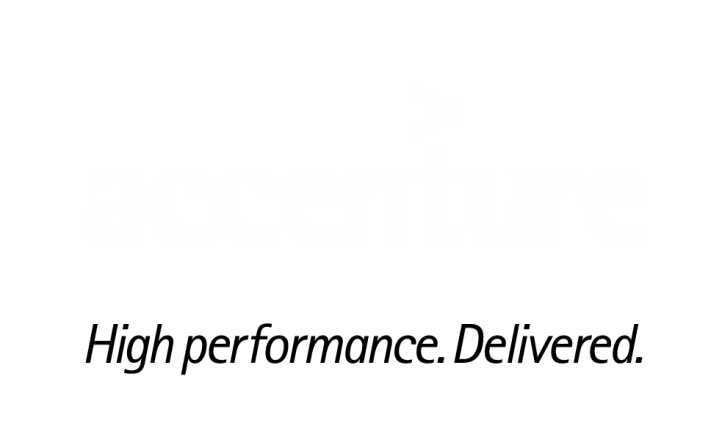
Troubleshooting Guide



**Missing / Undelivered email related issues**

Contents

[1. How to find missing emails from outlook. 3](#_Toc520980416)

[2. Maximum Mail size limit 5](#_Toc520980417)

[3. Send/receive email from external mailing list 5](#_Toc520980418)

[4. Unable to send email to Distribution List 6](#_Toc520980419)

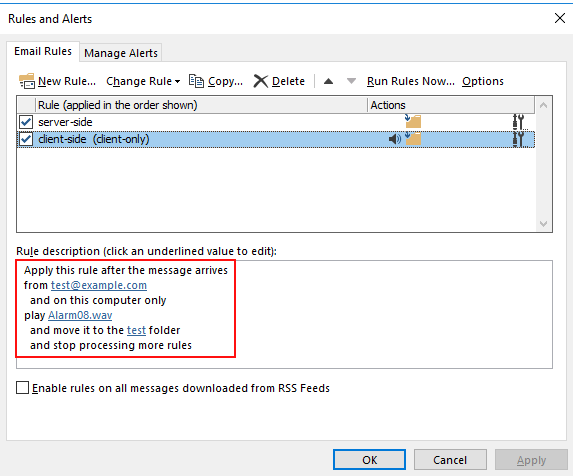
[5. Blocked emails due to Policy 8](#_Toc520980420)

[6. Emails blocked due to spoofing 12](#_Toc520980421)

[7. Junk E-Mail filter in Outlook 13](#_Toc520980422)

# How to find missing emails from outlook.

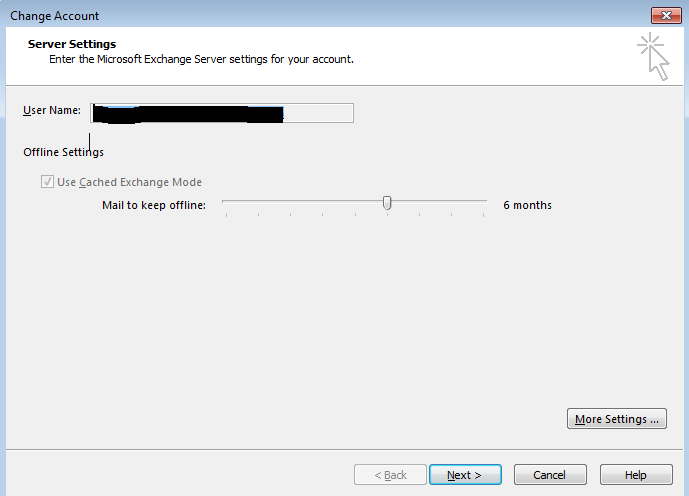
1. Check if any outlook rules are configured to move the specific emails. File -> Info -> Manage Rules & Alerts.



1. Check if the missing emails are showing up in OWA, if yes check the outlook cache slider settings (File -> Info -> Account Settings -> Account Settings -> Double Click on the account) and toggle the slider accordingly.

This feature is called Data Based Sync Slider. This allows you to limit the amount of data that is synchronized locally to your OST. The purpose of the slider is to make Outlook usable on devices that have limited or small amounts of local storage. ---- (1/3/6/12/All month)

*For example, if you set it to 24 months, the email up to 24 months would sync/cache to your local OST file, all older messages would stay at server*.



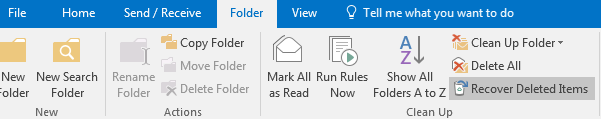
1. Check if user has created any PST and moved the emails to PST.
2. If the emails are not showing up in OWA, Check the below folders.

Online Archive Folders

Junk E-Mail

Deleted Items

Recover Deleted Items (Outlook->Folder)



1. Try to search by giving subject of the email, sender in the search option.
2. If the above steps are not fixing the issue, raise an incident with M&C team (**SNOW queue MSGCOLLAB-O365-OPER**).

# Maximum Mail size limit

User receives an error while sending the email: "MAXIMUM MAIL SIZE LIMIT EXCEEDED".

The maximum mail size limit to receive and send email is 25 MB. Provide the details below to the User and no changes or exception would be made to modify the limit. Kindly also note that the 25 MB limit includes all the contents of the email (i.e. message body, attachments).

Offerings for Licenses are mentioned below:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Feature** | **Office 365 Business Essentials** | **Office 365 Business Premium** | **Office 365 Enterprise E1** | **Office 365 Enterprise E3** | **Office 365 Enterprise E5** | **Office 365 Enterprise F1** |
| Size limit for messages (for subscribers using Office 365 Message Encryption legacy version) | 25 MB | 25 MB | 25 MB | 25 MB | 25 MB | 25 MB |

# Send/receive email from external mailing list

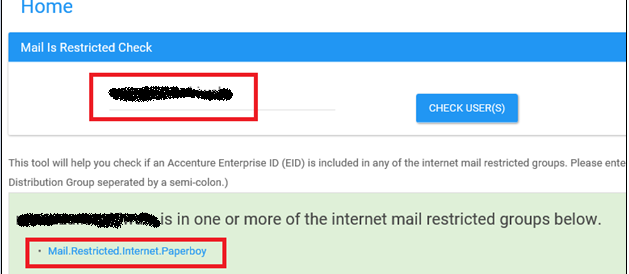
When user is unable to send or receive the emails from/to external email ID.

1. Service desk must verify if the user is a member of any Internet Block List from the portal:

<https://mcportal.accenture.com/WebTools/MailIsRestrictedCheckapp>

2. Enter the EID of the affected user and check.

3. If it returns any group like below, user need to reach out to the group owner (which can be checked on the web admin portal <https://directory.accenture.com/WebAdmin/search.aspx> ) to exclude his/her name or click upon the group itself on the site which would redirect you to the site for owner details.



1. If user is not a part of any restricted DL, service desk must assign the incident to M&C SNOW queue (MSGCOLLAB-O365-OPER).

# Unable to send email to Distribution List

**Case 1: No users can send email to a distribution list**

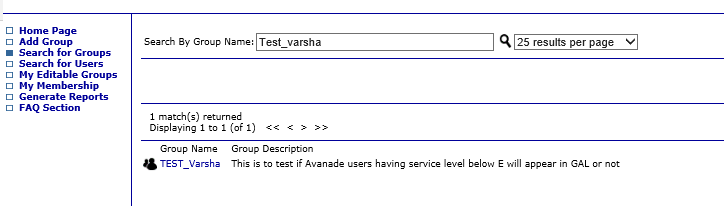
Users receives the NDR below while sending an email to the distribution list. Below is the error:

**550 5.7.124 RESOLVER.RST.RestrictedToGroupPermission; not authorized to send to the distribution list because the distribution list is set up to accept mail from list members only, or specific recipients only**

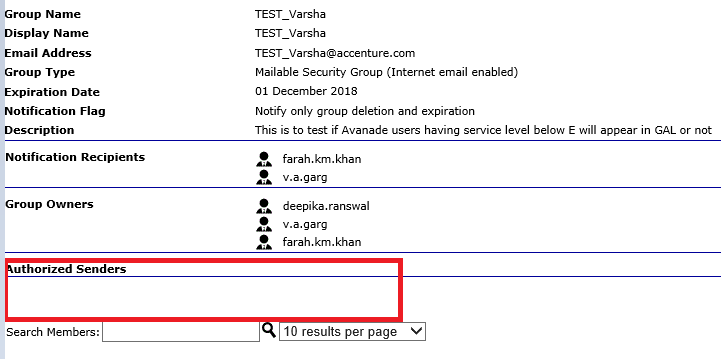
Steps to Fix the Issue:

1. Service desk must search the affected DL in the web admin portal:

<https://directory.accenture.com/WebAdmin/search.aspx>



2. If the DL has authorized senders and user is not a part of the same, the above-mentioned error will be received.



3. Also the user should be a member of the DL even though he/ she is an owner of the DL.

4. If all the above conditions are met and still user is unable to send the email, SD must assign the incident to M&C team SNOW queue MSGCOLLAB-O365-OPER

**Case 2: Users from the external ID receives NDR while sending the email to the distribution list.**

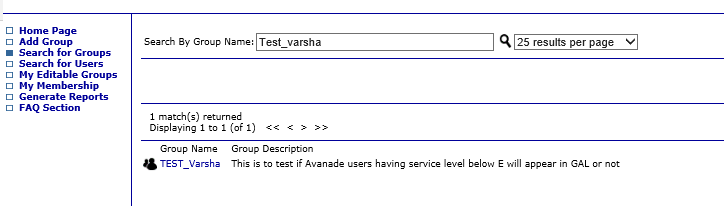
External users receive the NDR below while sending an email to the distribution list. Below is the error:

**550 5.7.124 RESOLVER.RST.RestrictedToGroupPermission; not authorized to send to the distribution list because the distribution list is set up to accept mails from inside organization only.**

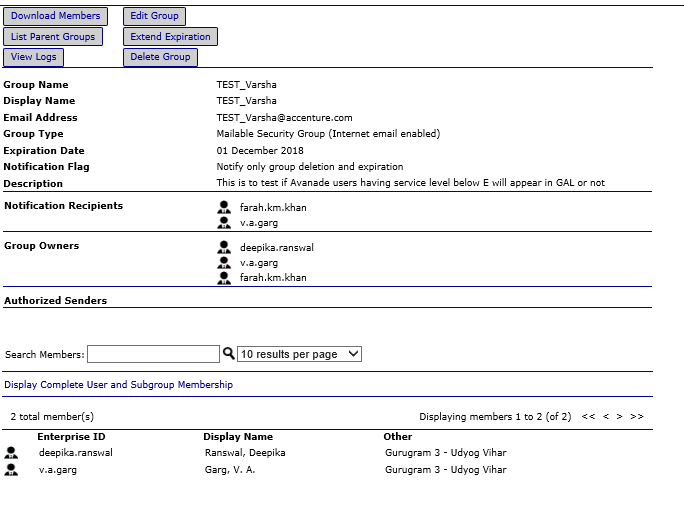
Steps to Fix the Issue:

1. Service desk must search the affected DL in the web admin portal:

<https://directory.accenture.com/WebAdmin/search.aspx>



2. If the DL has the missing attribute i.e. **Internet email enabled** from the **Group type** then SD must ask the user to reach out to the group owner to edit this property.



3. If all the above settings are fine and issue persist, SD must assign the incident to M&C team SNOW queue MSGCOLLAB-O365-OPER

# Blocked emails due to Policy

Users may reach out to M&C stating that certain emails are not being sent/received to/from the internal or external users. In such scenarios please have the contents being sent or the way the email is sent reviewed.

There are reasons you might get a Delivery Failure message. Below are examples that indicate Accenture has a security setting that is preventing your message from reaching the recipient.

**Emails blocked due to certain attachment**

Steps to Fix the Issue

**Delivery Failure because of Executable Content**  
 **Failure Text:** Your message with executable content attached was blocked.

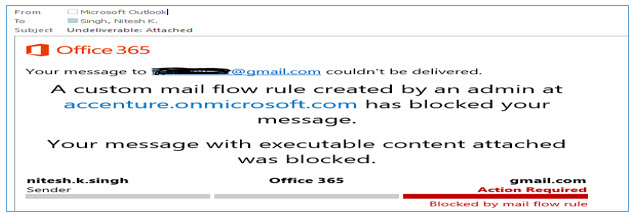
**What the Delivery Failure Means:** You message was not delivered. Due to security concerns, Accenture blocks e-mails containing attachments with executable content. Below is a list of executable blocked file types.

|  |  |
| --- | --- |
| **Extension** | **File type** |
| .ade | Microsoft Access project extension |
| .adp | Microsoft Access project |
| .app | Executable Application |
| .asp | Active Server Page file |
| .asx | Windows Media Audio / Video |
| .bas | Microsoft Visual Basic class module |
| .bat | Batch file |
| .chm | Compiled HTML Help file |
| .cmd | Microsoft Windows NT Command script |
| .com | Microsoft MS-DOS program |
| .cpl | Control Panel extension |
| .crt | Security certificate |
| .csh | Photoshop Custom Shapes File |
| .fxp | FoxPro Compiled Program |
| .gadget | Windows Gadget |
| .hlp | Help file |
| .ht | HyperTerminal Session File |
| .hta | HTML program |
| .inf | Setup Information |
| .ins | Internet Naming Service |
| .isp | Internet Communication settings |
| .its | Impulse Tracker Sample |
| .js | JScript file |
| .jse | Jscript Encoded Script file |
| .ksh | Unix Korn Shell Script |
| .lnk | Shortcut |
| .mad | Electronic Arts Madcow Movie File |
| .maf | Mutation Annotation Format File |
| .mag | Magic Circuit Layout File |
| .mam | Microsoft Access Macro |
| .maq | Microsoft Access Query |
| .mar | Mozilla Archive |
| .mas | rFactor Track File |
| .mau | Media Attachment Unit |
| .mav | Access View File |
| .maw | Access Data Access Page |
| .mda | Microsoft Access add-in program |
| .mdb | Microsoft Access program |
| .mde | Microsoft Access MDE database |
| .mdt | Microsoft Access workgroup information |
| .mdw | Microsoft Access workgroup information |
| .mdz | Microsoft Access wizard program |
| .mp4 | MPEG-4 Video File |
| .msc | Microsoft Common Console document |
| .msh | Orbiter 3D Mesh File |
| .msh1 | Microsoft Shell script file |
| .msh1xml | Windows Power Shell script file |
| .msh2 | Microsoft Shell script file |
| .msh2xml | Windows PowerShell script file |
| .mshxml | Microsoft XML type data file |
| .msi | Microsoft Windows Installer package |
| .msp | Microsoft Windows Installer patch |
| .mst | Microsoft Windows Installer transform; Microsoft Visual Test source file |
| .ops | Office XP settings |
| .pcd | Photo CD image; Microsoft Visual compiled script |
| .pif | Shortcut to MS-DOS program |
| .plg | Visual Studio Build Log File |
| .prf | Microsoft Outlook profile settings |
| .prg | Program File |
| .ps1 | Windows PowerShell Cmdlet File |
| .ps1xml | Windows PowerShell Display Configuration File |
| .ps2 | PCSX2 Memory Card File |
| .ps2xml | Windows PowerShell file |
| .psc | Papyrus Script |
| .psc1 | Windows PowerShell Console File |
| .psc2 | Microsoft Windows PowerShell script file |
| .pst | Outlook Personal Information Store File |
| .reg | Registration entries |
| .scf | Windows Explorer command |
| .scr | Screen saver |
| .sct | Windows Script Component |
| .shb /.shs | Shell Scrap object |
| .tmp | Temporary File |
| .url | Internet shortcut |
| .vb | VBScript file |
| .vbe | VBScript Encoded script file |
| .vbs | VBScript file |
| .vsm | Blackberry data file |
| .vsmacros | Microsoft Visual Studio binary-based macro project |
| .vsw | Microsoft Office Visio 2010 web drawing file |
| .wav | WAVE Audio File |
| .wma | Windows Media Audio File |
| .ws | Microsoft Windows script |
| .wsc | Windows Script Component |
| .wsf | Windows Script file |
| .wsh | Windows Script Host Settings file |
| .xi | Fasttracker 2 Extended Instrument File |
| .xnk | Exchange Shortcut |
| .xsl | XML Transformation Style Sheet |
| .zi | Renamed Zip File |

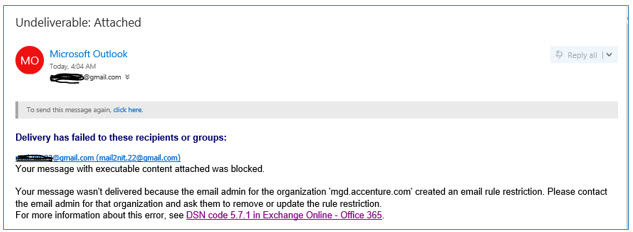
**Options to Send the Message:** If it is a requirement to send executable content, please add the file to a password protected .zip file before attaching it to your message.

For zipping the file please find the steps defined at [link](https://in.accenture.com/mycomputer/password-protected-winzip-files/)

**Screenshot of Delivery Failure:** When sending messages to an external recipient or an internal recipient on Exchange Online.



**Screenshot of Delivery Failure:** When sending messages to a recipient not on Exchange Online.



**Emails with certain extension in attachment block:** <https://in.accenture.com/mycomputer/delivery-failure-in-case-of-blocked-executable-file-types/>

**Zipping and password protecting email attachments:** <https://in.accenture.com/mycomputer/password-protected-winzip-files/>

# Emails blocked due to spoofing

As per updated e-mail security policy, the use of @accenture.com as a sender domain is restricted to internal services including Accenture user mailboxes and internally hosted applications. Internally hosted applications are those which are Accenture-managed/owned and behind Accenture firewalls blocking port 25 (SMTP) which means applications must use the Accenture mail gateways to send e-mail.

Accenture SMTP gateways do not allow external mail to route into the Accenture mail system when the From address is using the @accenture.com domain name. This is known as spoofing our email address.

If there is a business need application not hosted internally to send mails will need to be configured to send email from a dedicated subdomain or Use alternative sender domain.

Relevant steps to create subdomain include:

1. Confirm sub-domain is available

2. Request new sub-domain via smtp.accenture.com (include authorized hosts for the SPF record)

3. Request shared mailboxes, if needed

4. Once sub-domain is created, submit request to add as alias to mailboxes (if applicable)

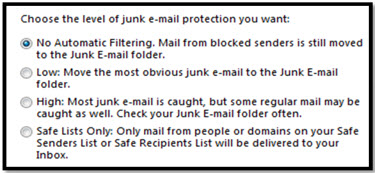
5. Test mailboxes (sending and receiving mail with the new sub-domain)

For spoofing details: <https://mcportal.accenture.com/smtp/SMTPApplicationGuide.pdf>, the application guide has the details on spoofing

# Junk E-Mail filter in Outlook

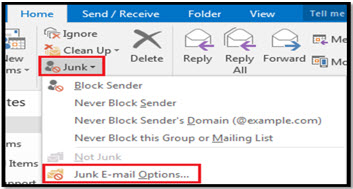
Users sometimes complaint of emails not being received in the inbox, it can be due to the possibility that user at some point of time has marked these senders as not safe or dues to certain setting of junk email.

By default, the Junk Email Filter is turned on and the protection level is set to No Automatic Filtering. You can make the filter more aggressive by changing the level of protection that it provides. The Junk Email Filter evaluates each incoming message based on several factors. These can include the time when the message was sent and the content of the message.



To change the options for the Junk Email Filter, do the following:

**Click Home > Junk > Junk Email Options.**



**Unable to receive emails in inbox due to junk email settings**

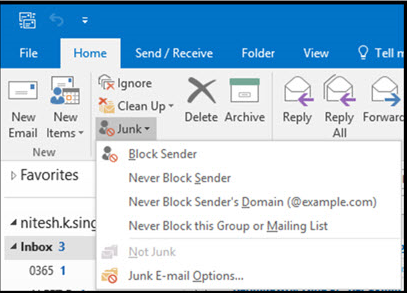
**Steps To Fix The Issue**

Messages from addresses or domain names in the Blocked Senders List are always treated as junk. Outlook moves any detected incoming message from senders in the Blocked Senders List to the **Junk E-mail** folder, regardless of the content of the message.

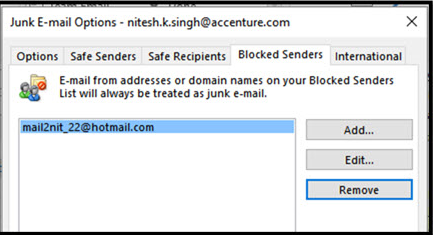
To add a specific sender to the Blocked Senders List, click a message from the sender. On the **Home** tab, in the **Delete** group, click **Junk** and then click **Block Sender**.

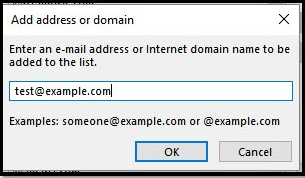
**To add names to the Blocked Senders List:**

1. On the **Home** tab, in the **Delete** group, click **Junk**, and then click **Junk E-mail Options**.



1. On the **Blocked Senders** tab, click **Add**.





1. In the **Enter an e-mail address or Internet domain name to be added to the list** box, enter the name or address that you want to add. For example, you can add:
   * A specific e-mail address, such as [someone@example.com](mailto:someone@example.com)
   * An Internet domain, such as @example.com, or example.com

 Click **OK** and repeat for each entry that you want to add.

**Add trusted names to the Safe Senders or Safe Recipients Lists**

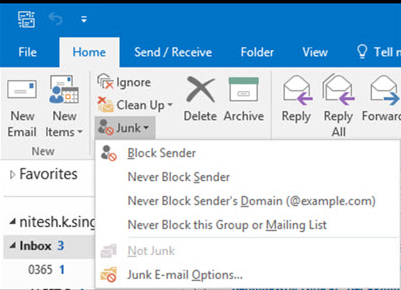
By adding e-mail addresses and domain names that you trust to the Safe Senders List, you instruct Outlook that messages from those sources are never to be considered as junk. If you belong to mailing lists or distribution lists, you can add these names to your Safe Recipients List.

To add a person to the Safe Senders List, click a message from the sender. On the **Home** tab, in the **Delete** group, click **Junk**, and then click **Never Block Sender**.

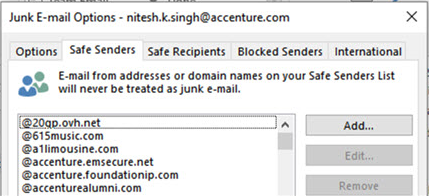
To add a specific address or domain to the Safe Recipients List, click a message from the sender. On the **Home** tab, in the **Delete** group, click **Junk**, and then click **Never Block the Group or Mailing List**.

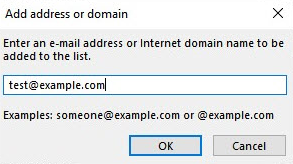
To manually add names or domains to these lists, do the following:

1. On the **Home** tab, in the **Delete** group, click **Junk**, and then click **Junk E-mail Options**.



1. Do one of the following:
   * To add safe senders, on the **Safe Senders** tab, click **Add**.
   * To add safe recipients, on the **Safe Recipients** tab, click **Add**.





1. In the **Enter an e-mail address or Internet domain name to be added to the list** box, enter the name or address that you want to add. For example, you can add:
   * A specific e-mail address, such as [someone@example.com](mailto:someone@example.com)
   * An Internet domain, such as @example.com, or example.com

**All External emails are going to Junk email:**

There will be scenario where all the external emails are going to junk email folder.

Modifications in OWA settings does not resolve this.

Accenture regularly conducts social engineering tests and maintains the Phishing Protection Program (PPP). Individuals are enrolled in PPP when they have failed 3 tests in the past 12 months. While in PPP, all of your external emails will be directed to your junk folder with links and attachments disabled. You will also receive increased testing as additional opportunities to be unenrolled from PPP and additional practice.

**How do I check if I am already enrolled in PPP?**

You can visit [My Phishing Results](https://go.accenture.com/MyPhishingResults) to view your performance on phishing tests.

In case of any further queries user can contact [SafeSenderSupport@accenture.com](mailto:SafeSenderSupport@accenture.com).

Refer the link: <https://in.accenture.com/protectingaccenture/data-security/social-engineering-testing/?referrer=mailer>

Below is a snippet of not passing phishing

