CREATE A COLLECTION

Collection configuration is available for paid Attack Surface Management customers.
If you would like to upgrade to a more feature-rich account, send a message using our contact form, **https://www.mandiant.com/contact-us**.

A Scan Workflow in Mandiant Advantage Attack Surface Management (MA-ASM) is a predefined set of tasks that are applied to a Collection. When you create a new Collection, you're required to select a Workflow. Various Scan Workflow templates are provided to guide you toward the setup that best suits your needs. Depending on the template you select, you're prompted to supply Seeds and integrations relevant to that selection. Once a Collection is created, the name of the Workflow associated with the Collection is available on the Collection Settings page.

- Collections created before the availability of Workflows are linked to Legacy Workflows.
- Once a Collection is created, the Workflow cannot be changed.

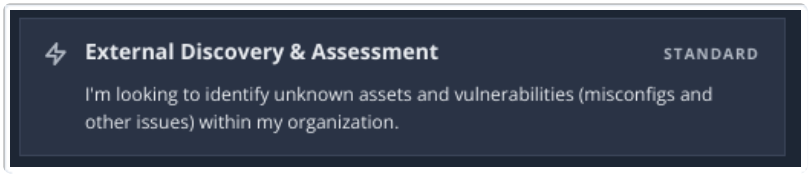
Scan Workflow templates

The following predefined Scan Workflows are available to aid in Collection customization.

- Integrations for the **External Discovery & Assessment** Workflow only retrieve DNS zones from cloud or DNS providers.
- Integrations for **Authenticated Cloud Discovery & Assessment** Workflow retrieve the full range of discoverable asset types from each respective cloud provider.
- Each Workflow accepts specific integrations and Seed types. For more information, see the **Workflow Seeds table**.

- External Discovery & Assessment (Standard)

  Identify shadow IT or unknown assets and vulnerabilities.



  Cloud integrations linked to this Workflow only pull in DNS records. Also, when you link to cloud integrations using this Workflow, an extra Collection is created for every linked cloud integration using the **Authenticated Cloud Discovery & Assessment** Workflow. Supported cloud integrations include:
  - **AWS (https://docs.mandiant.com/home/asm-aws-integration)**
  - **Azure (https://docs.mandiant.com/home/asm-azure-integration)**
  - **Google Cloud (https://docs.mandiant.com/home/asm-gcp-integration)**

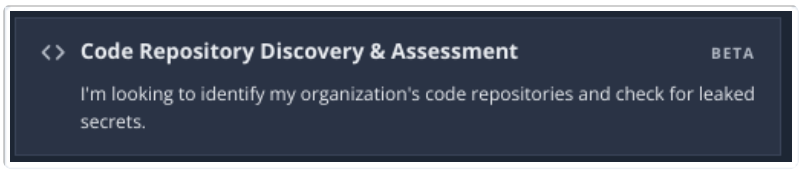
- Authenticated Cloud Discovery & Assessment

  Identify vulnerabilities across your cloud providers.

Cloud integrations linked to this Workflow pull in applicable cloud assets, such as Storage Buckets and Virtual Machine instances, in addition to DNS records.

- Code Repository Discovery & Assessment (Beta)

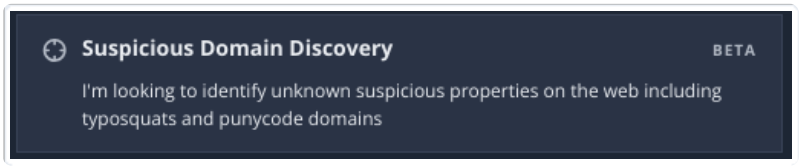
  Identify your company's known accounts for secrets and discover unknown rogue repositories.



This Workflow is used with GitHub. GitHub can be linked through **integration (https://docs.mandiant.com/home/asm-github-integration)**, or by Seed: `GithubAccount` or `GithubRepository`.

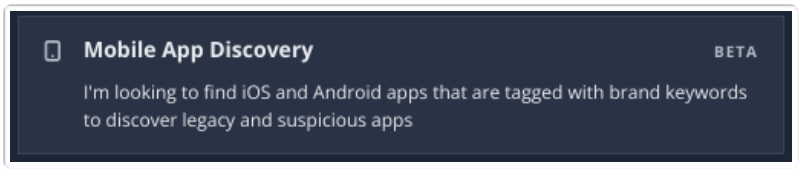
- Suspicious Domain Discovery (Beta)

  Identify unknown suspicious properties on the web including typosquats and punycode domains.



- Mobile App Discovery (Beta)

  Identify Android and iOS Apps tagged with your organization's brand keywords hosted in commonly used application marketplaces.



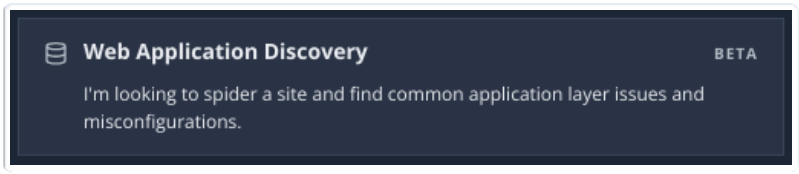
- Web Application Discovery (Beta)

  Identify web application endpoints derived from URLs.

This discovery method uses a recursive search feature for identifying additional assets. This recursive search works as follows:

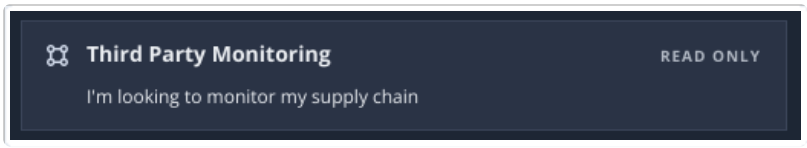
1. Fetch the base URL and the scan responses for additional URLs.
2. Log all returned URLs in the Entity details for the base URL.
3. Fetch and scan all returned URLs for additional URLs and log new URLs in the Entity details.

This recursive process continues until no additional new URLs are found, or until a predefined timeout duration is reached.



- Third Party Monitoring (Read Only)

  Monitor your supply chain. For more information, see **Third Party Monitoring Workflow (https://docs.mandiant.com/home/asm-third-party-monitoring-workflow)**.



Two additional Scan Workflows may be observed, but are not available for selection:

- **Legacy**: This Workflow applies to all Collections that existed before Scan Workflows were introduced to the collection creation process.
- **Freemium Discovery**: This Workflow applies to all Freemium Collections.

Create a Collection using a Scan Workflow

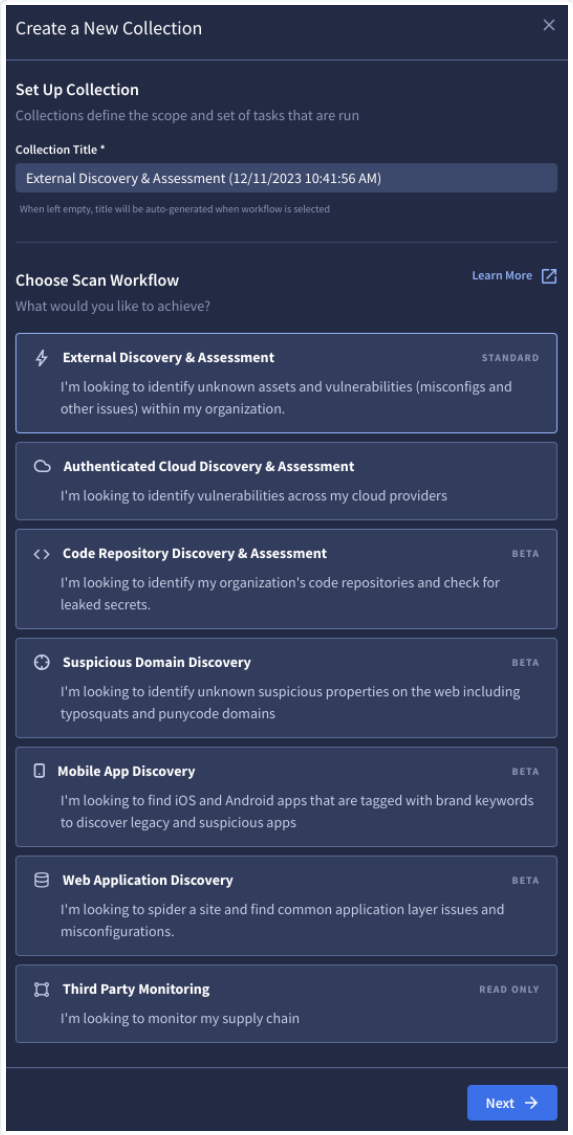
1. In MA-ASM, select **Settings** from the **Collections** menu.
2. Click **+ Create New Collection**.

   The **Third Party Monitoring** Workflow follows a different set of steps. For more information, see the "Create a Collection for Third Party Monitoring" section of **Third Party Monitoring Workflow (https://docs.mandiant.com/home/asm-third-party-monitoring-workflow)**.

3. Enter a title for your Collection and choose the **Scan Workflow** that best suits your needs for this particular task.

   If you do not title a new Collection, a title is auto-generated.

4. Click **Next**.



New Collection Title and Scan Workflow configuration

5. **Add Seeds**, as necessary. Enter a **Seed (https://docs.mandiant.com/home/asm-seeds)** and select the **Seed Type** from the drop-down. You can add multiple Seeds using **+ Add Another**.

> Accepted Seed types are specific to the Scan Workflow that you have selected. For more information, see the **Workflow Seeds table**.

- Seeds can be uploaded from a CSV file. Download our **CSV Seed** (https://asm.advantage.mandiant.com/docs/exports-seed-csv-example.csv) template or create your own CSV file with two columns. The first row must have `TYPE,NAME` and each subsequent row must have a comma-separated type-name pair. For example:

```
TYPE,NAME
Domain,intrigue.io
Domain,mandiant.com
```

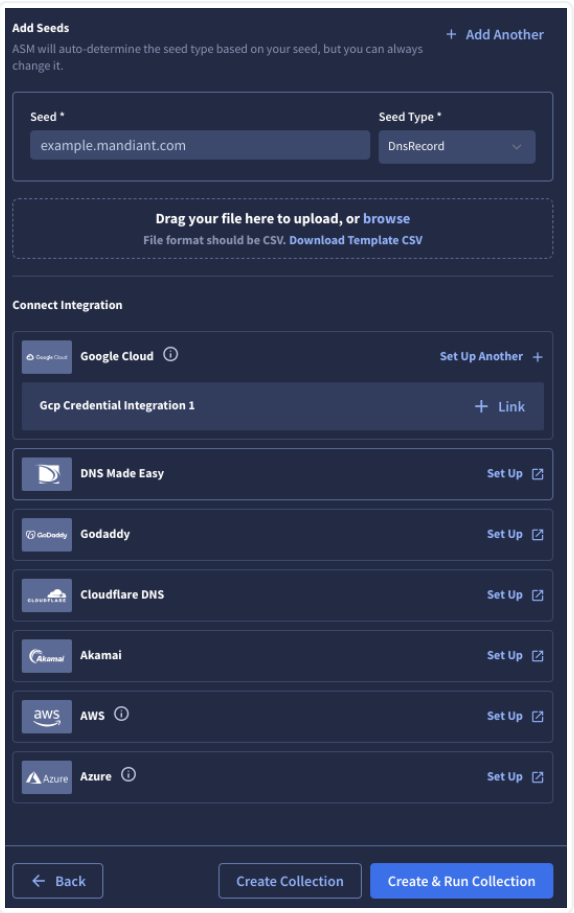
- Capitalization matters when uploading a CSV file of Seeds.

6. **Connect Integration**, if appropriate.

If integrations have already been added to the current project, they are available using **Link**. Otherwise, you can add an integration using **Set Up Another** or **Set Up**.

7. Click **Create Collection** to save without starting a scan right away or click **Create & Run Collection** to initiate the first scan for this new Collection.

- Collection scans run for a maximum of 72 hours.
- If you choose **Create Collection**, you're directed to the **Collection Settings** (https://docs.mandiant.com/home/asm-customize-collections) for this Collection where you can configure Collection settings before the first scan. In specific, you may choose to disable specific Issue types before scanning begins.
- The **Create & Run Collection** option is not available for the **Third Party Monitoring** Workflow.



New Collection Seed and Integration configuration

Workflow Seeds

The following table outlines which integrations and Seeds are accepted by each Workflow.

Workflow → / Seed ↓	External Discovery & Assessment (Standard)	Authenticated Cloud Discovery & Assessment	Code Repository Discovery & Assessment (Beta)	Suspicious Domain Discovery (Beta)	Mobile App Discovery (Beta)	Web Application Discovery (Beta)	Third Part Monitorin (Read Only)
Integrations available to be added	All Cloud and DNS Integrations	All Cloud Integrations	GitHub Integration Only	None	None	None	None
DnsRecord	✔						
Domain	✔			✔			
IpAddress	✔						
NetBlock	✔						
Uri	✔					✔	
Nameserver	✔						

Workflow → / Seed ↓	External Discovery & Assessment (Standard)	Authenticated Cloud Discovery & Assessment	Code Repository Discovery & Assessment (Beta)	Suspicious Domain Discovery (Beta)	Mobile App Discovery (Beta)	Web Application Discovery (Beta)	Third Part Monitorin (Read Only)
UniqueKeyword	✔		✔		✔		
GithubAccount			✔				
GithubRepository			✔				

The **Legacy** Workflow supports all **inbound integrations** (https://docs.mandiant.com/home/asm-inbound-integrations) and all the Seeds listed in this table as well as `ApiEndpoint`, `UniqueToken`, `AwsS3Bucket`, `EmailAddress`, and `AutonomousSystem`.

Modify an existing Collection

1. In MA-ASM, navigate to your Collections by selecting **Settings** from the **Collections** menu.
2. Select **Settings** for the Collection that you want to modify.
3. Modify the Collection as necessary.