

## KASM and Cloudflare Tunnel with Cloudflare Access

### Pre-Requisites

1. Configured working KASM environment
2. Configured working Cloudflare Tunnel

For KASM environment refer to Setting up KASM workspace and their official documentation.

For Cloudflare Tunnel, refer Cloudflare Tunnel official documentation.

### Quick Overview on KASM and Cloudflare Tunnel Setup/Configuration

In this example

[← Back to cft1](#)

#### Public hostnames

Edit public hostname for cft1

Hostname

Subdomain

space

Domain (Required)

lay.network

Path

(optional) path

Service

Type (Required)

HTTPS

URL (Required)

192.168.1.237

For example, https://localhost:8001

Additional application settings

Save

### Settings under TLS

Additional application settings

TLS

Origin Server Name

Hostname that cloudflared should expect from your origin server certificate.

Null

Certificate Authority Pool

Path to the certificate authority (CA) for the certificate of your origin. This option should be used only if your certificate is not signed by Cloudflare.

Null

No TLS Verify

Disables TLS verification of the certificate presented by your origin. Will allow any certificate from the origin to be accepted.

ON

TLS Timeout

Timeout for completing a TLS handshake to your origin server, if you have chosen to connect Tunnel to an HTTPS server.

10 seconds

HTTP2 connection

Attempt to connect to origin using HTTP2. Origin must be configured as https.

OFF

HTTP Settings

Connection

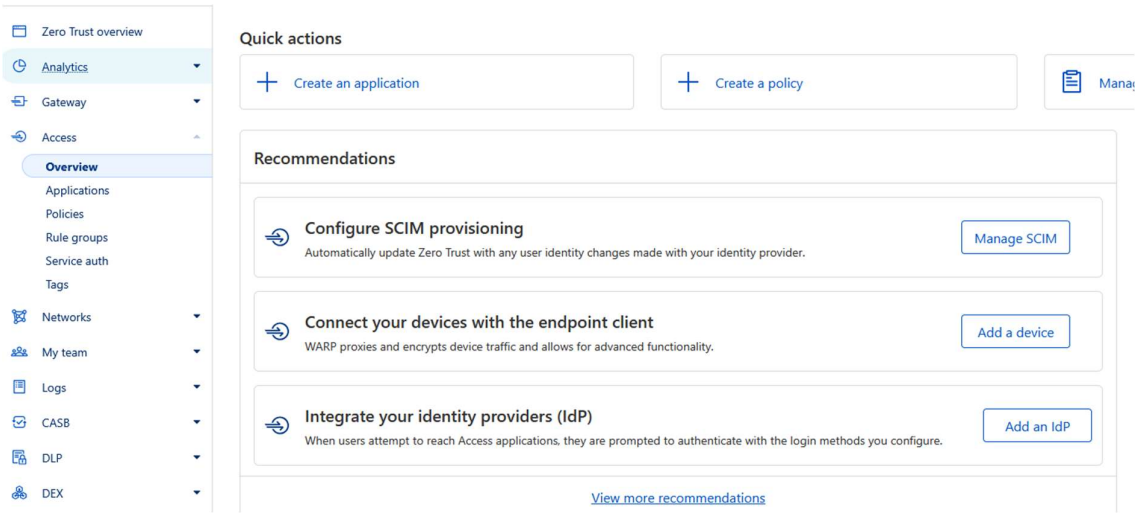
Access

HTTP Settings, Connection, Access all left as default.

### Adding to Cloudflare Access

Since the public hostname “space.lay.network” is accessible outside, it can now be gated behind cloudflare access.

Create a policy



Click on Create a policy and build one.

Provide a name, and define the action – in this case, Allow. Define the session duration if required.

**Basic Information**  
Name your policy and choose the action Access should take. [Access action documentation](#)

<b>Policy name</b> (Required)	<b>Action</b> (Required)	<b>Session duration</b>
<input type="text" value="Secure Users"/>	<input type="text" value="Allow"/>	<input type="text" value="Same as application session timeout"/>

12 / 350

Adding rules

Choose a selector, eg. Email, or any available.

**Add rules**  
Define the policy's scope using rule types, selectors, and selector values. Selectors are the type of criteria or attributes you want users to meet. Configure additional selectors by adding lists, login methods, and device posture checks. [Selector documentation](#)

**Include** OR

If more than one Include rule is configured, users only need to meet one of the criteria.

Selector (Required)	Value
<input type="text" value="Select..."/>	<input type="text" value="Select criteria for your rule"/>

+ Any Access Service Token

+ Authentication Method

+ Common name

+ Country

+ Emails

+ Emails ending in

+ Everyone

+ External Evaluation

**Purpose justification** ☒   
Requires a user to enter a justification for any access to this application.

**Purpose justification prompt**  
This is a sensitive domain. Please provide a business reason for your need to access before continuing.

In this case, "Emails" will suffice, add those emails you want to have users access to, if they are whitelisted, they are allowed to access the service after authenticating.

Add rules

Define the policy's scope using rule types, selectors, and selector values. Selectors are the type of criteria or attributes you want users to meet. Configure additional selectors by adding lists, login methods, and device posture checks. [Selector documentation](#)

Include

OR

If more than one Include rule is configured, users only need to meet one of the criteria.

Selector (Required)

Value

Emails

testing@hotmail.com | email@example.com

+ Add include

+ Add require

+ Add exclude

Enter and tab as many email addresses you can, limited to 50 on the free Cloudflare Access

Policy tester

The policy tester evaluates the last seen identity of active users. Login decisions may differ if there are changes to user attributes evaluated by this policy.

Test policy

Additional settings (optional)

Purpose justification

Requires a user to enter a justification for any access to this application.

Purpose justification prompt

This is a sensitive domain. Please provide a business reason for your need to access before continuing.

Temporary authentication

Beta

Requires a user to obtain temporary access from authorized approvers.

Email addresses of the approvers

Cancel

Save

Click Save, this saves the policy for email authentication using only [testing@hotmail.com](#)

Access / Policies

Policies

Control inbound traffic to your Access applications. Only users who match your policies will have access to your configured applications. [Access policies documentation](#)

Your policies Showing 1-5 of 5

Manage the rule groups, actions, and settings of your reusable policies. You can use these policies across multiple different applications.

+ Add a policy

Search

Show filters

Policy name	Action	Rules	Used by applications	Policy ID
Secure Users	ALLOW	1	0	6cbefd7d-424a-47dd-863f-91bce00846df

Once the policy is setup, time to add the application KASM

Access / Applications

Applications

Protect your Self-Hosted, SaaS, and Private applications with Zero Trust policies. Only users who match your policies can access your configured applications. [Applications documentation](#)

Your applications Showing 1-4 of 4

Manage the policies, authentication, and settings of your configured applications.

+ Add an application

Search by app name or URL

Show filters

When you click on Add an application

[← Back to Applications](#)


## Add an application

Configure the policies, authentication, and settings of your application.

What type of application are you adding?

Tip: Self-hosted applications are the most common.


You can now configure the "private network" app type by choosing self-hosted.



**Self-hosted**

Applications you have created or host in your own environment.


Select



**SaaS**

Applications you do not host, like Salesforce or Workday. Requires set up outside of Access.


Select



**Private network**

Non-HTTP applications you host that do not have public DNS records.


Select



**Infrastructure** NEW

Servers and resources in your infrastructure managed by a cloud provider or you.

Select



**Bookmark**

Add a URL to your App Launcher without adding Access policies.

Select

Select Self-Hosted, you will be redirected to:

[← Back to Applications](#)

## Add an application

Configure the policies, authentication, and settings of your application.

Select type > **Configure application** > Experience settings (optional) > Advanced settings (optional)

### Basic information

Configure your application's basic details and paths. Enter hostnames or IPs to protect an entire website or specific subdomains and paths.

Application name (Required)

Enter an application name

0 / 350

Session Duration (Required)

24 hours

+ Add public hostname + Add private hostname + Add private IP

### > Browser rendering settings

Cloudflare currently supports rendering a terminal for SSH, VNC, or RDP sessions in a user's browser.

### Access policies

Define who can access your applications. Add from your existing policies or create new ones.

**Note:** Access will evaluate policies with Bypass and Service Auth actions first. Then, policies are evaluated in top-to-bottom order. [Order of execution documentation](#) ↗.

Select existing policies + Create new policy

Order	Policy name	Action	Rules	Policy ID
-------	-------------	--------	-------	-----------

Fill in the information as requested:

[← Back to Applications](#)

## Add an application

Configure the policies, authentication, and settings of your application.

Select type > **Configure application** > Experience settings (optional) > Advanced settings (optional)

### Basic information

Configure your application's basic details and paths. Enter hostnames or IPs to protect an entire website or specific subdomains and paths.

Application name (Required)

kasmworkspace

13 / 350

Session Duration (Required)

24 hours

### Public hostname

Input method Subdomain

Default

space

Domain (Required)

lay.network

Path

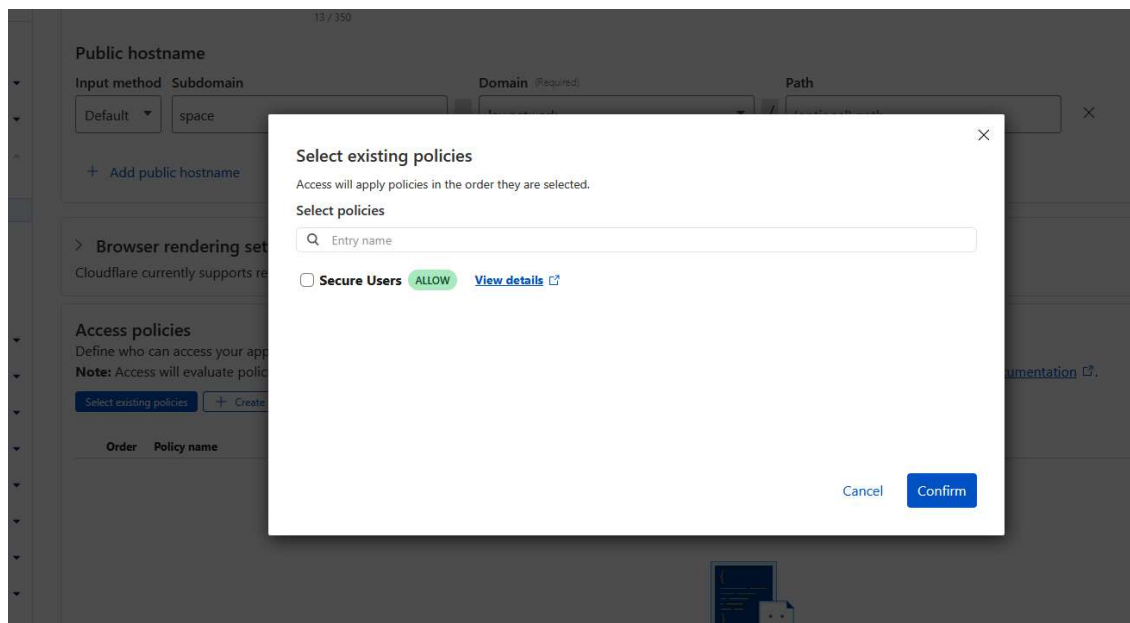
(optional) path

+ Add public hostname

+ Add private hostname

+ Add private IP

Scroll down to Access policies, and select existing policies, select the policy and hit confir



It will become:

Access policies				
Define who can access your applications. Add from your existing policies or create new ones.				
<b>Note:</b> Access will evaluate policies with Bypass and Service Auth actions first. Then, policies are evaluated in top-to-bottom order. <a href="#">Order of execution documentation</a>				
<a href="#">Select existing policies</a> <a href="#">+ Create new policy</a>				
Order	Policy name	Action	Rules	Policy ID
1	Secure Users	ALLOW	1	6cbed7d-424a-47dd-863f-91bce00846df

Scroll down to Login methods

Depending on how many options you have set, in this example, only One-time PIN is available.

Login methods

Select the identity providers your users can use to log in to this application. If you do not add an identity provider, a one time pin will be used by default.  
[Manage login methods.](#)

Accept all available identity providers

☒

Allow users to log in with any identity providers configured on your account, including ones added in the future.

Showing 1 - 1

Name

One-time PIN

1 - 1 | Items per page: 20

Instant Auth

☐

Allow users to skip identity provider selection when only one login method is available.

Search

Make sure to check the box, as shown below:

Login methods

Select the identity providers your users can use to log in to this application. If you do not add an identity provider, a one time pin will be used by default.  
[Manage login methods.](#)

Accept all available identity providers

☒

Allow users to log in with any identity providers configured on your account, including ones added in the future.

Showing 1 - 1

Name

One-time PIN

1 - 1 | Items per page: 20

Instant Auth

☒

Allow users to skip identity provider selection when only one login method is available.

Search

WARP authentication identity

Beta

Allow users to log in with their WARP/Gateway session identity. Users need to reauthenticate based on default session durations. WARP authentication identity must be turned on in your device enrollment permissions.  
[Manage default settings.](#)

Turn on WARP authentication identity

☒

Changes to this setting affect this application only.

Back

Cancel

Next

Click Next

You may customise the page and error messages otherwise, click Next

Custom pages

Manage the landing experiences of login pages, block pages, and the App Launcher.  
[View custom page settings](#)

Block page

Choose what will display to users if they fail to meet the criteria for identity or non-identity based policies.  
[Learn more about block pages](#)

Identity failure block page

☒ Cloudflare default

☐ Redirect URL

Cloudflare error text

Create a custom login page message for users who are denied access

Non-identity failure block page

☒ Cloudflare default

☐ Redirect URL

Back

CancelNext

## Under Advanced Settings (optional)

[← Back to Applications](#)

### Add an application

Configure the policies, authentication, and settings of your application.

Select type > Configure application > Experience settings (optional) > **Advanced settings (optional)**

#### > Cross-Origin Resource Sharing (CORS) settings

Manage settings that allow web applications running on one origin to reach selected resources in a different origin.

#### > Cookie settings

Configure enhanced cookie settings for added security. Access checks all requests for a valid cookie that contains the user's identity in the form of a JSON Web Token (JWT).

#### > 401 Response for Service Auth policies

Return a 401 status code in service authentication rules on failed requests.

Back

CancelSave

Leave it as default and click Save

Once done: it should look something like:

[Access](#) / [Applications](#)

## Applications

Protect your Self-Hosted, SaaS, and Private applications with Zero Trust policies. Only users who match your policies can access your configured applications. [Applications documentation](#)

### Your applications Showing 1-4 of 4

Manage the policies, authentication, and settings of your configured applications.

[+ Add an application](#)

[Show filters](#)

Application name	Application URL	Total domains	Policies assigned	Type
 kasim	space.lay.network	1	1	SELF-HOSTED

[← Back to Applications](#)

# kasm

Manage the policies, authentication, and settings of your configured applications.

[Configure](#)

[Basic information](#) [Policies](#) [Login methods](#) [Experience settings](#) [Advanced settings](#)

**Basic information**  
Configure your application's basic details and paths. Enter hostnames or IPs to protect an entire website or specific subdomains and paths.

Application name (Required)

Session Duration (Required)

kasm

24 hours

**Public hostname**

Input method

Domain

Default

space.lay.network

▼ **Browser rendering settings**

Cloudflare currently supports rendering a terminal for SSH, VNC, or RDP sessions in a user's browser.  
[Browser rendering documentation](#)

Allow automatic Cloudflared authentication OFF

**Browser rendering**  
Cloudflare will render an SSH terminal, VNC connection, or RDP session for this application in a web browser.  
Disabled

**Application Audience (AUD) Tag**  
Access assigns a unique AUD tag for each application. Copy the below value into a token validation script to check its signature against your public key.  
[Validate JWTs documentation](#)

19ce2f740fb6b61ef3464fca14d6afb79e568297700da80103523ed3875cee7

[Basic information](#) [Policies](#) [Login methods](#) [Experience settings](#) [Advanced settings](#)

**Access policies**  
Define who can access your applications. Add from your existing policies or create new ones.  
**Note:** Access will evaluate policies with Bypass and Service Auth actions first. Then, policies are evaluated in top-to-bottom order. [Order of execution documentation](#)

Order	Policy name	Action	Rules	Policy ID
1	personal-emails	ALLOW	1	876ba649-575d-4e02-a96f-dbe6fae2e2c2

▼ **Policy details**

> personal-emails ALLOW

**Policy tester**  
The policy tester evaluates the last seen identity of active users. Login decisions may differ if there are changes to user attributes evaluated by this policy. Save changes before [testing a single user](#).

[Test policies](#)

[Basic information](#) [Policies](#) [Login methods](#) [Experience settings](#) [Advanced settings](#)

**Login methods**  
Select the identity providers your users can use to log in to this application. If you do not add an identity provider, a one time pin will be used by default.  
[Manage login methods](#)

Accept all available identity providers OFF  
Allow users to log in with any identity providers configured on your account, including ones added in the future.

Showing 1 - 1

Search

Name	Status
One-time PIN	ON

1 - 1 | Items per page: 20

< 1 of 1 page >

Instant Auth OFF  
Allow users to skip identity provider selection when only one login method is available.

**WARP authentication identity** Beta  
Allow users to log in with their WARP/Gateway session identity. Users need to reauthenticate based on default session durations. WARP authentication identity must be turned on in your device enrollment permissions.  
[Manage default settings](#)

Turn on WARP authentication identity OFF  
Changes to this setting affect this application only.



#### Application Appearance

Customize how the application appears to your users in the App Launcher.

[Manage app launcher settings](#)

Show application in App Launcher ON

##### Application logo

This will appear in the App Launcher and the main Applications page.

- ☒ Default
- ☐ Use custom logo

##### Application domains

Select a domain to use as the App Launcher link. Note: The App Launcher will not display application domains that contain wildcards (\*).

- ☒ Default (first domain listed) space.lay.network
- ☐ Use custom domain:

#### Tags

Add tags to filter applications in the App Launcher. For best practice, we recommend a max of three tags per application. You can create up to 100 custom tags. Tags have a maximum of 35 characters.

[Manage tags](#)

Tags

#### Custom pages

Manage the landing experiences of login pages, block pages, and the App Launcher.

[View custom page settings](#)

##### Block page

Choose what will display to users if they fail to meet the criteria for identity or non-identity based policies.

[Learn more about block pages](#)

##### Identity failure block page

- ☒ Cloudflare default
- ☐ Redirect URL

##### Cloudflare error text

Create a custom login page message for users who are denied access

##### Non-identity failure block page

- ☒ Cloudflare default
- ☐ Redirect URL

#### Cross-Origin Resource Sharing (CORS) settings

Manage settings that allow web applications running on one origin to reach selected resources in a different origin.

[CORS settings documentation](#)

Bypass options requests to origin OFF

Send all options requests directly to the origin server.  
This will remove all existing CORS settings for this application.

Access-Control-Allow-Credentials OFF

##### Access-Control-Max-Age (seconds)

Maximum number of seconds the results can be cached.

##### Access-Control-Allow-Origin

- ☐ Allow all origins

##### Access-Control-Allow-Methods

- ☐ Allow all methods

##### Access-Control-Allow-Headers

- ☐ Allow all http headers

▼ **Cookie settings**

Configure enhanced cookie settings for added security. Access checks all requests for a valid cookie that contains the user's identity in the form of a JSON Web Token (JWT).

[Cookie settings documentation](#) 

**HTTP Only** ☐

Prevents any client-side scripts from accessing the cookie.

**Enable Binding Cookie** ☐

Protects against stolen authorization tokens. Do not use for non-HTTP applications that rely on protocols like SSH and RDP.

**Enforce cookie path attribute** ☐

Turn on to scope this application's JWT to the application path. If turned off, the JWT will scope to the hostname by default.

**Same Site Attribute**

Only sends the cookie if the cookie's defined site matches the site requested in the browser.

undefined

▼ **401 Response for Service Auth policies**

Return a 401 status code in service authentication rules on failed requests.

**Return 401 Response** ☐