CONFIGURING ORGANIZATION SETTINGS

During your Managed Defense (MD) onboarding process, the Mandiant Support team will set up your organization's account and establish all user accounts and access privileges. Your organization's profile page contains information about your organization's MD service, including your MD Consultant's (MDC) contact information, MD subscription plan information, and subscription expiration date.

If you are assigned the Team Admin view, you can view, edit and manage your organization's information using your MD Portal's Settings. This includes:

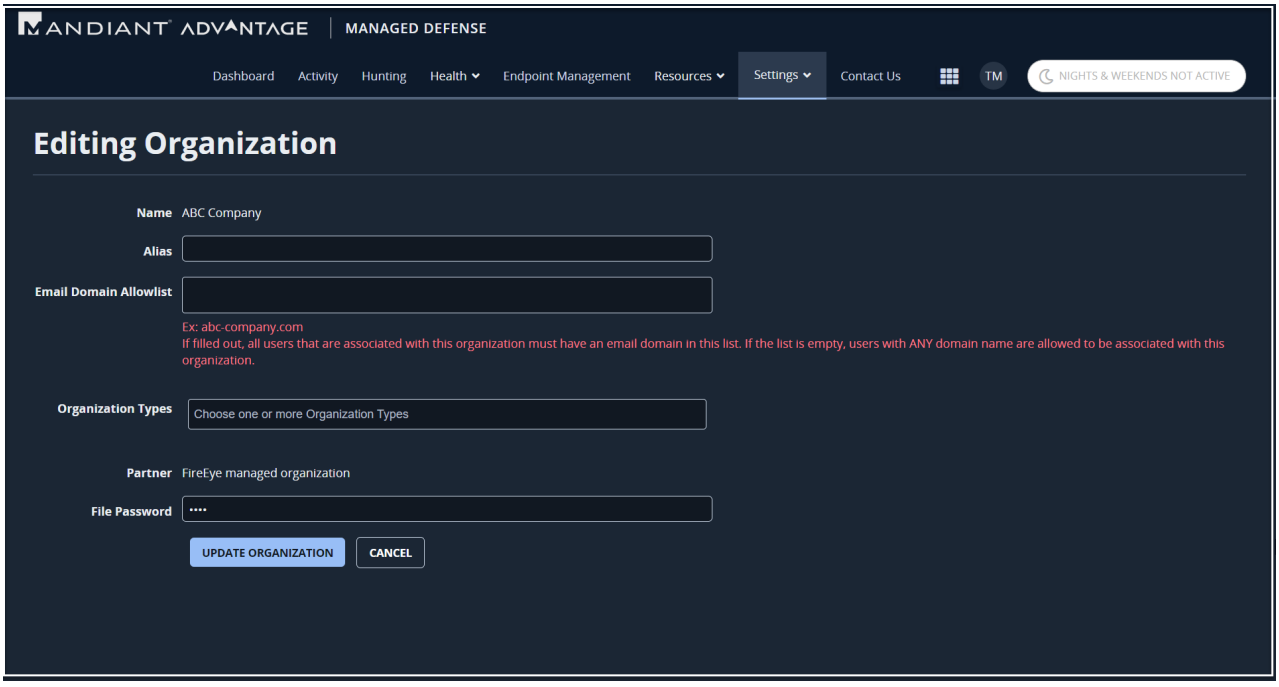
- Modify basic Organizational information
- Restricting access to your account using an **Email Domain Allow list**
- Configuring Notifications

NOTE: Only users with admin privileges can view and edit your organization's profile page. Admins can also edit account settings for users in their organization.

Modifying Your Organization's Settings

The MD Portal's **Settings** menu allows users assigned as a Team Administrator to modify their organization's profile settings.

NOTE: If your MD account has multiple organizations, you need to access each organization separately in order to view and manage the settings.



Setting	Description
Organization **Alias**	An alternative name for your organization that is commonly known and used by the employees.
Email Domain Allow list	Grants team members within your organization user access to your organization's MD account only if they have an assigned email domain.
File Password	Externally saves and secures PDF copies of the compromise reports. The default password is **openpdf**. **NOTE:** Only MD Portal admins have access to change the file password.

TO MODIFY YOUR ORGANIZATION'S SETTINGS:

1. In the MD Portal, click **Settings** and select **Organization**.
2. Click the **Gear Icon** on the top right then click the **Edit Organization** menu.
3. Enter your organization's alternative name in the **Alias** field.
4. Enter an email domain in the **Email Domain Allowlist** field.
5. Enter a new password in the **File Password** field.
6. Click **UPDATE ORGANIZATION**.

Email Domain Allow list

If your organization is one with multiple subsidiaries, divisions, or brands operating under a parent company, you can restrict user access to your MD 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, let's say 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 allows you to enter the *abcconstruction.com* email domain and restrict MD access to users with that email domain only. Employees who have an email domain of *abcholdings.com* would not have access to your organization's MD account.

NOTE: If your Allow-list setting is empty, users with any domain name are allowed to be associated with your organization.

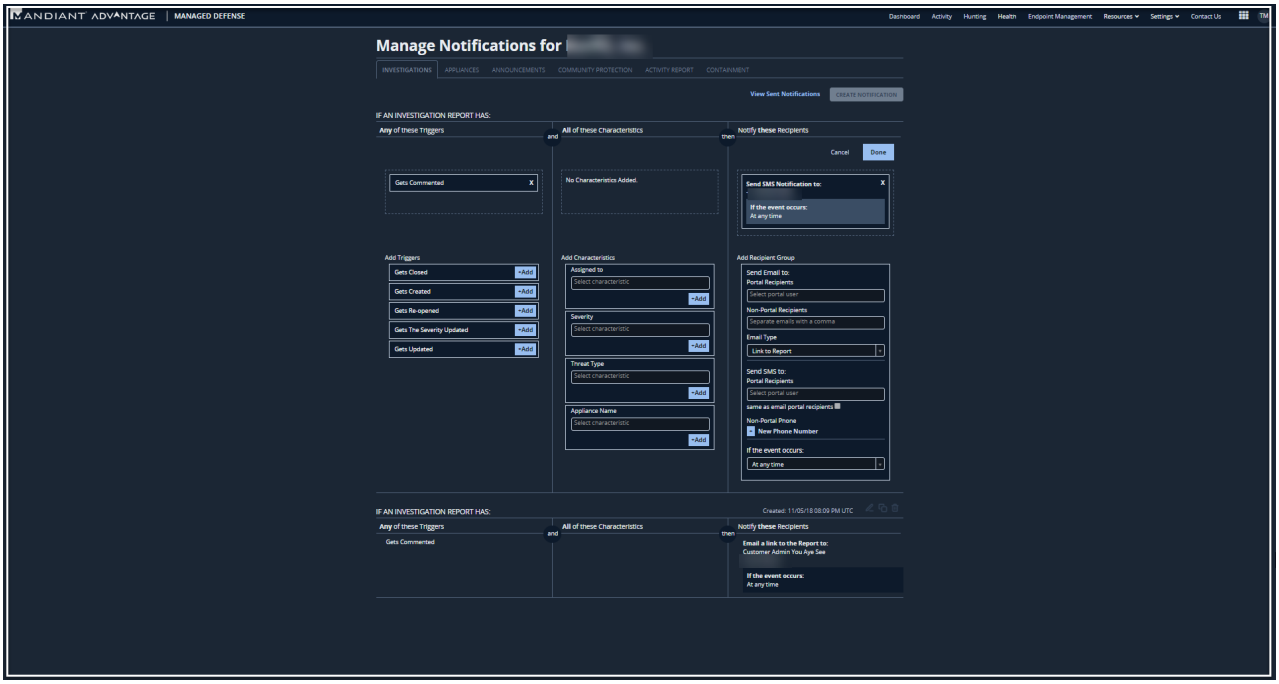
Configuring Organization Notifications

The MD Portal's notifications feature allows users in your organization to receive important communications about Investigation events, Appliance events, Announcement events, Community Protection events, Activity Report events, and Containment events. You can define notifications for specific user groups or your entire organization.

NOTE: Only users assigned the Team Admin or MDC role can view, create, or modify their organization's notification settings.

NOTE: You will receive notifications based on your organization's notification settings and your user notification settings. See **Managing User Notification Settings** **(https://docs.mandiant.com/home/md-configuring-user-settings)** for more details about creating user specific notifications for your account.

Use the **Gear Icon** and **View Notification Settings** menu to view and configure automated MD notifications for users in your organization.



TO CREATE A NEW ORGANIZATION NOTIFICATION SETTING:

1. In the MD Portal, select **Organization** from the **Settings** menu.
2. Click the **Gear Icon** then click the **View Notification Settings** menu.

   > **NOTE:** The *INVESTIGATIONS* tab is selected by default.

3. From the *INVESTIGATIONS* tab, click the **CREATE NOTIFICATION** button to create a new notification setting.
4. Enter the following notification settings: *Triggers*, *Characteristics*, and *Recipients*. As you complete notification settings for *Triggers*, click **Next** to move to *Characteristics* settings and then click **Next** to *Recipients* settings.
5. Click **Done**.
6. Click the *APPLIANCES*, *ANNOUNCEMENTS*, *COMMUNITY PROTECTION*, *ACTIVITY REPORT*, and *CONTAINMENT* tabs and repeat steps 3-5 to create notifications for these areas.

TO VIEW SENT NOTIFICATIONS:

1. In the MD Portal, select **Organization** from the **Settings** menu.
2. Click the **Gear Icon** and then click **View Notification Settings**.
3. Click the **View Sent Notifications** link.
4. Find the notification you want to view in the **Recent Events** table. The table has the following fields: Event Id, Originating Event, Trigger, Status, Notified at (UTC), Deliveries, and Message Details.
5. Click the **Originating Event** link to view the notification details.