# How to create alert policies? What are those policies used for?

|  |  |
| --- | --- |
| Reference |  |
|  |  |
|  |  |

# Assigning permission in SCC.

|  |  |
| --- | --- |
| Reference |  |
|  |  |
|  |  |

# How to import .PST files?

|  |  |
| --- | --- |
| Reference |  |
|  |  |
|  |  |

# What is Submission explorer? How to submit emails?

|  |  |
| --- | --- |
| Reference | <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/admin-submission?view=o365-worldwide> |
| Submission Explorer | * In Microsoft 365 organizations with mailboxes in Exchange Online, admins can use the Submissions portal in the Security & Compliance Center to submit email messages, URLs, and attachments to Microsoft for scanning. * When you submit an email, you will get information about any policies that may have allowed the incoming email into your tenant, as well as examination of any URLs and attachments in the mail. |
| Roles Required | * **Organization Management** or **Security Administrator** in the **Security & Compliance Center** * **Organization Management** or **Hygiene Management** in **Exchange Online** |
| **Submit Emails through Submission Explorer** | |
| Please go to –  <https://protection.office.com>  Please navigate to –   Threat management > ② Submission > ③ New Submission  For Email –  Choose Object type, Submission format, Reason for submission & press submit  For URL/Attachment –  Mention URL link/download the attachment, choose Reason for submission & press submit |  |

# What are the reasons for a user to be restricted from sending email? How to unblock users from restricted users?

|  |  |
| --- | --- |
| Reference | <https://tinyurl.com/y4hqqtkm> |
| Reasons for Restriction from Sending Email | * If a user exceeds one of the outbound sending limits (e.g. 30 messages/minute) as specified in the service limits or in outbound spam policies. * The user is restricted from sending email, but they can still receive email. * When they try to send email, the message is returned in a **non-delivery report** **(NDR)** with the error code **5.1.8 (Access Denied)** and the following text: |
| **Unblock user from Restricted User** | |
| * In the Security & Compliance Center, go to **Threat management** > **Review** > **Restricted users** * Find and select the user that you want to unblock. In the **Actions** column, click **Unblock**. * Click **Next** when done. * The next screen has recommendations to help prevent future compromise. Enabling multi-factor authentication (MFA) and changing the passwords are a good defense. Click Unblock user when done. * It may take 30 minutes or more before restrictions are removed. | |
| **How to Resolve the Issue (5.1.8 – Access Denied)** | |
| * If the user is doing is willingly, admin may warn user and unblock. * If the user account is hacked, then admin can **reset password, enable MFA, Do MHA, try Message trace** | |

# What is the purpose of Anti-Phishing & Anti-Spam Policies? How to set up these policies?

|  |  |
| --- | --- |
| Reference |  |
|  |  |
|  |  |

# How to create an outbound spam policy?

|  |  |
| --- | --- |
| Reference |  |
|  |  |
|  |  |