Revocation of Email Protected by Office 365 Message Encryption

Posted on [**October 26, 2020**](https://office365itpros.com/2020/10/26/ome-revoke-message/) by [**Tony Redmond**](https://office365itpros.com/author/thoughtsofanidlemind/)

OWA Gets Remove External Access Feature

Office 365 notification MC216367 (updated August 27) announced that end users would be able to revoke messages protected by Office 365 Message Encryption (OME) if they are eligible for the advanced form of OME, licensed through Office 365 E5 or other licenses (like Microsoft 365 E5 compliance). OME allows users to encrypt or mark messages with *Do Not Forward* using OWA and Outlook desktop. Microsoft automatically enables OME for all Office 365 tenants with E3 or above licenses.

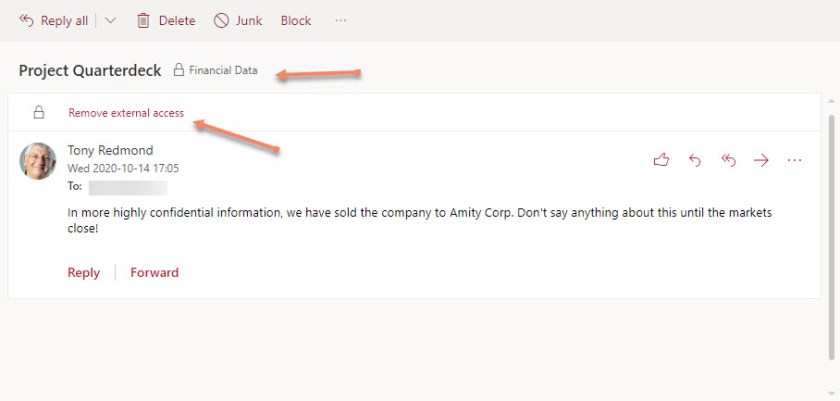
The new feature means that after you send a revocable message, you can use the **Remove external access** option to revoke access to the message (Figure 1). This feature is only available in OWA and only works for some external recipients (see below), but it’s still a nice option to have if you suddenly need to withdraw access to sensitive content that’s been distributed outside your tenant.

Graphical user interface, text, application, email

Description automatically generated

Figure 1: The Remove external access option in OWA for a protected message

In addition to being able to revoke messages sent with the standard OME Encrypt-Only or Do Not Forward protection, the Remove external access feature also works for messages with an [**Office 365 sensitivity label**](https://petri.com/using-office-365-sensitivity-labels), which can use rights management based encryption to secure access to content. Figure 2 shows a message protected by the *Financial Data* sensitivity label. Revoking access for external recipients works in the same way.

Figure 2: Remove external access for a message protected by a sensitivity label

After the message is revoked, the OWA message header is changed to confirm that external access has been removed. At this point, any attempt by the recipient to open the content will be declined because “*this message has been revoked by the sender.*”

What Messages Can be Revoked

Revocation only works for external recipients. You can’t revoke a message delivered to recipients in your tenant. OME divides external recipients into two categories:

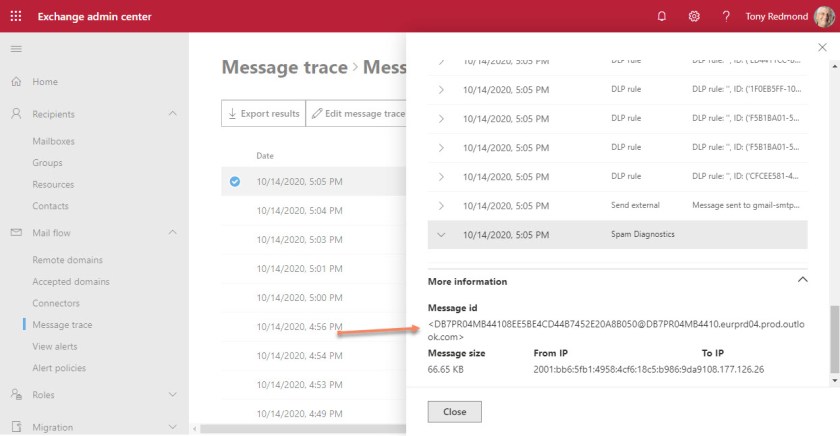
* Accounts in Office 365 domains and Outlook.com: You can’t revoke messages delivered to these recipients.
* Accounts in any other domain: Messages sent to these recipients can be revoked because the actual message is not delivered to their mailboxes. Instead, they receive a notification directing them to the OME portal. These notifications are called link-based messages. Recipients must authenticate with the OME portal by signing in or using a one-time passcode to access the protected content.

Revocation is possible for link-based messages because you can guarantee to block access at the OME portal. Revocation of messages delivered to other Office 365 domains or Outlook.com would require the ability to interfere with mail flow in those domains, and that’s not possible today.

Administrator Revocation

Prior to this development, protected messages could only be revoked by administrators using PowerShell or the [**Message encryption report**](https://protection.office.com/reportv2?id=EncryptionReport) in the compliance center. As the message encryption report is usually a few days behind real time and the need to retrieve sensitive information often makes revocation something that happens “now,” the best approach is to run a message trace in the new Exchange admin center (EAC) or the old Security and compliance center to find the message identifier and then revoke it with PowerShell.

Figure 3 shows the results of a message trace in the new EAC. After finding the message we want to revoke, we can check its properties to find the message identifier.

Figure 3: Finding the identifier for a message we want to revoke

After saving the message identifier, we can use it with the *Get-OMEMessageStatus* cmdlet to check if it can be revoked (see below).

**$msgId** = "DB7PR04MB44108EE5BE4CD44B7452E20A8B050@DB7PR04MB4410.eurprd04.prod.outlook.com"

Get-OMEMessageStatus -MessageId **$MsgId**

ObjectState : New

Container : SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}@office365itpros.onmicrosoft.com

Subject : Project Quarterdeck

ReceivedTime : 01/01/0001 00:00:00

Revoked : False

IsRevocable : True

In this case, the IsRevocable flag is True, so we can go ahead and revoke using the *Set-OMEMessageRevocation* cmdlet:

Set-OMEMessageRevocation -Revoke **$True** -MessageId **$MsgId**

The encrypted email with subject "Project Quarterdeck" and Message ID "DB7PR04MB44108EE5BE4CD44B7452E20A8B050@DB7PR04MB4410.eurprd04.prod.outlook.com" was successfully revoked.

Running *Get-OMEMessageStatus* for the message will now show that the Revoked property has changed from False to True and the recipient will no longer have access to the content.

One irritation is that *Get-OMEMessageStatus* shows that these messages can be revoked and you can try to revoke them with *Set-OMEMessageRevocation* (which tells you that the revocation is successful), but recipients will still have access to the messages. I guess the cmdlet can’t tell the difference between messages sent by link and those which go direct