

How to run the Get-MessageTrackingLog cmdlet in Exchange?

Created by Aftab Alam
Just a moment ago • 3 min read • Analytics

- Introduction
- Important points to remember before checking the message logs in Exchange
- How to run the Get-MessageTrackingLog cmdlet in the Exchange Management Shell?
- Practical usage of Message tracking logs
- Conclusion

Introduction

The Exchange Server's robust security measures ensure the continuous integrity of mailboxes, maintaining a consistent state where incoming and outgoing emails are automatically sorted into their respective folders. Typically, managers are relieved from the burden of managing individual emails or monitoring mail flow. However, in exceptional situations, they may find it necessary to inspect message activity within the transport pipeline.

To streamline the process of monitoring mail flow, the Exchange Server maintains a message tracking log accessible via the Exchange Management Shell. This log offers valuable insights, furnishing you with the following essential information:

- Learn what happened to an email message that a user delivered to a certain recipient.
- Determine if a transport rule, sometimes referred to as a mail flow rule, affected a message.
- Check to see if a message that was delivered through the Internet made it into your Exchange organization.
- Find every message that was sent by a certain user during a given time frame.

Important points to remember before checking the message logs in Exchange

- The Administrator account must have additional permissions like Organization Management Role, Records Management Role, and Recipient Management.
- The Microsoft Exchange Transport Log Search service must be active in order to search the message tracking logs. You cannot run delivery reports or check the message tracking logs if you disable or

Kernel Documentation

All content

Blogs +

Space settings

ADVANCED FEATURES

Automation **NEW**

Analytics **PREMIUM**

Content manager...

Calendars **PREMIUM**




SHORTCUTS



No shortcuts in this space

CONTENT

No content in this space

Kernel Documentation / How to run the Get-MessageTrackingLog c...

 Summarize
 

[Share](#)


terminate this service. However, disabling this service has no impact on Exchange's other functions.

- The Get-MessageTrackingLog cmdlet cannot be used to search the message-tracking log files copied from another Exchange server. Additionally, if you manually save an existing message tracking log file, the query logic that Exchange uses to search the message tracking logs is broken due to the change in the file's date-time stamp.
- Message tracking logs on Exchange 2013 Mailbox servers and Exchange 2010 Hub Transport servers in the same Active Directory site may be searched using the Get-MessageTrackingLog cmdlet in Exchange 2016. The message tracking logs on Exchange 2016 and Exchange 2013 Mailbox servers inside the same Active Directory site may be searched using the Get-MessageTrackingLog cmdlet in Exchange 2019.

How to run the Get-MessageTrackingLog cmdlet in the Exchange Management Shell?

After launching the Exchange Management Shell as the Administrator, you have several options for running the Get-MessageTrackingLog command.

- The basic usage of the cmdlet is the following-

```
1 Get-MessageTrackingLog
```

It will bring the first 1000 recent message log entries from the single server.

- For getting some specific entries from a specific time frame, you can input the cmdlet a little differently.

```
1 Get-MessageTrackingLog -ResultSize Unlimited -Start "3/28/2015 8:00AM" -End "3/28/2015 5:00PM"
```

The results will bring a list of emails sent from the given sender between a start and end date.

- Various events in Exchange require a quick glance, and you can check them using another cmdlet.

```
1 Get-MessageTrackingLog [-Server <ServerIdentity>] [-ResultSize <Integer> | Unlimited] [-Start <StartDateTime>] [-End <EndDateTime>] [-Mailbox <MailboxName>] [-MessageId <MessageId>] [-MessageSubject <MessageSubject>] [-MessageBody <MessageBody>] [-MessageAttachments <MessageAttachments>] [-MessageSize <MessageSize>] [-MessageStatus <MessageStatus>] [-MessageSubject <MessageSubject>] [-MessageBody <MessageBody>] [-MessageAttachments <MessageAttachments>] [-MessageSize <MessageSize>] [-MessageStatus <MessageStatus>]
```

Invite people

All content

Blogs +

Space settings

ADVANCED FEATURES

Automation NEW

Analytics PREMIUM

Content manager...

Calendars PREMIUM

SHORTCUTS +

No shortcuts in this space

CONTENT +

No content in this space

Practical usage of Message tracking logs

Message tracking logs can play a good part in solving different purposes of a business-

- **Resolving email delivery issues:** message monitoring logs can provide information about why a message wasn't delivered if it arrived late, and more. Especially it may create several issues, such as whether Exchange cannot open the mailbox or show some specific errors.
- **Statistics:** Every communication that passes via your servers is tracked in message tracking logs. How many messages were processed or who sent the most messages inside the firm are two examples of data that can be obtained relatively easily for analysis.
- **Forensics:** You don't have an email backup, and someone deletes an email. Even worse, your rival firm received an email that included private information. Message monitoring logs can help you in this situation by giving you useful email-related information.
- **Litigation:** similar to the preceding circumstance, it is frequently employed When a message-tracking record is needed as evidence in court.

Conclusion

If you're attempting to access message tracking logs for deleted messages and exploring methods for their recovery, it's advisable to review the retention policies configured within your organization. However, relying solely on manual techniques for retrieving deleted messages may not yield satisfactory results. For more effective recovery of deleted and corrupted items, consider utilizing specialized software like [Kernel for Exchange Server](#).

The software boasts a comprehensive recovery capability, effortlessly restoring emails, contacts, calendars, notes, and various other critical details. It seamlessly reinstates the lost items to their original positions, precisely where they resided before deletion. Its adaptive functionality ensures successful [retrieval of deleted mailboxes in both Exchange 2010](#) and more recent iterations, offering a versatile and dependable solution.

+ Add label

Invite people