# Integrating Mimecast

https://campus.barracuda.com/doc/98222117/

To deploy Mimecast, do the following procedures (See below):

When a user's password is changed or the account is disabled, any set of Access Key and Secret Keys for that user will also be revoked. A new set of Access and Secret Keys will need to be generated to continue making API calls.

If new Access and Secret Keys need to be generated, remove the user from any administrative role. Re-add the user after new keys have been obtained.

## Create an API application

1. Log into the Administration Console.
2. Navigate to **Administration > Services > API and Platform Integrations**.
3. Click the **Your Application Integrations** tab.
4. Click **Add API Application**.
5. Fill in the **Details** section as outlined below:
   - **Application Name** – Name for the application. For example, *Barracuda XDR Log Collector.*
   - **Category** – Select **SIEM Integration**.
   - **Service Application** – Enable the **Enable Extended Session option** checkbox. This is recommended for integrations with a valid access and secret key pair to call the API frequently using just authorization.
   - **Description** – Description of the application. For example, *Barracuda XDR Managed Detection and Response provider.*
6. Click **Next**.
7. Fill in the **Settings** section as outlined below:
   - **Technical Point of Contact** – Name of a person or group to contact if Mimecast needs to speak with the maintainer of this API application.
   - **Email** – Email address of person or group to contact if Mimecast needs to speak with the maintainer of this API application.
   - **Opt-In** – Select this option to receive updates on API changes.
8. Click **Next**.
9. Review the **Summary** page to ensure all details are correct.
10. Click **Add**. The application details will display in a slide-in panel.
11. Copy and paste the **Application ID** and **Application Key** to a safe place to use later in the process.
    **Note** that it can take up to 30 minutes for this process to complete.
12. While waiting for the application to go live, continue to the next step.

## Create a Service Account User

1. Navigate to **Administration > Directories > Internal Directories**.
2. Click on the domain to add the user to.
3. Click **New Address**.
4. Complete the user's **Email Address**. For example, *skout-siem-@yourdomain.tld*.
   **Note**: The service account user does not need a mailbox or access to mail flow to function unless MFA will be used.
5. Enter a **Password** and **Confirm Password**. Remember this password to use later in the process.
6. Click **Save**.

## Create a Profile Group

1. Navigate to **Administration > Directories > Profile Groups**.
2. Click on the **+** icon next to the **Root** folder.
3. Click on the new folder to open the **Edit Group** text box and rename the folder. For example, *Barracuda XDR API Profile Group*.
4. Press **Enter** to save the new name.
5. Click **Build > Add Email Addresses**.
6. Enter the service account user's email address in the **Group Additions** text box.
7. Click **Save** and **Exit**.

## Create an API user Authentication Profile

1. Navigate to **Administration > Services > Applications > Authentication Profiles**.
2. Click **New Authentication Profile**, and then enter a profile name. For example, *Barracuda XDR Authentication Profile*.
3. If the service user does not have a mailbox, disable all the SAML and 2FA options.
4. Set the **Authentication TTL** to **Never Expire**.
5. Click **Save** and **Exit**.

## Create Application Settings

1. Navigate to **Administration > Applications**.
2. Right-click **Default Application Settings** and select **Clone Configuration**. This will create a new application settings definition.
3. Assign the **Profile Group** and **Authorization Profile** you just created to this settings definition. This will apply the settings to the service account.
4. Click **Save** and **Exit**.

## Create API keys

You must wait 30 minutes after creating your API application before creating the API keys.

1. Navigate to **Administration > Services > API Applications**.
2. Click the new API Application from the application list.
3. Click **Create Keys**. The "Create Keys" wizard is displayed with the **Account** tab selected.
4. Enter the **Email Address** of your service account.
5. Click **Next**.
6. Complete the **Authentication** dialog with the following:
    - **Type** – Cloud.
    - **Password**– Enter the service account's password.
7. Click **Next**.
8. If prompted to verify the service account, follow the instructions on the screen, and then click **Next**.
   The **Keys** tab is displayed with the generated keys hidden by default.
9. Copy the **Access Key** and **Secret Key**.
10. Click on the **Finish** button to exit the wizard and return to the application list.

## Granting API Service Account User Permissions

Due to the Administration Authentication Profile and its ability to override authentication for any user granted rights by an administrator role, it is recommended to generate the Access and Secret Keys before adding the user to the administrative role.

1. Navigate to **Administration > Account > Roles**.
2. Click **New Role**.
3. Enter a **Role Name** and **Description**. For example, *Barracuda XDR Integration*.
4. In the **Application Permissions** section, select the boxes for each of the following permissions to be used by the service user account:
    - Account | Logs | Read permission
    - Monitoring | Data Leak Prevention | Read permission
    - Monitoring | Attachment Protection | Read permission
    - Monitoring | Impersonation Protection | Read permission
    - Monitoring | URL Protection | Read permission
    - Services | Gateway | Tracking | Read permission
5. Click **Save** and **Exit**.
6. Locate the newly created role and click on the role name.
7. Click **Add User to Role**.
8. Click the email address of the API service user account.

## Enable Enhanced Logging

1. Navigate to **Administration > Account > Account Settings**.
2. Expand the **Enhanced Logging** section and enable the following:
    - Enhanced inbound email logging
    - Enhanced outbound email logging
    - Enhanced internal email logging

## Obtain the Base URL

1. Log into Mimecast and obtain your Base URL from Mimecast Data Centers and URLs.

## Enter Values into XDR Dashboard

Enter the following values obtained from Mimecast into the Barracuda XDR Security Dashboard:

- Application ID
- Application Key
- Access Key
- Secret Key
- Base URL