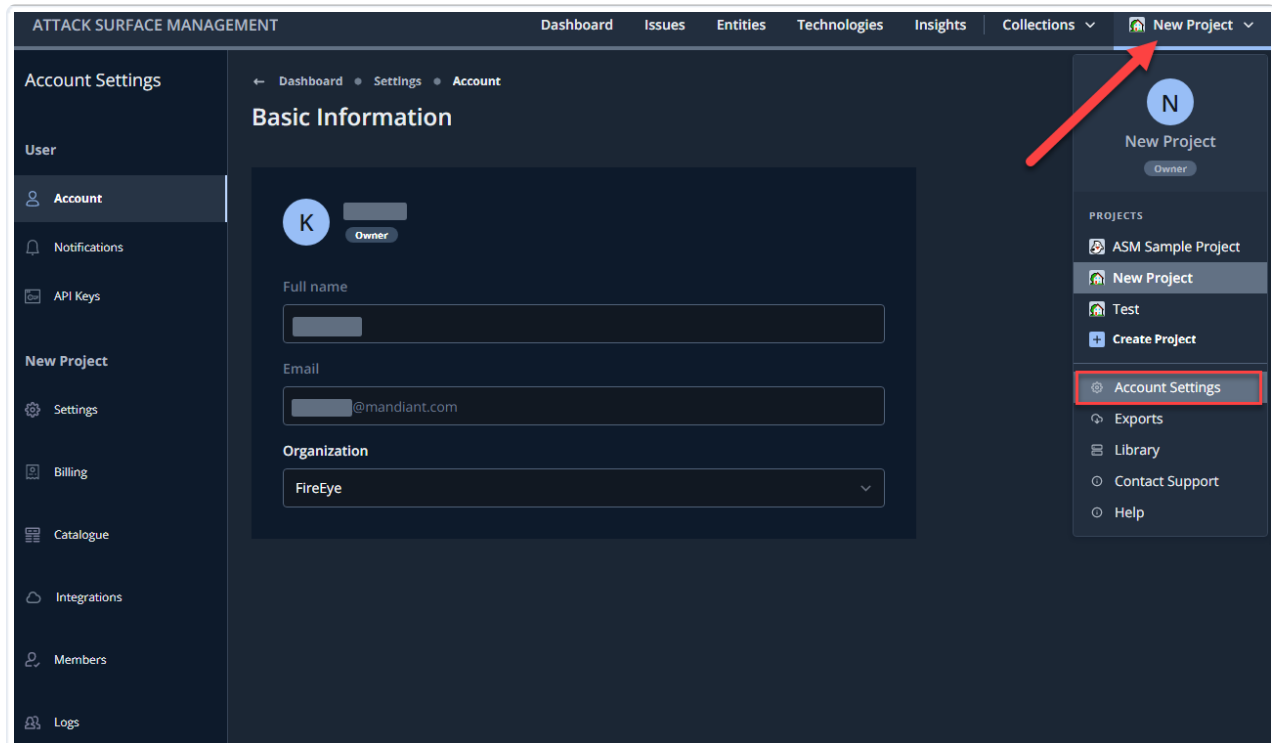


ACCOUNT SETTINGS OVERVIEW

Mandiant Advantage Attack Surface Management (MA-ASM) **Account Settings** include both user- and project-specific settings. This is where you can generate API keys, add integrations, and manage project membership.

Account Settings are available under the **Projects and Settings** menu in MA-ASM.



The following **Account Settings** are available:

User

- **Account**
- **Notifications**
- **API Keys**

Project

- **Settings**
- **Billing**
- **Integrations**
- **Members**
- **Logs**



The availability of each setting depends on your role (owner or member) within the selected project. If a setting is only available to project owners, that is called out for you.

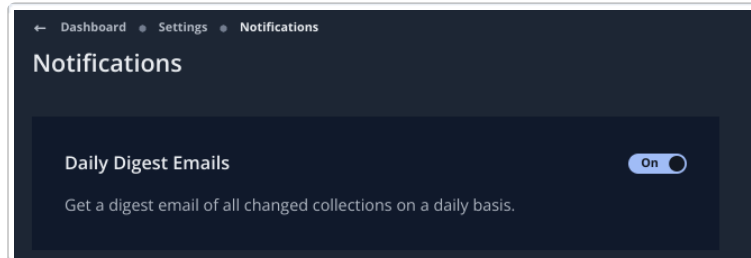
Account

This category shows **Basic Information** associated with your account including role (**Owner** or **Member**), **Full name**, **Email**, and **Organization**. For more information on switching organizations, see [ASM Organization Switcher](#)

(<https://docs.mandiant.com/home/asm-organization-switcher>).

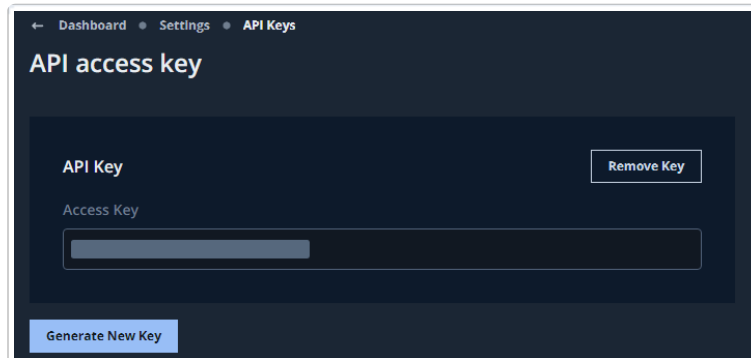
Notifications

This setting allows you to toggle **Daily Digest Emails** on or off. These emails serve as a digest of new results found in your collections.



API Keys

Application programming interface (API) keys are unique identifiers used to authenticate to the MA-ASM API. An **API access key** is required when linking integrations. For more information on using the API, see [Attack Surface Management API](#) (<https://docs.mandiant.com/home/asm-api-redirect>).

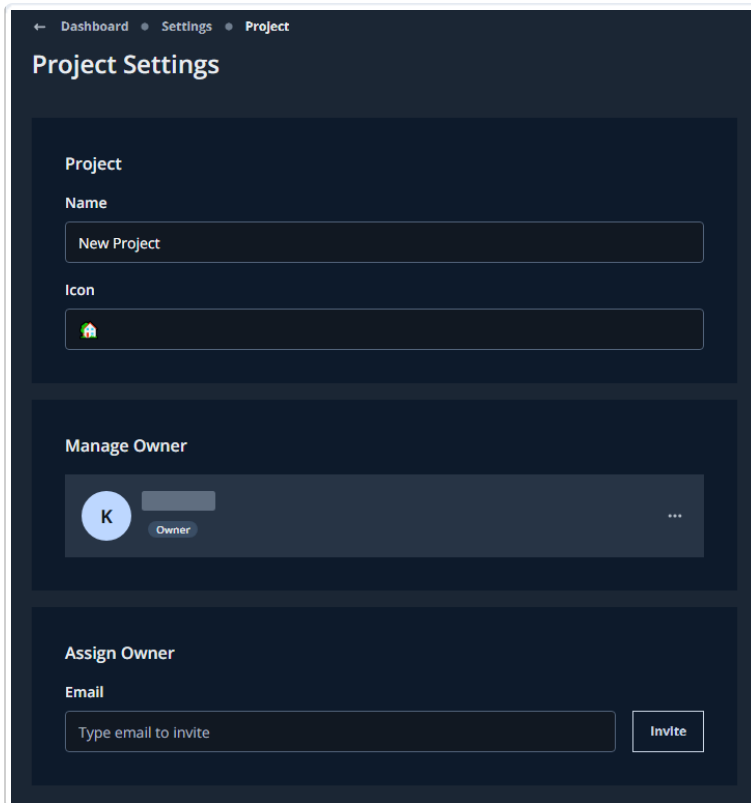


Settings



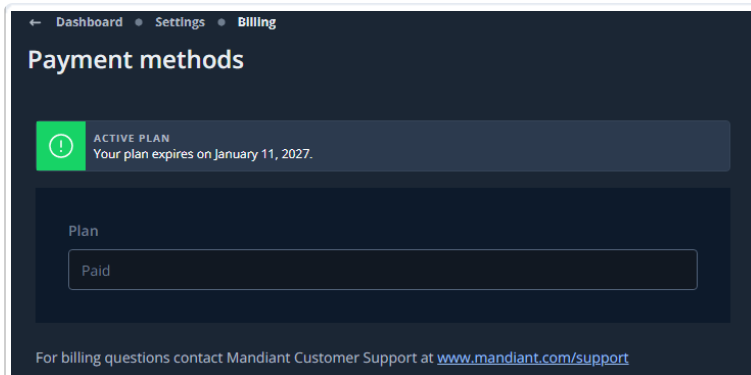
You must be the project owner to view and modify **Settings**.

These **Project Settings** allow you to edit the project **Name** and **Icon**, as well as manage project owners.



Billing

This setting gives you information about your **plan version** (<https://docs.mandiant.com/home/asm-versions>), including the status of your plan and the expiration date.

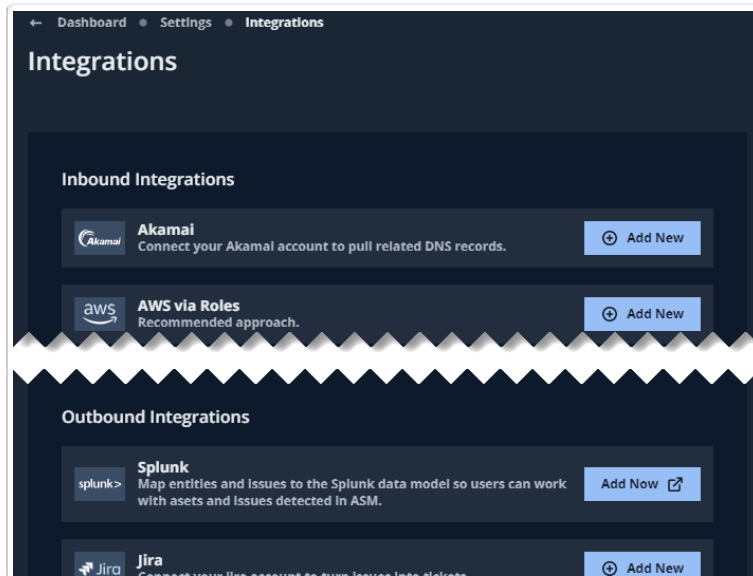


Integrations




You must be the project owner to view and modify **Integrations**.

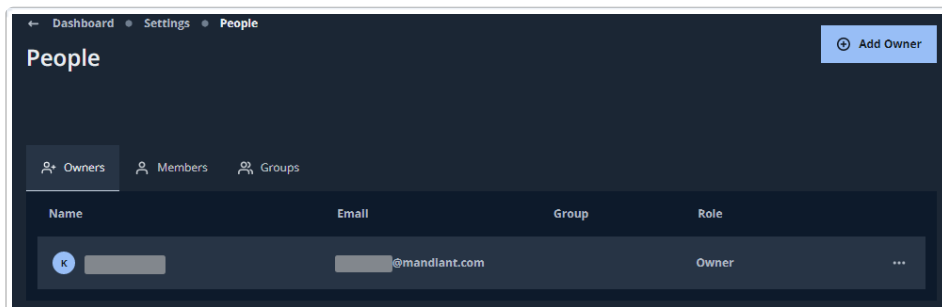
Here, you can manage various inbound and outbound **Integrations**. For more information about configuring specific integrations, see **Integrations** (<https://docs.mandiant.com/home/asm-integrations>).




Members


 You must be the project owner to view and modify **Members**.

This setting allows you to manage project members, including owners and groups of members. For more information, see [Manage Project Membership \(https://docs.mandiant.com/home/asm-project-membership\)](https://docs.mandiant.com/home/asm-project-membership).



Logs

 You must be the project owner to view **Logs**.

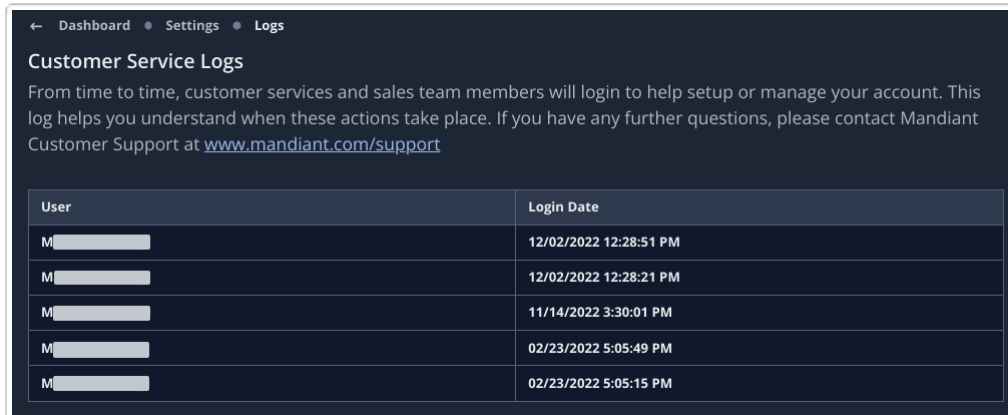
 This may also be referred to as an impersonation log.

Mandiant employees may access customer environments in an effort to provide support. Some scenarios when impersonation by Mandiant employees may prove beneficial include:

- To assist with collection configuration
- To view entities or issues specific to your environment
- To monitor ongoing support issues

Customer Service Logs are maintained so that you know when these impersonations take place. The **User** column provides the name of the user that was impersonated by a Mandiant employee, while the **Login Date** column identifies

the time and date of the impersonation.



The screenshot shows a web interface with a dark theme. At the top, there is a navigation bar with a back arrow and three items: 'Dashboard', 'Settings', and 'Logs'. Below this is the title 'Customer Service Logs' and a paragraph of text explaining the log's purpose and providing a support link. A table with two columns, 'User' and 'Login Date', contains five rows of data. The 'User' column contains redacted names, and the 'Login Date' column contains specific timestamps.

User	Login Date
M [REDACTED]	12/02/2022 12:28:51 PM
M [REDACTED]	12/02/2022 12:28:21 PM
M [REDACTED]	11/14/2022 3:30:01 PM
M [REDACTED]	02/23/2022 5:05:49 PM
M [REDACTED]	02/23/2022 5:05:15 PM