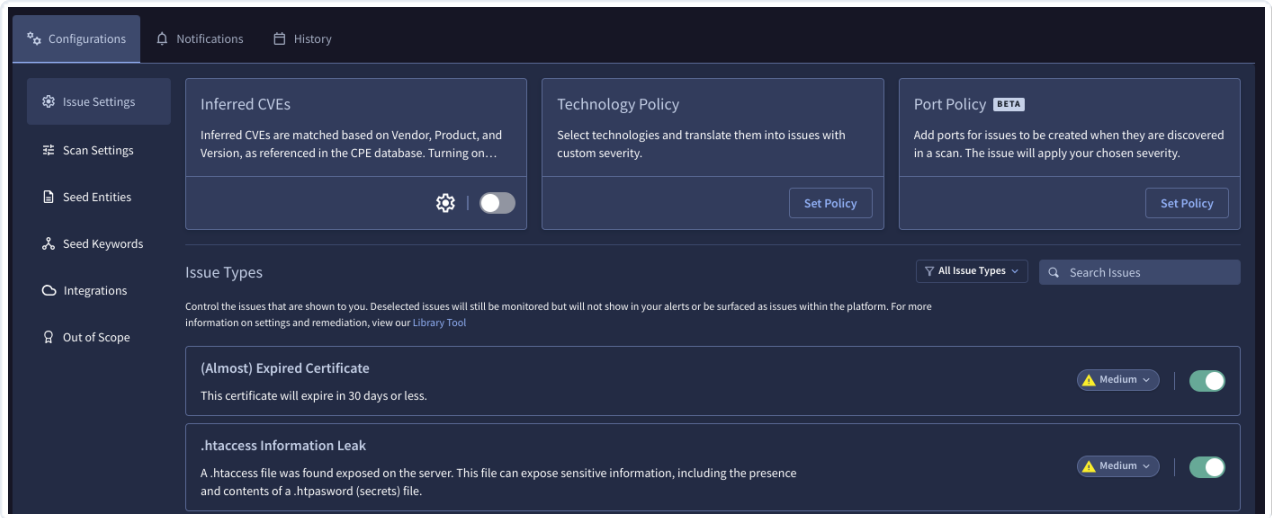
ISSUE SETTINGS

In Mandiant Advantage Attack Surface Management (MA-ASM), you decide what Issues you see for each Collection that you create. There are a variety of settings that you can establish and modify to curate the Issues exposed to you for each of your Collections.

Access the **Collections Settings** (https://docs.mandiant.com/home/asm-customize-collections) for an existing Collection to customize any of the following **Issue Settings**:

- **Inferred CVEs**
- **Technologies**
- **Ports**
- **Issue Types**

> You can modify **Issue Settings** before a Collection is scanned for the first time. To do so, when you **create a Collection** (https://docs.mandiant.com/home/asm-create-a-collection#create), click **Create Collection**, rather than **Create & Run Collection**, to be directed to the **Issue Settings** for the new Collection.



Issue Settings for a Collection

Inferred CVEs

You can employ Inferred CVE data to create Issues. For more information, see **ASM Mandiant Advantage Threat Intelligence Integration** (https://docs.mandiant.com/home/asm-mati-integration).

> - Updates to these settings require a Collection refresh. For an immediate refresh, click **Scan Collection**.
> - If you choose to turn off this setting, no additional Issues are automatically created from Inferred CVEs. Issues remain that have already been created from Inferred CVEs.

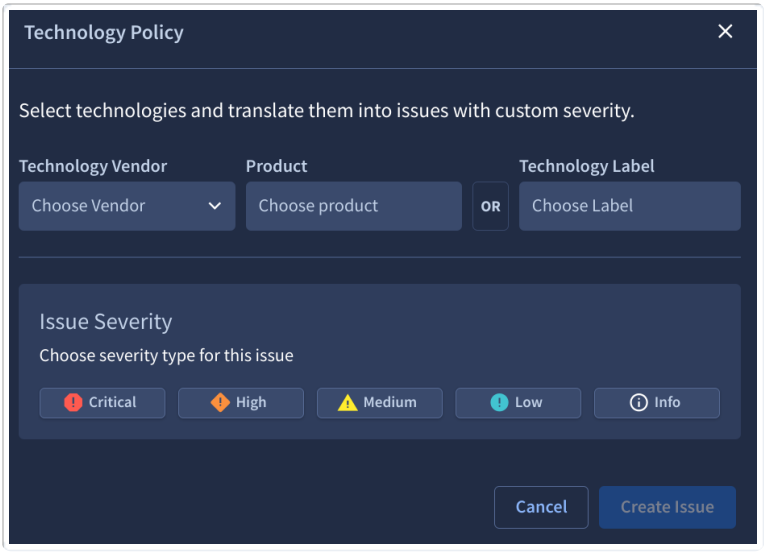
Technology Policy

You can select technologies to be translated into Issues. When the technology you define is identified in a scan, an Issue is

created with the severity that you have selected.

To establish a Technology Policy:

1. Navigate to the **Collections Settings** (https://docs.mandiant.com/home/asm-customize-collections) for one of your existing Collections.
2. Click **Set Policy** on the **Technology Policy** tile.
3. Select a **Technology Vendor**.
4. Select a **Product** or a **Technology Label**.
5. Choose a **severity** (https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples) for Issues created as a result of this new policy.
6. Click **Create Issue**.



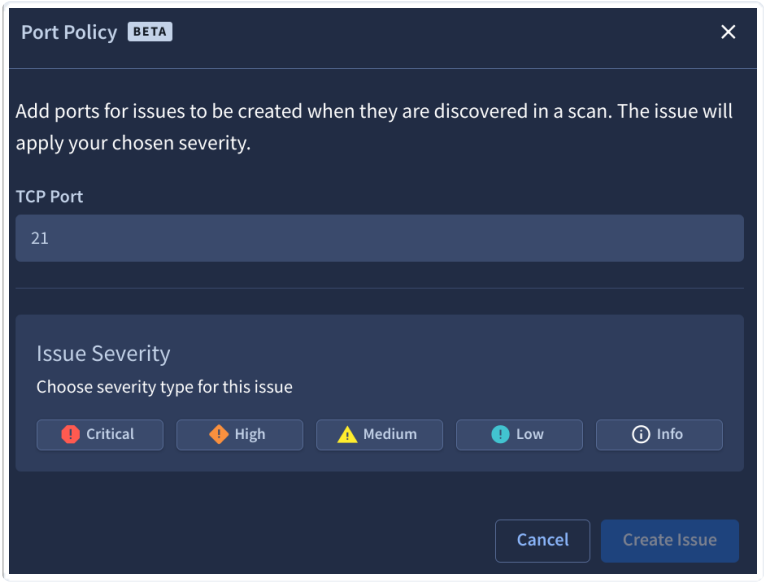
Technology Policy settings

Port Policy (Beta)

You can add ports to create Issues. When the port you define is discovered in a scan, an Issue is created with the severity that you have selected.

To establish a Port Policy:

1. Navigate to the **Collections Settings** (https://docs.mandiant.com/home/asm-customize-collections) for one of your existing Collections.
2. Click **Set Policy** on the **Port Policy** tile.
3. Enter a **TCP Port**.
4. Choose a **severity** (https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples) for Issues created as a result of this new policy.
5. Click **Create Issue**.



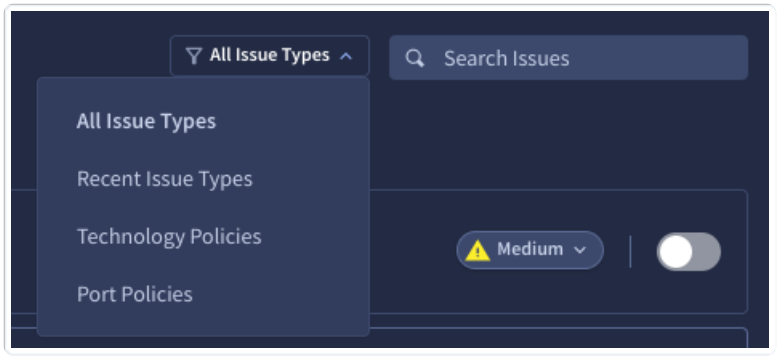
Port Policy settings

Issue Types

You can disable Issue Types so that they are not shown for a Collection. Toggle off any Issue Types you do not want to see. You can also adjust the **severity** (https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples) for each Issue Type to suit your needs.

The (Almost) Expired Certificate Issue Type toggled off

To help you easily identify specific Issue Types, you can filter or search. The Issue Types filter options include **All Issue Types**, **Recent Issue Types**, **Technology Policies**, and **Port Policies**.



Filter and Search options for Issue Types

- Updates to these settings require a Collection refresh. For an immediate refresh, click **Scan Collection**.
- Active checks are not run for disabled Issues.