CONFIGURE ORGANIZATION SETTINGS

During your Mandiant Threat Defense onboarding process, the Mandiant Support team will set up the account of your organization and establish all user accounts and access privileges. The profile page of your organization contains information about the Mandiant Threat Defense **Subscription** plan of your organization, subscription **Expiration** date, and **Partner** information.

If you're a Team Administrator, you can view, edit, and manage the subscription details of your organization using the **Settings** menu option of your Managed Defense (MD) Portal. This option includes:

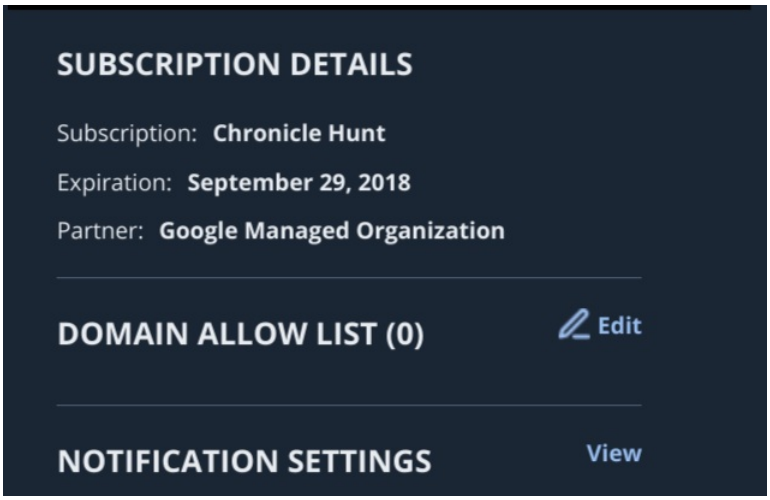
- Modifying basic Organizational information.
- Restricting access to your account using the **Domain Allow List**.
- Setting up **notifications** **(https://docs.mandiant.com/home/mh-manage-notification-settings#manage-organization-notification-settings)** for team members across the organization.

> If you have administrator privileges, you can view and edit the profile page of your organization. Administrators can also edit account settings for users in their organization.

Modify Your Organization Settings

The **Settings** menu of the MD Portal lets you modify the profile settings of your organization provided you're assigned as a Team Administrator.

> If your Mandiant Threat Defense account has multiple organizations, you need to access each organization separately in order to view and manage the respective settings.



Organization Settings

Settings	Description
Subscription	Your Mandiant Threat Defense subscription name.
Expiration	Your Mandiant Threat Defense subscription expiration date.
Partner	Partner name.

Settings	Description
Domain Allow List	Team members within your organization are only granted access to the Mandiant Threat Defense account if they have an allowed email domain assigned.
Notification Settings	Settings for notification across the organization.

Modify your Organization settings

1. In the MD Portal, select **Settings > Organization**.
2. Add allowed domains after selecting the **Domain Allow List** edit.
3. View and manage **Notification Settings (https://docs.mandiant.com/home/mh-manage-notification-settings)** after selecting **View**.

Email Domain Allow List

If your organization is one with multiple subsidiaries, divisions, or brands operating within a parent company, you can restrict user access to your Mandiant Threat Defense service by using an email **Domain Allow List**. An allow list grants user access to team members with an assigned email domain only. For example, suppose that *ABC Construction* is a division of *ABC Holdings*, which is also the parent company to five other organizations. As a network security administrator for *ABC Construction*, you want to restrict access to employees of *ABC Construction* only. An email **Domain Allow List** lets you enter the *abcconstruction.com* email domain and restrict Mandiant Threat Defense access to users with that email domain only. Employees who have an email domain of *abcholdings.com* would not have access to the Mandiant Threat Defense account of your organization.

If your **Domain Allow List** setting is empty, users with any domain name are allowed to be associated with your organization.