

Track Messages in Office 365

Last Modified on 23/01/2020 2:28 pm GMT

At times, you may need to find out what happened to an email that was processed by the Office 365 service. Exchange Online provides the ability to trace messages for up to 90 days from the date they were processed.

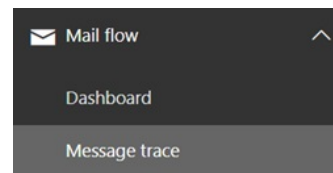
Start a Message Trace

Message traces can be started in the Security & Compliance Center for the Office 365 tenant you wish to trace on.

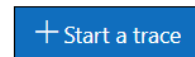
1. Log into the tenant's Office 365

Security & Compliance Center using global admin details:

<https://protection.office.com>



2. Go to 'Mail Flow > Message trace'
3. Select **Start a trace**



4. Select the conditions for search you want to perform:

- By these people – the email address or user that sent the email
- To these people – The email address(es) or user(s) who received the emails
- Within this time range – The timescale to perform the search against

A screenshot of the 'New message trace' form in the Security & Compliance Center. The form has a dark header with the title 'New message trace'. Below the header, there are several sections: 'Find messages that were sent:' with a help icon; 'By these people' with a text input field and a clear button; 'To these people' with a text input field and the text 'All recipients'; 'Within this time range (UTC+01:00) - DST' with a help icon, a 'Slider' control, and a 'Custom' link; a time range slider with markers for 90, 30, 15, 10, 7, 2, 1 day, 12 hr, 6 hr, and 0; a 'More search options' dropdown; and a 'Choose report type' dropdown with 'Summary report' selected. At the bottom, there are three buttons: 'Search', 'Save', and 'Cancel'.

5. Press **Search**

Note: If you attempt to perform a search that goes back past 10 days, your trace will be requested and you will need to return back to download it once it has completed. An email notification will be sent to confirm once this has completed.

Understanding Message Traces

Message traces can show a lot of information about an email. Some of the information that may not be immediately obvious is described below.

Message Status

Status	Meaning
Delivered	The email was delivered to the specified mailbox or recipient server
Pending	The email has not yet been delivered – The delivery will be re-attempted
Expanded	The email was sent to a group and was distributed to that group's members
Failed	The email was not delivered – The Message Events will show more information
Filtered as Spam	The email was handled as spam – Depending on your settings, this will either be routed to Junk or rejected
Quarantined	The email is held by the Exchange Online Quarantine service and is pending release
Getting Status	The email is still being processed by Office 365, the status will be updated shortly – The email may have already been delivered

Message Events

Event	Meaning
Receive	The email was received for processing by the Exchange Online service
Send	The email was sent on by the Exchange Online service
Fail	The email could not be passed on to the next step – An error message will confirm the reason for this

Deliver	The email was delivered to the recipient mailbox
Expand	The email was sent to a group and was distributed to that group's members
Defer	The email delivery was delayed – An error message will show the reason for the delay
Resolved	The recipient address was updated – Generally occurs when an email is sent to an alias

More Information

Field	Meaning
Message ID	A unique identifier for the email
From IP	The IP address of the source of the email as it is passed to Office 365
To IP	The IP address of the next hop the email was passed to

Note: *Message traces can also be ran via Exchange Admin Centre > Mail Flow.*