MANAGING EMAIL ACTIONS SETTINGS (PROFILES & RULES)

To run Email Actions, you must first create at least one Email Profile and one Email Rule. You must also set up your email server for use by the Director as described in **Email Settings** (https://docs.mandiant.com/home/email-settings#_Ref462406961). The majority of these settings are configured on the Email Actions Settings page.

NOTE: This menu is only available if you have the Email Theater license applied.

- **Creating Email Profiles**
  You can create one or more email profiles that use different email servers and accounts.
- **Creating Email Rules**
  You can create Email Rules that define how automatic responses to emails (such as responses stating that an email or attachment was blocked) are assessed by the Director.
- Setting general time settings

Creating Email Profiles

To run Email Actions, you must have at least one email profile configured.

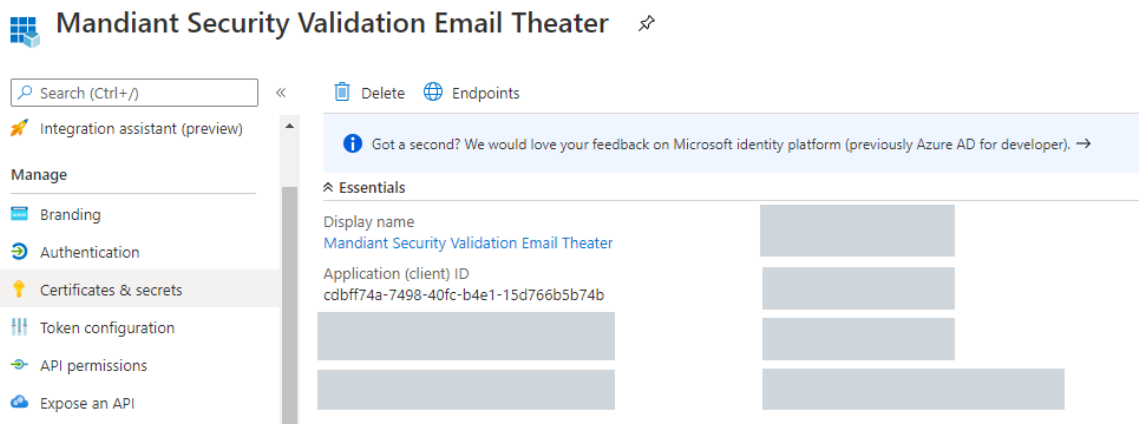
Email profiles establish accounts and email servers for use by Actors during Actions involving email. Multiple email profiles may be created to support multiple Actors.

Email Actions can contain malicious files and malware. Use a dedicated email account for Validation Platform Actors that users do not interact with. Restrict the account's access so that users cannot interact with it manually.

Creating an Email Profile for Microsoft Office 365 Graph API server type

1. Go to **Settings** > **Director Settings**. The System Settings page opens.
2. Select **Email Actions**.
3. Click **Add Email Profile**.
4. In the Add Email Profile form, enter the necessary information, and then click **Submit**.
   - **Server Type:** Select **Microsoft Office 365 Graph API**.
     (Optional) Select **Send verification email manually**.

     Select this option if you cannot use the SMTP server configured on the Director to confirm the email accounts (for example, if the email account the Validation Platform uses cannot send external mail).
   - **Email Address:** Specify the email account that will be used for Email Actions.
   - **Select Security Zone:** Choose a Security Zone to filter the list of Actors. The default is **All zones**.
   - **Select Actor(s):** Select one or more Actors that can pull from the specified email address.
   - **Tenant ID:** (Azure tenant setting) Specify the Azure Tenant/Directory ID assigned to the Azure AD tenant the email account belongs to.
   - **Client ID:** (Azure tenant setting) Enter the Azure Tenant Application (client) ID. This represents the Email Theater application in the Azure tenant.



- **Secret:** (Azure tenant setting) Create a client secret, which is an expiring value created in the Azure UI.

  Be sure to copy the value of the client secret, as it will not display in its entirety once it has expired. For more information, see **Configuring Email Settings for Office 365 with Graph API (https://docs.mandiant.com/home/msv-email-settings-for-common-email-providers#Configur2)**.

Creating an Email Profile for Gmail API

1. Go to **Settings** > **Director Settings**. The System Settings page opens.
2. Select **Email Actions**.
3. Click **Add Email Profile**.
4. In the Add Email Profile form, enter the necessary information, and then click **Submit**.
   - **Server Type:** Select **Gmail API**.

     (Optional) Select **Send verification email manually**.

     NOTE: Select this option if you cannot use the SMTP server configured on the Director to confirm the email accounts (for example, if the email account the Validation Platform uses cannot send external mail).
   - **Email Address:** Specify the email account that will be used for Email Actions.
   - **Select Security Zone:** Choose a Security Zone to filter the list of Actors. The default is **All zones**.
   - **Select Actor(s):** Select one or more Actors that can pull from the specified email address.
   - **Client ID:** Specify the ID created within the Google Cloud console.
   - **Client Secret:** Specify the Secret created within the Google Cloud console.

Creating an Email Profile for other server types

1. Go to **Settings** > **Director Settings**. The System Settings page opens.
2. Select **Email Actions**.
3. Click **Add Email Profile**.
4. In the Add Email Profile form, enter the necessary information, and then click **Next**.
   - **Server Type:** Select the protocol used by the incoming email server.

     (Optional) Select **Send verification email manually**.

> **NOTE:** Select this option if you cannot use the SMTP server configured on the Director to confirm the email accounts (for example, if the email account the Validation Platform uses cannot send external mail).

- **Email Address:** Specify the email account that will be used for Email Actions.

> **NOTE:** This email address does not have to correspond to the server account you specified, but it must be a valid email address. The account you specified must have ownership of the email address you enter. The Director will use the Account credentials to verify this.

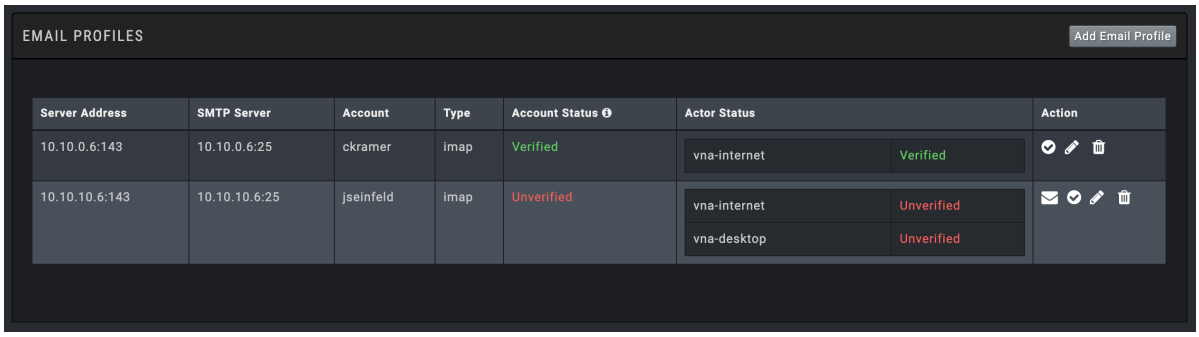
- **Select Security Zone:** (optional) Choose a Security Zone to filter the list of Actors. The default is **All zones**.
- **Select Actor(s):** Select one or more Actors that can pull from the specified email address.
- **Account Username**: Specify the account the Director will use to log in to the email server. The Account Username can be either of the following account types:
  - user@domain
  - DOMAIN\user
- **Account Password** - Specify the password for the username entered above.

> **NOTE:** The account specified must be the same on both your incoming email server and your outgoing email server. If your email account uses two-factor authentication, you may need to obtain an application-specific password from your email provider. For guidance, see **Email Settings for Common Email Providers** **(https://docs.mandiant.com/home/msv-email-settings-for-common-email-providers)** or refer to similar instructions in your email provider's documentation.

5. Enter the Incoming Mail Server information, and then click **Next**.
   - **Server Address:** Enter the IP address or fully qualified domain name of the incoming email server.
   - **Server Port:** Enter the port used for incoming email traffic.
   - **Authentication Type:** Select **Plain** or **NTLM**.
6. Enter the Outgoing Mail Server information and click **Submit**.
   - **SMTP Server Address:** Specify the hostname or IP address of the outgoing email server.
   - **SMTP Server Port:** Specify the port used by the outgoing email server.
   - **SMTP Encryption:** Select **SSL/TLS** or **STARTTLS**. The default value is **Off**.
   - **SMTP Requires Authentication:** Select this checkbox if your outgoing email server uses authentication, and then specify the type in the next field.
     - **SMTP Authentication Type:** Select **Plain** or **NTLM**. This field is hidden unless the SMTP Requires Authentication checkbox is selected.
7. Click **Submit**.

Verifying the Email Profile

You must verify the Email profile is configured correctly before you can use it. Before verification, your Email Actions settings page will look as shown here, in the screenshot below .



Verify Email Profile

After the verification process completes, each Actor shows Verified or Unverified in the Actor Status column of the Email Profiles table. If it failed, additional information is provided to help you troubleshoot the issue.

If you are concerned that validation will fail, connect to the Actor first to validate connectivity to the email host port for inbound & outbound email. You can use the following commands:

- For IMAP (993) and POP (995) (the TLS ports)

  ```
  openssl s_client -connect [ip]:[port]
  ```

  If you get certificate back, you have connectivity
- For IMAP (143) and POP (110)

  ```
  telnet [ip/hostname] [port]
  ```

- For SMTP (25)

  ```
  telnet [ip/hostname] [port]
  ```

- For SMTP (465) and SMTP (587) (The SSL and TLS ports respectively)

  ```
  openssl s_client -connect [ip]:[port]
  ```

  If you get a certificate back, you have connectivity

If the verification fails, the Actors' interface configuration could be a reason. If the interfaces are on the same subnet and were setup using DHCP, this can result in communication issues.

To verify the Email Profile Using the Director

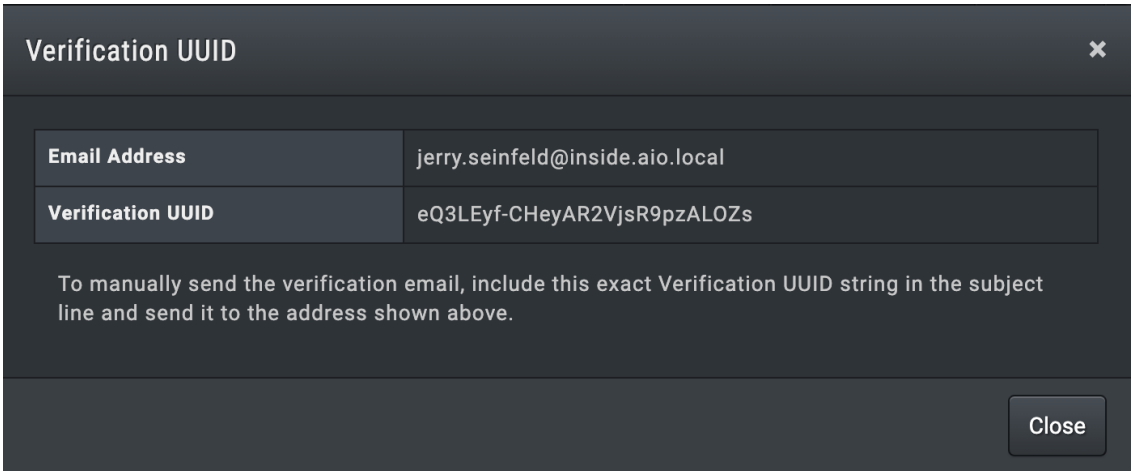
Click **Verify** for the profile to start the verification process.

During the verification process, the Director sends an email from the email address you specified in **Email Settings (https://docs.mandiant.com/home/email-settings)** to the email address you defined in your email profile.

An email address containing a unique code in the subject line is sent for each Actor you associated with the profile. The Actor checks the inbox for that email account and looks for the code. If the Actor can successfully retrieve the code, verification for that Actor on that email address is considered complete.

To Manually verify the Email Profile

1. Click **View UUID Code** for the profile you need to verify.



Verification UUID

> **NOTE:** If the View Verification Code is not visible, edit the Email Profile and select **Send verification email manually**.

2. Send an email to verify the profile. After you send the email, the Email Profile table updates when the email address is verified or if the verification fails.
   a. To Email address: The email address listed in the Verification UUID form
   b. Subject: `(<UUID_STRING>)`, including the parentheses, where *UUID_STRING* is the verification UUID code.

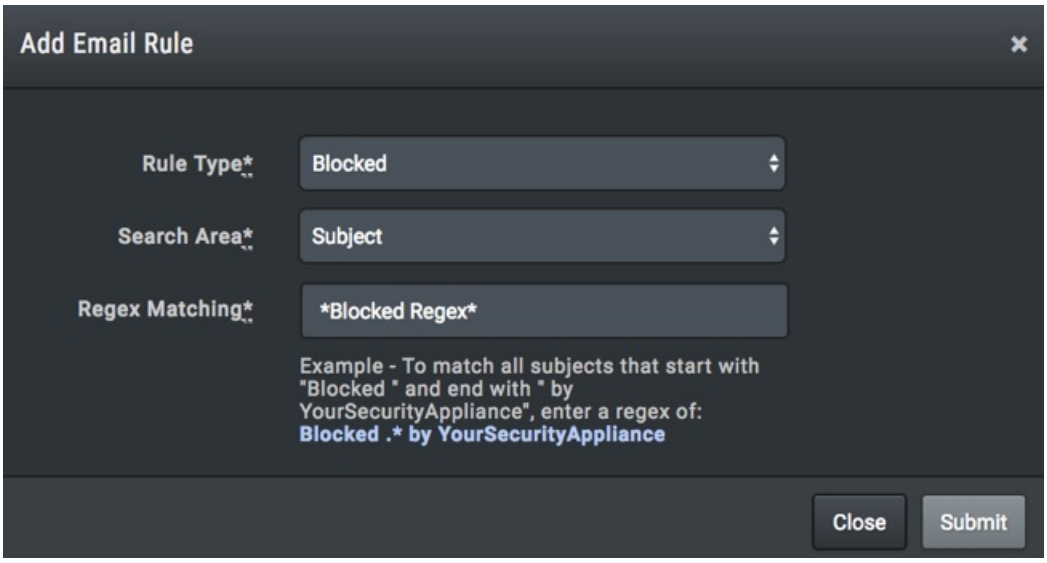
3. Click **Verify** for the profile. The Actor checks the inbox for that email account and looks for the code. If the Actor can successfully retrieve the code, verification for that Actor on that email address is considered complete.

Creating Email Rules

Email Rules specify how the email account defined in the email profile should handle incoming email from Actions. They tailor Security Validation's ability to identify blocking or detection outcomes based on customer defenses.

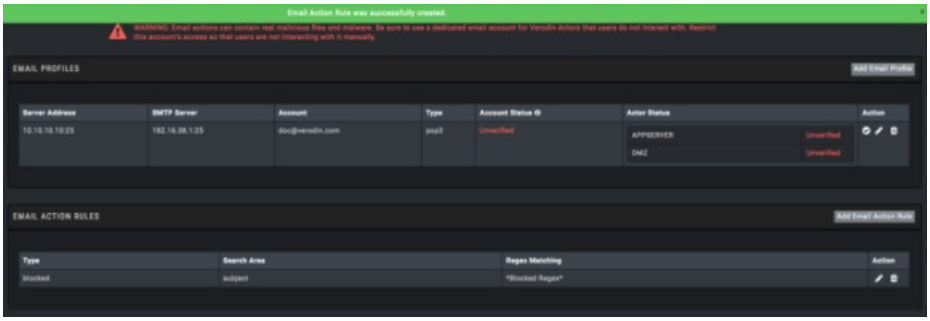
TO ADD A NEW EMAIL ACTION RULE

1. Go to **Settings** > **Director Settings**. The Systems Settings page opens.
2. Select **Email Actions**.
3. Click **Add Email Action Rule**.
4. Specify the Rule Type: **Blocked** or **Error**.
5. Specify the Search Area: **Subject** or **Body**.
6. Specify **Regex Matching** for the email.



Add Email Rule

7. Click **Submit** to save the Email Rule.
   The Email Rule will be saved and applied to all Actions involving email.



Email Action Rule Added