TTP Device Enrollment in Mimecast

Last Modified on 06/12/2019 4:16 pm GMT

Device Enrolment works as part of the Targeted Threat Protection to ensure users to be identified for these services. The service works by having the user enter a one-time code sent to their mailbox when trying to access the service when their identity is unknown. A cookie is then stored in their browser to identify the user.

Device Enrolment allows for:

- **Reporting on which users click a link:** If a user forwards an email to another internal recipient, or an email was sent to a group, device enrolment allows the link click to be tracked to that user.
- **Release Attachments to the correct user**: If a user forwards an email to another internal recipient, or an email was sent to a group, device enrolment allows released attachments to be sent to the correct user.

Enable/Disable

Device Enrolment is enabled by default on your Mimecast account. You will need to disable the setting in your Account Settings in the Administration Console. Note that this is a global setting, it can't be disabled for a subset of users.

1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**
3. Go to **'Administration > Account > Account Settings'**
4. Expand the **User Access and Permissions** section
5. Toggle the checkbox for **Targeted Threat Protection Authentication**

User Experience

Remove Enrolment

If you have issues with enrolment or a device is lost/stolen, you can revoke the enrolment to force the device to need to re-register again.

6. Press **Save**

This process will remove all device enrolments for user, so they will need to re-enrol all their devices again.

Sign-In Prompt

If a user click onto a re-written link or requests an attachment and the web browser used is not enrolled, they will be prompted to enter their email address. This will send them an Authentication code.

Enrolment Code

When the user requests the code, they will receive an email from the Postmaster address for the Mimecast account.

This code will need to be entered into the browser. Once accepted, the device will remain enrolled until the authentication expires. The cookie will be renewed each time it is used, so most users will not need to re-enrol again.

Troubleshooting

Due to the nature of the device enrolment, you may need to troubleshoot this service at times.

Below are some common restrictions that can result in unintended behaviour.

- Cookies must be enabled on the web browser being used
- If cookies are not set to persist between sessions or Private Browsing is used, enrolment will be prompted when the session is closed
- The cookie is stored on the web browser, so each browser will need to enrol individually
- Users must sign in with their primary email address for device enrolment
- A support browser must be used:

1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**

3. Go to **‘Administration > Directories > Internal Directories’**

4. Click into the User’s domain
5. Click into the User
6. Under Targeted Threat Protection, select

Revoke Authentication

7. Confirm to proceed with the unenrolment

https://community.mimecast.com/s/article/Mimecast-Browser-Support-Matrix-470511400

- Only a single Apple device can be registered for a single user at once, additional devices will always prompt for enrolment