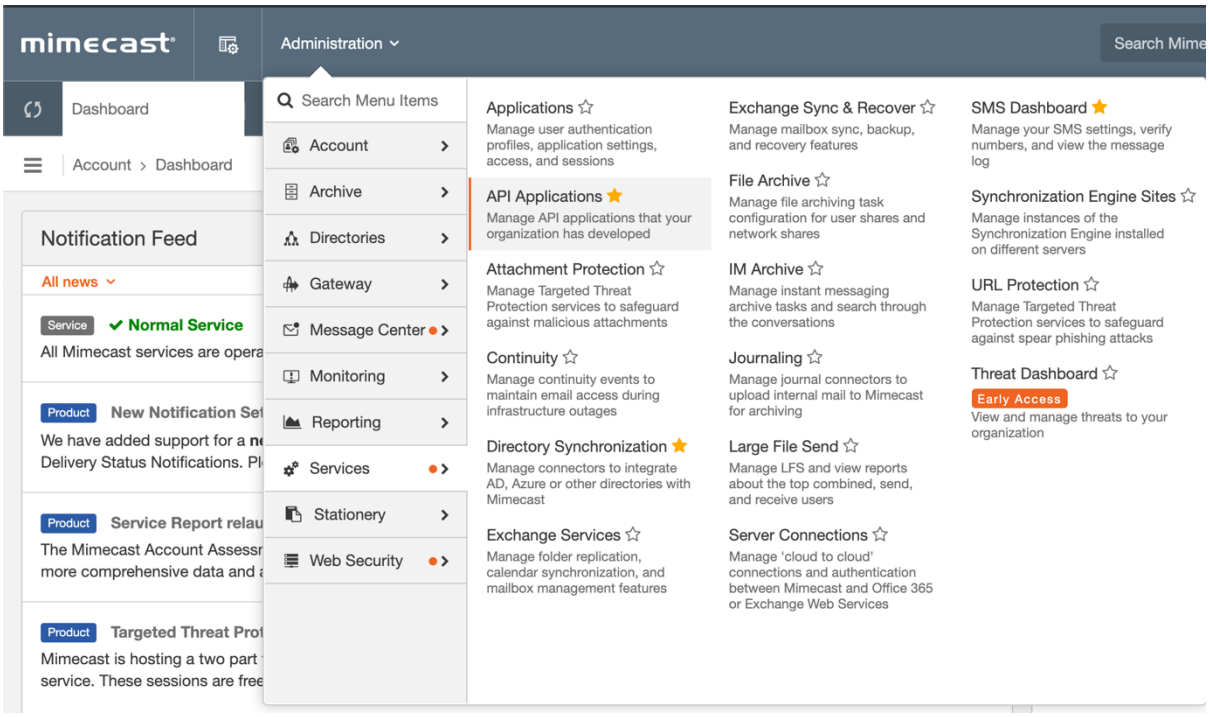
Mimecast Palo Alto Cortex Integration – Admin Guide

Prerequisites

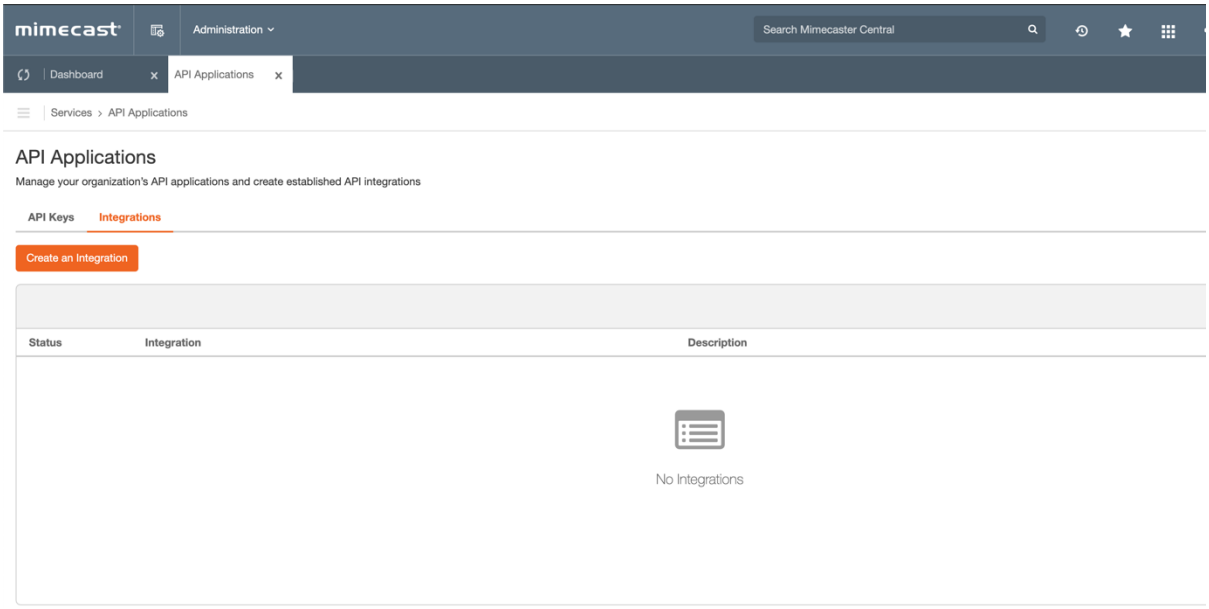
- Mimecast Directory Sync Connector
  - The ***sAMAccountName*** or ***userPrincipalName*** Active Directory attribute needs to be synced with the Mimecast platform in order to identify users.
  - Please see the following for further information on Directory Linked attributes;
    - Managing Attributes
    - Synchronizing User Attributes with Azure Active Directory
- A Palo Alto Cortex Hub Account and Palo Alto Cortex Data Lake
  - NGFW must captures the source user identity by either their sAMAccountName or userPrincipalName directory attribute

Configuration

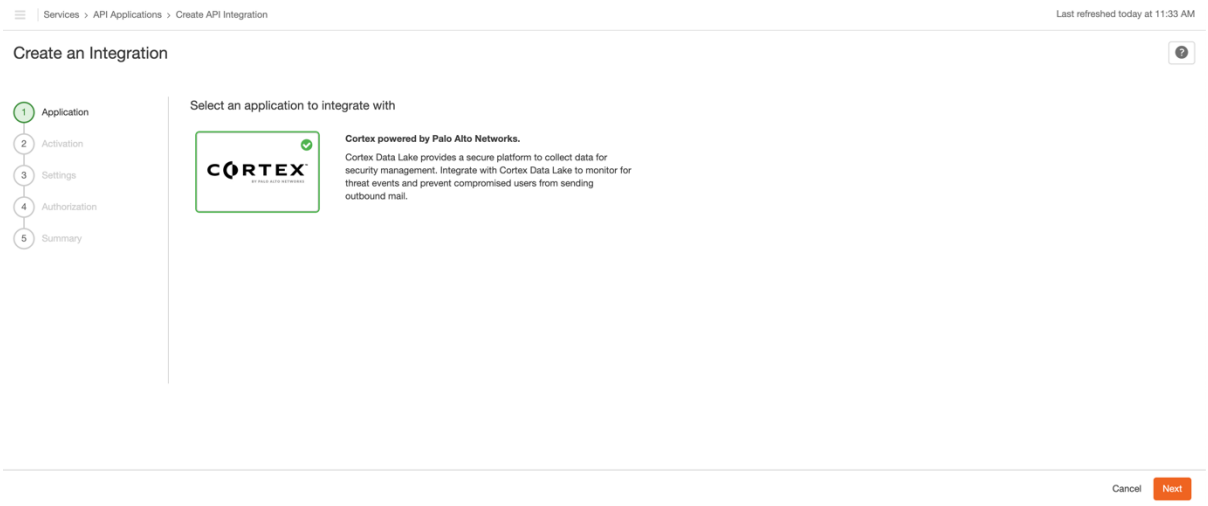
1. Login to the Mimecast Administration Console
2. Select ***Administration*** > ***Services*** > ***API Applications***



3. Click on the ***Integrations*** tab heading



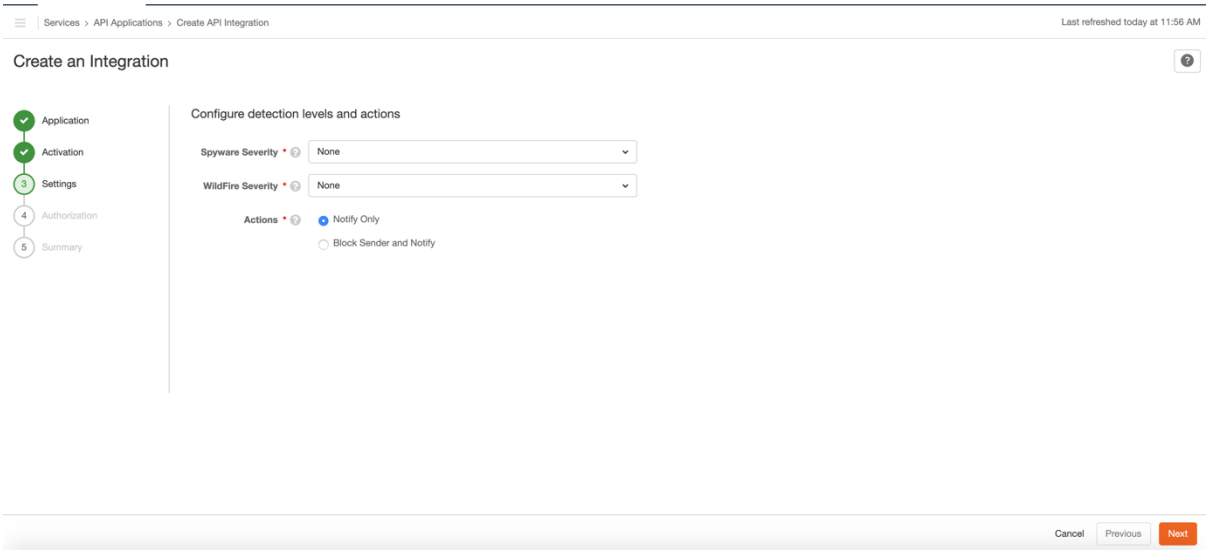
4. Click on the ***Create an Integration*** button
5. Select the Cortex tile, followed by clicking on Next



6. Follow the on-screen instructions to activate the Mimecast app;
    i. Open a new browser tab
    ii. Log in to your ***Palo Alto Networks Hub*** account.
    iii. Locate the **Mimecast** app and click 'Activate'. Follow the instructions provided by Cortex Data Lake.

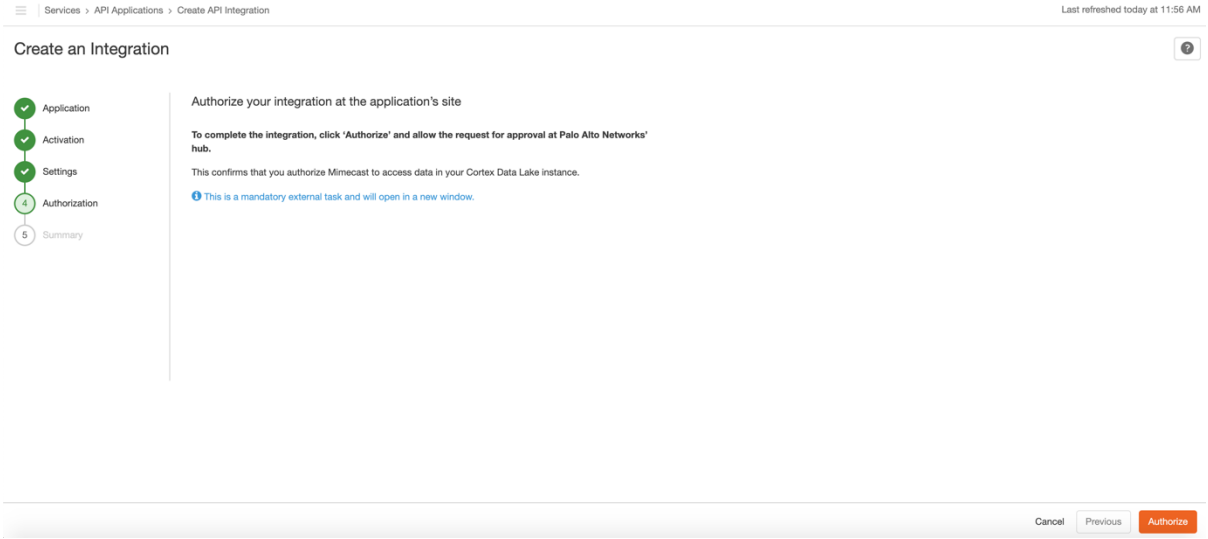
    Note: The above steps must be completed before the next step (2) in the wizard can be reached.

7. Click the activated Mimecast app to continue configuring the integration from the Mimecast Administration Console.
8. Configure the severity levels for Spyware and Malware events and the action to be taken. Events at the configured severity level or higher will trigger the configured action. Click Next to proceed to the next step.

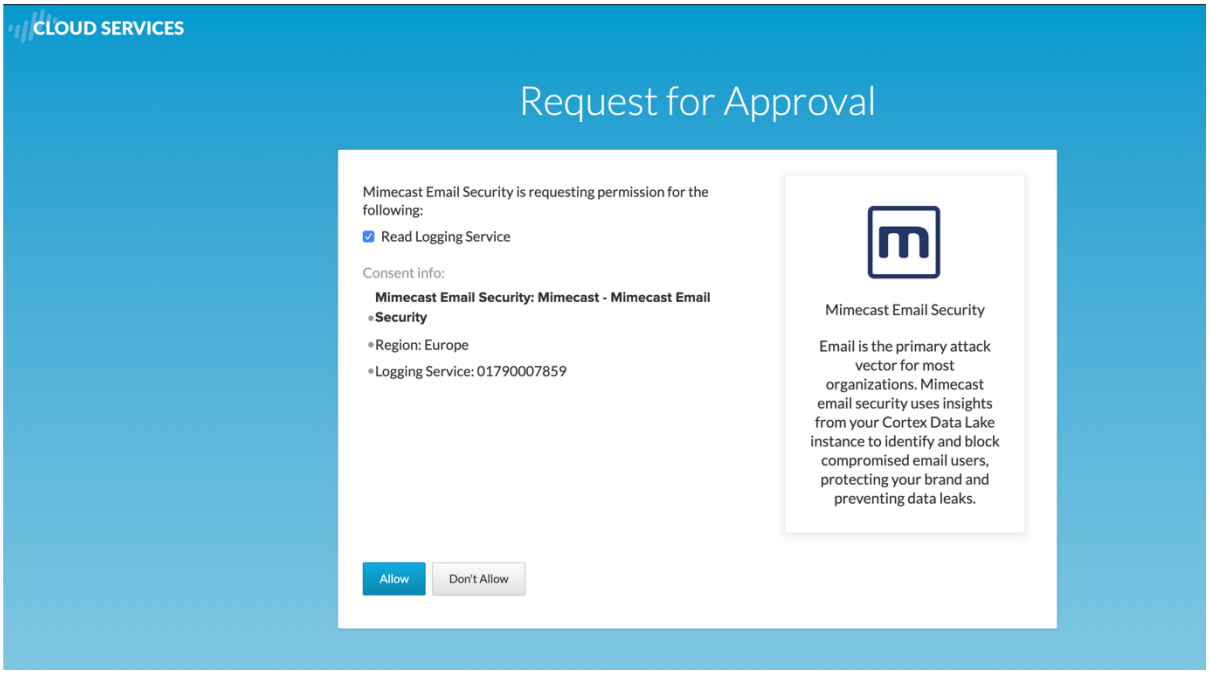


Note: Notifications are sent to the address set for ***Notification Postmaster Address*** under ***Administration*** > ***Account*** > ***Account Settings*** > ***System Notifications***

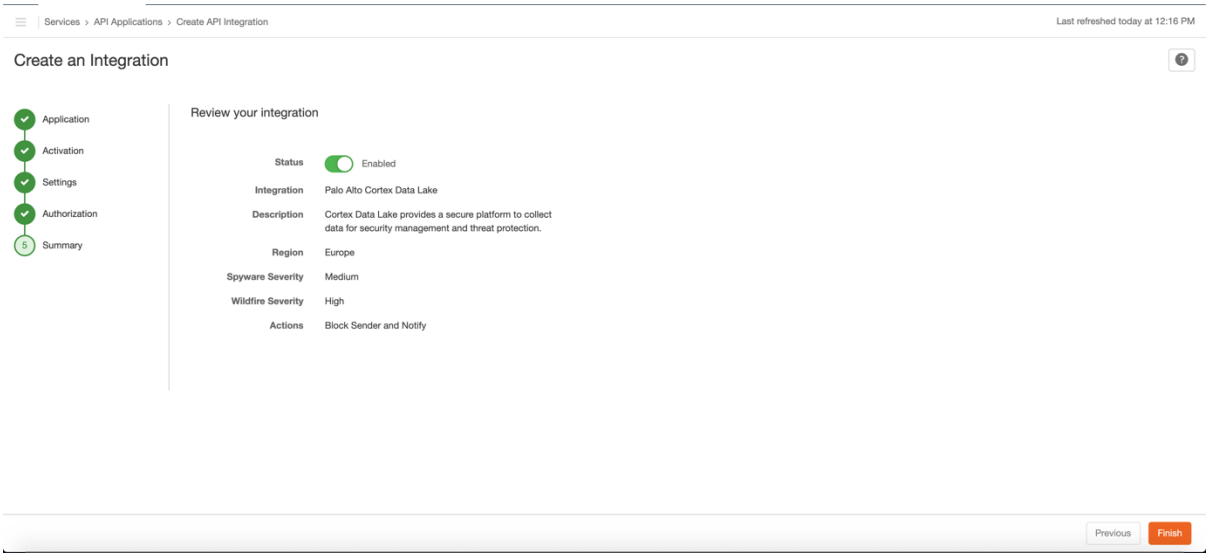
9. The Authorization step authorizes the Mimecast app activated in step 6, click on **Authorize**



10. You will be taken to the Palo Alto Networks Cortex Hub, where you will be asked to Allow/Disallow the Mimecast platform to communicate with the Mimecast app activated in step 6, click on the **Allow** button



11. You will be returned the Mimecast Administration Console and shown a summary of the settings that have been configured



12. Enable the integration, followed by clicking on the **Finish** button
13. The integration is now activated, configured and authorized.
14. The following changes will take place on the account when a Spyware or Malware event that matches or exceeds the configured severity level is first detected;

    a. A **Cortex Integration** Blocked Senders policy and Profile Group are created
    b. The Blocked Senders policy is configured to block emails from members of the **Cortex Integration** Profile Group to **Everyone**