net/auth/saml2/idp/SSOS...

Login Name Attribute

token

Entity ID

zscalertwo.net

Org-Specific Entity ID

☐ Enabled

☒ Disabled

IdP SAML Certificate

server2017.crt.zscaler.pem

[Upload](#)

IdP SAML Certificate Expiration Date

August 26, 2027

Vendor

[Others](#)

**Default IdP**

☒ Enabled

CRITERIA

Locations

[Any](#)

**Authentication Domains**

[Any](#)



SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request



SP Metadata

[Download Metadata](#)

PROVISIONING OPTIONS

Enable SAML Auto-Provisioning



User Display Name Attribute

token

Group Name Attribute

profile

Department Name Attribute

profile

Enable SCIM Provisioning



Save

Cancel

AUTHENTICATION PROFILE

IDENTITY PROVIDERS

NEW

AUTHENTICATION BRIDGES

[+ Add Identity Provider](#)

[+ Add Zscaler Client Connector Portal as IdP](#)

No.	ID	Name	Status	Location	IdP SAML Certifica...	Authentication Do...	Default IdP
1	5427	Your-Company-IdP	✓	CLOUDIFI-with-idp	September 12, 2024	mck.cloudi-fi.net	<input type="radio"/>
2	5250	cloudifi	✓	Any	August 26, 2027	Any	<input checked="" type="radio"/>

Save the ID assigned to Cloudi-Fi IDP and share it with Cloudi-Fi team.

2.5 Create Cloudi-Fi Custom URL Categories

Go to Administration > URL Categories > Add URL Category :

We need to create 2 custom categories:

- **Cloudi-Fi Portal URL** : This category contains all URLs to be whitelisted in order to display our captive portal properly :

```
.cloudi-fi.net
.cloudi-fi.com
```

Cloudi-Fi Connectivity Check URL : This category contains all the URL used by guest's devices to detect the presence of a captive portal.

Below the Custom URL and Custom Key Words to be added :

Custom URLs:

```
captive.apple.com
www.apple.com/library/test/success.html
detectportal.firefox.com
www.msftconnecttest.com
www.msftncsi.com
```

Custom Key words:

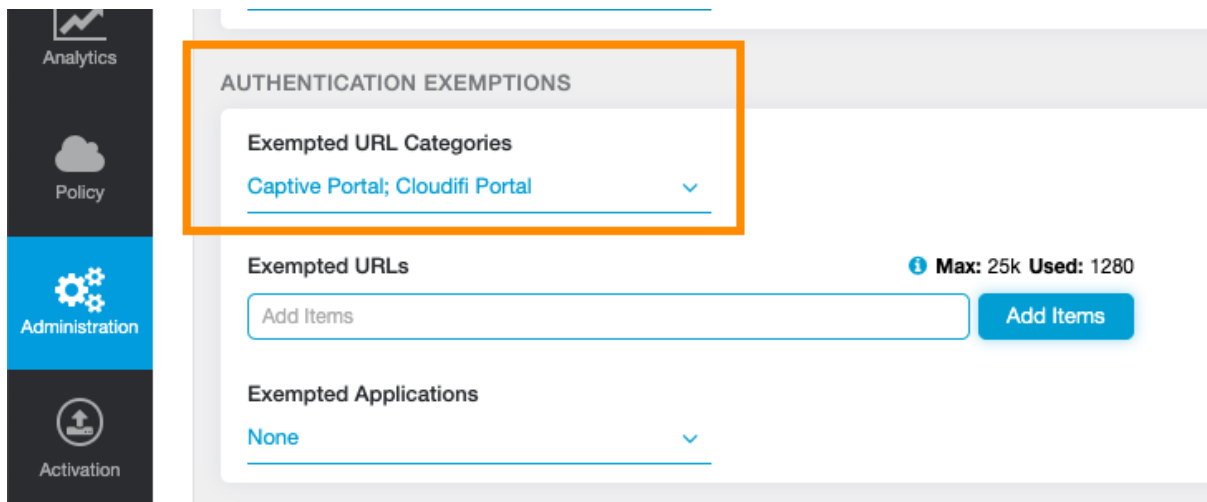
```
/generate_204
/gen_204
```

2.6 Create Authentication By-pass

To prevent visitors to be redirected to your Authentication IdP, we configure a by-pass for the 2 URL Categories we created previously.

Go to **Administration > Advanced Settings:**

- In **Authentication Exemptions** section, add our 2 custom categories.



The screenshot shows the Zscaler Administration console interface. On the left is a sidebar with icons for Analytics, Policy, Administration (highlighted in blue), and Activation. The main content area is titled 'AUTHENTICATION EXEMPTIONS'. It contains three sections: 'Exempted URL Categories' with a dropdown menu showing 'Captive Portal; Cloudifi Portal' (highlighted with an orange box), 'Exempted URLs' with an 'Add Items' input field and a status indicator 'Max: 25k Used: 1280', and 'Exempted Applications' with a dropdown menu showing 'None'.

- **Enable Policy for Unauthenticated Traffic** : Enabled

POLICY FOR UNAUTHENTICATED TRAFFIC

Enable Policy For Unauthenticated Traffic

☒

Note : If this option was initially disabled in your account, an additional URL policy rule should be added when you will create Cloudi-Fi policy rules in the next section.

2.7 URL filtering policies for guests

Configure this bundle of rules in order to redirect your guests on your captive portal, allow authentication users to browse Internet and prevent them from accessing forbidden categories. Cloudi-Fi team can assist you in the creation of these rules.

And thanks to dynamic groups, you don't need to update these rules every time you deploy a new Guest location (more information in the next section).

URL & Cloud App Control

Configure URL & Cloud App Control Policy
Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is allow all.

URL FILTERING POLICY **CLOUD APP CONTROL POLICY** ADVANCED POLICY SETTINGS

+ Add URL Filtering Rule

Rule Order	Rule Name	Criteria	Action	Description
1	Valley Garden	LOCATION GROUPS CLOUDIFY REQUEST METHODS OPTIONS: GET HEAD POST PUT DELETE TRACE CONNECT OTHER URL CATEGORIES Cloudify Portal	Allow	
2	Cloudify Redirection	DEPARTMENTS Unauthorized Transactions LOCATION GROUPS CLOUDIFY REQUEST METHODS OPTIONS: GET HEAD POST PUT DELETE TRACE CONNECT OTHER	Click With Redirect Redirect URL: https://login.cloudify.net/auth/oauth2/http://SSOService.php?openid=api.opendataservice.net&id=4505505845f721855d5c7d5d	
3	Denied Categories	LOCATION GROUPS CLOUDIFY REQUEST METHODS OPTIONS: GET HEAD POST PUT DELETE TRACE CONNECT OTHER URL CATEGORIES Other Adult Material, Adult Themes, Languages/Games, Nudity, Pornography, Sexuality, Adult Sex Education, K-12 Sex Education, Other Drugs...	Deny	Default categories blocked for ...
5	Guest Allow	DEPARTMENTS Guest LOCATION GROUPS CLOUDIFY REQUEST METHODS OPTIONS: GET HEAD POST PUT DELETE TRACE CONNECT OTHER THE Business Hour URL CATEGORIES Other Business and Economy, Corporate Marketing Finance, Professional Services, Classifieds, Other Education Continuing EducationCo...	Allow	Default allow rule for auth users
6	BYOD Allow	DEPARTMENTS BYOD LOCATION GROUPS CLOUDIFY REQUEST METHODS OPTIONS: GET HEAD POST PUT DELETE TRACE CONNECT OTHER	Allow	Allow rule for employees
7	Block rule	REQUEST METHODS OPTIONS: GET HEAD POST PUT DELETE TRACE CONNECT OTHER	Click With Redirect Redirect URL: https://login.cloudify.net/home.php	

Note: if the option **Enable Policy for Unauthenticated Traffic** was disabled in Advanced Settings (see previous section), you must add the following rule **at the end of Cloudi-Fi rules**:

11	Allow Unauthenticated Traffic	<p>DEPARTMENTS</p> <p>Unauthenticated Transactions</p> <p>REQUEST METHODS</p> <p>OPTIONS; GET; HEAD; POST; PUT; DELETE; TRACE; CONN...</p> <p>PROTOCOLS</p> <p>DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP over HTTP; ...</p>	Allow
----	-------------------------------	---	-------

2.8 Dynamic group of Cloudi-Fi location(s)

Zscaler Dynamic group can be leveraged to simplify the management of guest rules, logs and policy into an existing Zscaler account.

This will allow any new location named Guest to dynamically belong to this Group. Alternatively the condition would be to include all locations with authentication disabled

From now, any new guest location will belong automatically to the group "CLOUDIFI". This will add it automatically to policy rules, reports and logs and will segregate clearly the data and configuration between the guest and the corporate traffic. (see section 9 for more information about it).

Define a condition for your Guest location.

Go to `Administration > Location Management > Location Groups tab > Create New

Edit Dynamic Group

1 Group Information

2 Preview Locations

GENERAL

Name

CLOUDIFI

Description

Locations managed by Cloudi-Fi

GROUP CONDITIONS

Name

Contains

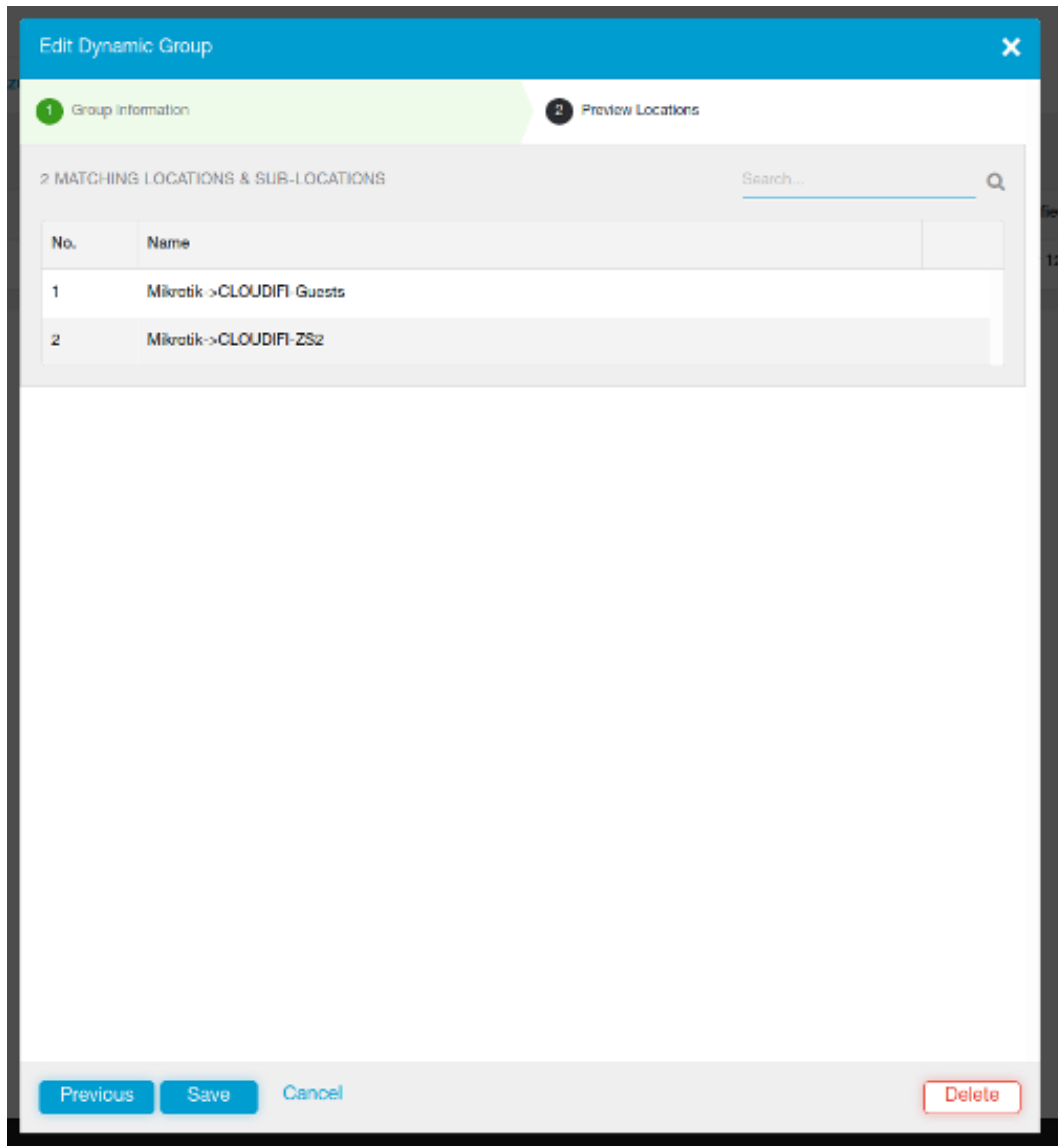
CLOUDIFI

Add New Condition

Next

Cancel

Delete



2.9 Create your Guest location/sub-location

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).

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 match the condition of your Cloudi-Fi dynamic group
- **Enforce Authentication**: ON
- **Enable IP Surrogate (both options)** : Timers should be equal to Cloudi-Fi lifetime session
- **Enforce Firewall control** : ON

15

2.10 Create the Guest Firewall policy rules

Notes : We recommend to configure these rules at the beginning of your Firewall Policy.

Go to **Policy > Firewall control**

FIREWALL FILTERING POLICY

NAT CONTROL POLICY

+ Add Firewall Filtering Rule

Rule Order	Rule Name	Criteria	Action
2	Allow Web Guest locations	LOCATION GROUPS CLOUDIFI NETWORK SERVICES DNS; HTTP; HTTPS	Allow
3	Deny All Guest	LOCATION GROUPS CLOUDIFI	Block/Drop

2.11 Administration and reporting

Administrators can have restricted scope to the dynamic location and can only see guest (or non guest) data

ADMINISTRATOR

Login ID	
guestadmin	@ cloudi-demo-corpo.cloudi-fi.net
Email	Name
subscribe@cloudi-fi.com	
Role	
Guestadmin	
Scope	Location Groups
Location Group	Guest

Alternatively an administrator with all access can build specific reports/insights/log views for guest (or by extension non guest) data.

Custom reports built for guest only

1. Report Data Class

Web

2. Timeframe

Current Month: 11/1/2020 - 11/19/2020 ▾

☐ Allow time to be set for each widget

3. Select Filters

Location Group



Guest



Add Filter



Custom logs research

Insights

Logs

↺ Start Over

Timeframe

Current Day: 11/19/2020 ▾

Number of Records Displayed

1k

✓ 5k

10k

25k

Select Filters

✕ Clear Filters

Location Group

✕

Guest ▾

Add Filter ▾

Apply Filters