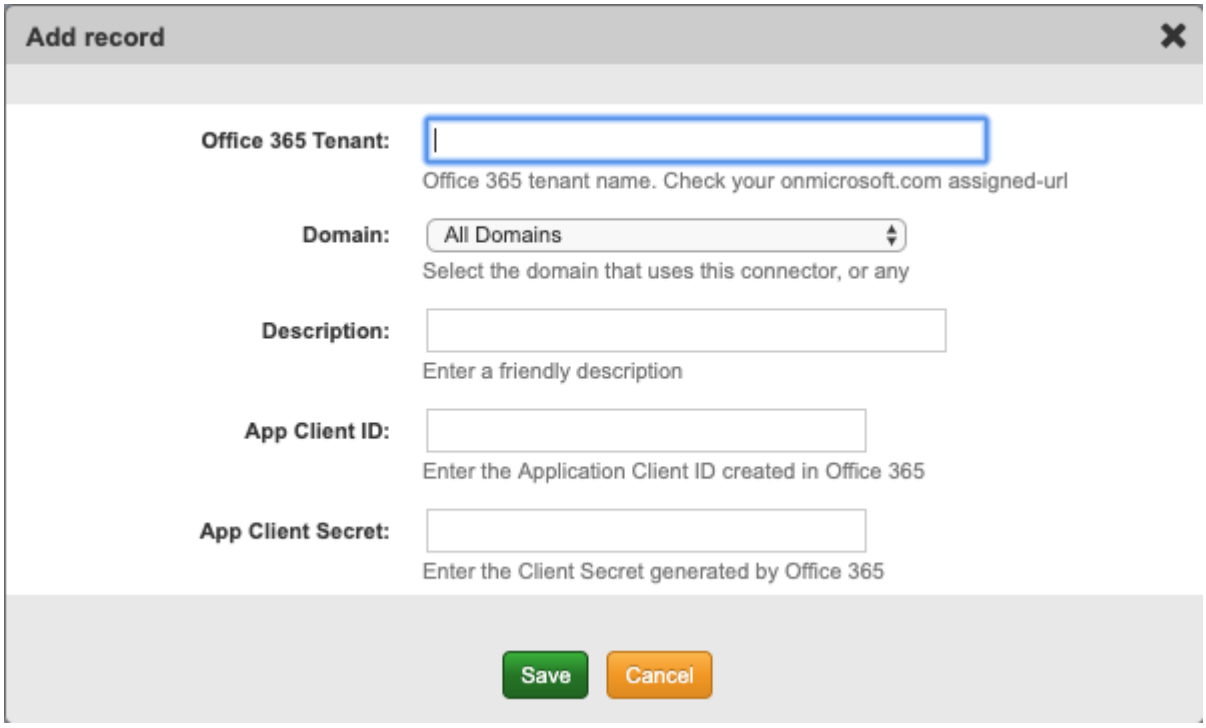
Office 365 Threat Remediation Settings

Libraesva ESG Threat Remediation feature fully support Microsoft Office 365. Office 365 relies on Azure Active Directory as directory service. Each Office 365 tenant corresponds to an Azure AD tenant where its user information is being stored. This guide will cover the steps needed to grant your Libraesva ESG permissions on your Office 365 tenant. No changes are made to the Office 365 tenant itself by Libraesva ESG.

Configure Office 365 connection

- First thing is to grant the correct permissions, see: Microsoft Azure AD Libraesva App registration
- Now navigate to your Libraesva ESG and select **System > Authentication > Office 365 Configuration**
- Click **[+] New**
- Insert your tenant name in the Office 365 tenant field (This is the tenant name of your office 365, if your admin account is admin@testcompany.onmicrosoft.com, your tenant will more likely just be testcompany.onmicrosoft.com)
- Select the Domain you want to bind this configuration to or leave All Domains
- Give a friendly description to the new connection
- Insert the **Application ID** you copied before
- Insert the password you copied above in the **App Client ID** field
- Click **Save**.



- **Test** your Configuration by clicking the > icon next to the entry.

×**NOTE:** If you receive an **Insufficient privileges to complete the operation** error wait a few minutes for Azure to clean caches and retry.

Configure Threat Remediation Connector

Now select **System > Authentication > Threat Remediation Connector**

- Click **[+] New**
- Select your Office 365 domain from the dropdown Domain list
- Give a friendly description to the connector
- Select **Office 365** as **Mail Server version**
- Libraesva Version **<= 4.8:** Enter the username/password to access Microsft 365 API. **This user must have impersonation role.**

×**NOTE:** You can follow this guide: Setup an impersonation account in Office 365

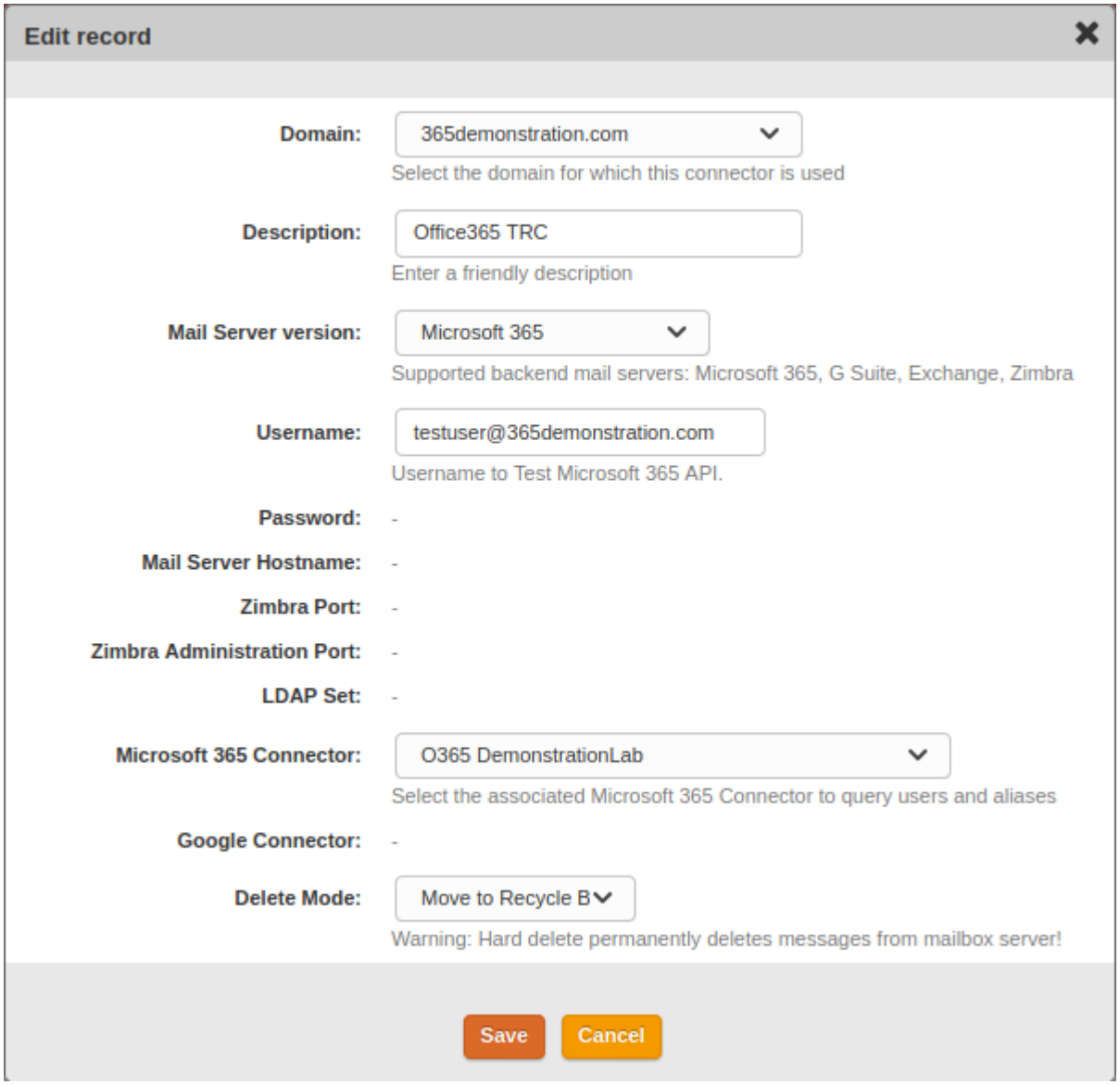
- Libraesva Version **>= 4.9:** Enter Username to test Microsoft 365 API.

×**NOTE:** Starting from version 4.9 the Threat Remediation Connector uses the Microsoft Graph API to recall the message. You don’t need to provide a User with Impersonation Role

- Select the connector you created above from the dropdown list
- Specify the preferred **Delete Mode**
  - **Soft Delete** – Recalled messages will be deleted but still available for recovery in the Recoverable Items folder
  - **Hard Delete** – Recalled messages will be permanently deleted
  - **Move to Recycle Bin** – Recalled messages will be moved to the user recycle bin

×**WARNING:** In order to use **Hard Delete** mode from Libraesva ESG 4.9 and onwards, please check the settings described in this guide

- Click **Save**



- Test your Connector by clicking the > icon next to the entry.