

## ASM CLOUDFLARE INTEGRATION

The Mandiant Advantage Attack Surface Management (MA-ASM) Cloudflare integration is designed to pull all DNS Records from zones for which the Cloudflare API Token was authorized. The records pulled downstream are then created as Entities based on their respective type. For example, A/AAAA records will be created as IPAddress Entities and the associated name and label will be turned into DnsRecord Entities.

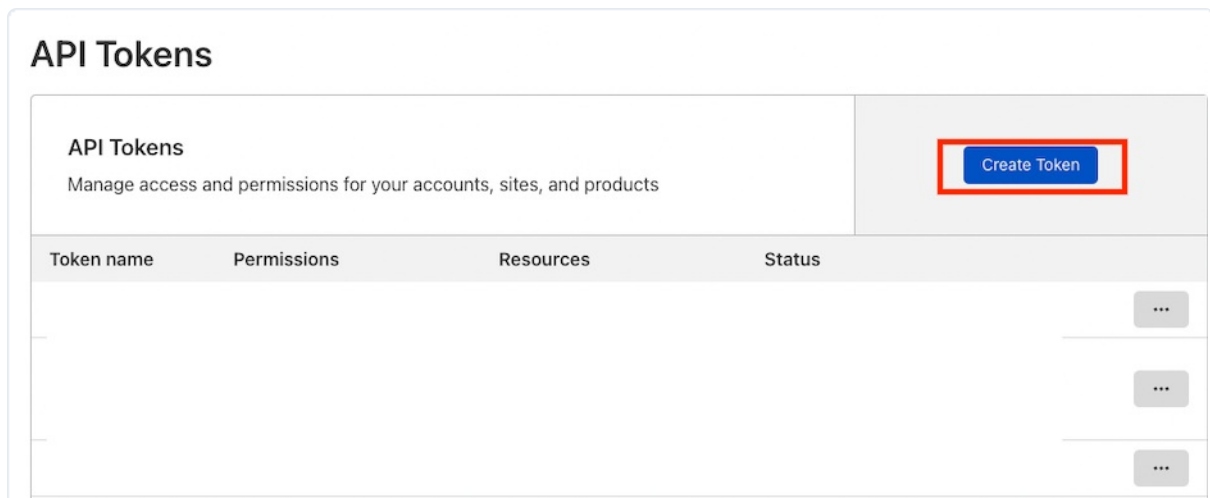
This increases the quality of **Seeds** (<https://docs.mandiant.com/home/asm-seeds>) in cases where the Cloudflare account is managing a substantial amount of records.

Adding this integration requires two steps:

1. **Create Cloudflare API Token**
2. **Provide Cloudflare API credentials for MA-ASM integration**

### Create Cloudflare API Token

1. Once authenticated on <https://cloudflare.com>, browse to <https://dash.cloudflare.com/profile/api-tokens> and click **Create Token**.



2. Within the **API Tokens** interface, click **Get Started** next to **Create Custom Token**.

## API Tokens

[← Back to view all tokens](#)

### Create API Token

Select a template to get started or create a custom token from scratch

#### API token templates

Get started with a few pre-configured permissions.

Edit zone DNS	<a href="#">Use template</a>
Read billing info	<a href="#">Use template</a>
Read analytics and logs	<a href="#">Use template</a>
Edit Cloudflare Workers	<a href="#">Use template</a>
Edit load balancing configuration	<a href="#">Use template</a>
WordPress	<a href="#">Use template</a>
Create Additional Tokens	<a href="#">Use template</a>
Read and write to Cloudflare Stream and Images	<a href="#">Use template</a>
Read all resources	<a href="#">Use template</a>

#### Custom token

Create a custom API token by configuring your permissions and token settings by hand.

<input type="text" value="Create Custom Token"/>	<a href="#">Get started</a>
--	-----------------------------

3. Within the **Create Custom Token** interface, populate the fields as defined here and click **Continue to summary**:
  - a. **Token name**: A friendly name that's easily remembered such as *Mandiant ASM Cloudflare Integration*
  - b. **Permissions**:
    - i. Zone - Zone - Read
    - ii. Zone - DNS - Read
  - c. **Zone Resources**: Include - All zones



Cloudflare provides the flexibility to allow the API Token to access all zones, a specific zone, or exclude specific zones. Typically most organizations would select **All Zones**, however adjust this option to fit your organization's requirements.

d. **Client IP Address Filtering**: Leave blank

e. **TTL**: Leave blank

## API Tokens

[← Back to view all tokens](#)

### Create Custom Token

Token name  
Give your API token a descriptive name.

Permissions  
Select edit or read permissions to apply to your accounts or websites for this token.

Zone	Zone	Read	×
Zone	DNS	Read	×

[+ Add more](#)

**Zone Resources**  
Select zones to include or exclude.

Include	All zones
---------	-----------

[+ Add more](#)

Client IP Address Filtering  
Select IP addresses or ranges of IP addresses to filter. This filter limits the client IP addresses that can use the API token with Cloudflare. By default, this token will apply to all addresses.

Operator	Value
Select item...	e.g. 192.168.1.88

[+ Add more](#)

TTL  
Define how long this token will stay active.

Start Date	→	End Date
------------	---	----------

[Cancel](#) [Continue to summary](#)

4. Review and click **Create Token**.

## API Tokens

[← Edit token](#)

**Mandiant ASM Cloudflare Integration API token summary**

This API token will affect the below accounts and zones, along with their respective permissions

└─ All zones - **Zone:Read, DNS:Read**

---

- Copy this token to be used when **providing credentials to MA-ASM**.



For security reasons, these credentials will only be shown once. Please copy and store in a secure location.

## API Tokens

**Mandiant ASM Cloudflare Integration API token was successfully created**


Copy this token to access the Cloudflare API. For security this will not be shown again. [learn more](#)

cloudflare\_api\_token\_will\_be\_shown\_here

### Provide Cloudflare Credentials for MA-ASM Integration

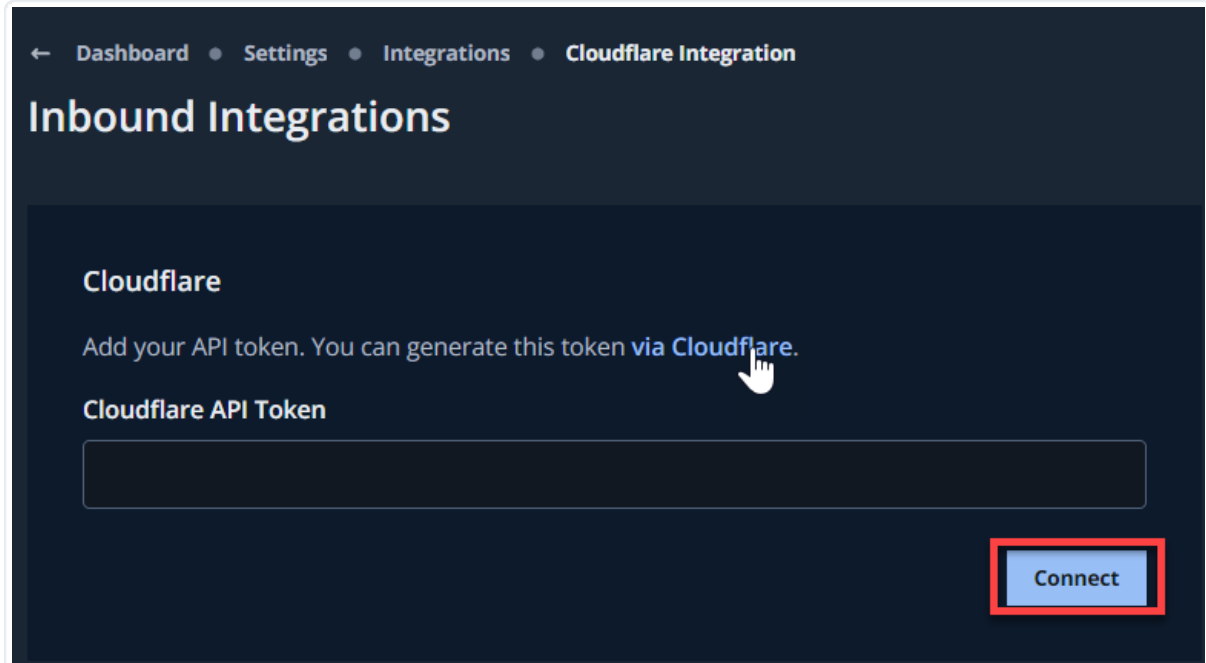
Add your Cloudflare API Token into the integration page and then on the Collection, choose which Collection you would like to pull the entities into.


- From the **Projects and Settings** menu in MA-ASM, select the appropriate Project then click **Account Settings**.
- Click **Integrations**.
- Under **Inbound Integrations**, click **Add New** for Cloudflare.

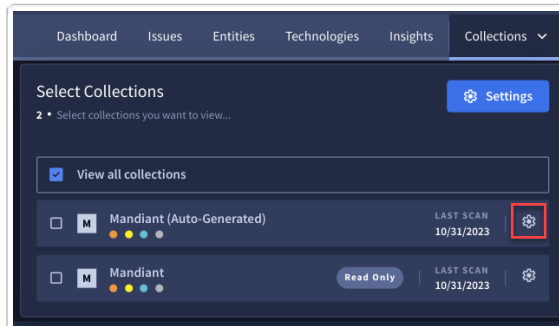


**Cloudflare**  
Increase visibility on your DNS records.

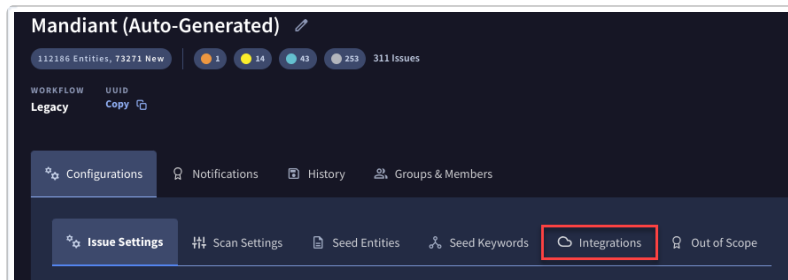
- Paste the token value from the **Create Cloudflare API Token** process outlined above into the **Cloudflare API Token** field and click **Connect**.



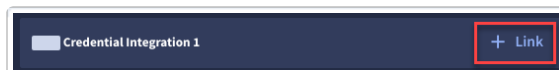
5. Connect the integration to the appropriate Collection.
  - a. Click **Collections** and click  **Collection Settings** for the Collection that you want to connect the integration to.



- b. Select the **Integrations** tab.



- c. Select **Connect Integration** and **Link** the integration.




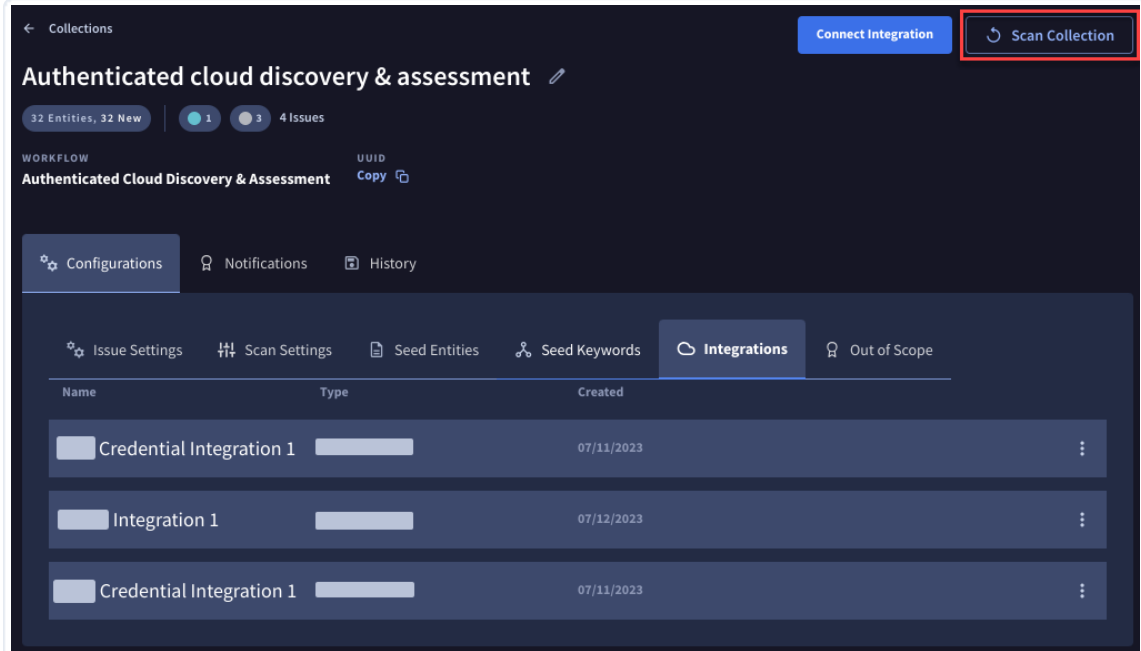
The integration is immediately added to the Collection.

Click  to remove the integration from this Collection.



**Credential Integration 1** Linked 

- d. Click  to close the **Connect Integration** pane. Click **Scan Collection** to update your Collection with the current settings and integrations. Otherwise, your newly configured integration is incorporated at your regularly scheduled scan interval.



← Collections Connect Integration Scan Collection

### Authenticated cloud discovery & assessment

32 Entities, 32 New | 1 | 3 | 4 Issues

WORKFLOW Authenticating Cloud Discovery & Assessment UID Copy

Configurations | Notifications | History

Issue Settings | Scan Settings | Seed Entities | Seed Keywords | **Integrations** | Out of Scope

Name	Type	Created	
Credential Integration 1		07/11/2023	⋮
Integration 1		07/12/2023	⋮
Credential Integration 1		07/11/2023	⋮