# TTP Detail – T1098.002

## TTP Information

Name: Additional Email Delegate Permissions

Description: Adversaries may grant additional permission levels to maintain persistent access to an adversary-controlled email account.

For example, the <code>Add-MailboxPermission</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlet, available in on-premises Exchange and in the cloud-based service Office 365, adds permissions to a mailbox.(Citation: Microsoft - Add-MailboxPermission)(Citation: FireEye APT35 2018)(Citation: Crowdstrike Hiding in Plain Sight 2018) In Google Workspace, delegation can be enabled via the Google Admin console and users can delegate accounts via their Gmail settings.(Citation: Gmail Delegation)(Citation: Google Ensuring Your Information is Safe)

Adversaries may also assign mailbox folder permissions through individual folder permissions or roles. In Office 365 environments, adversaries may assign the Default or Anonymous user permissions or roles to the Top of Information Store (root), Inbox, or other mailbox folders. By assigning one or both user permissions to a folder, the adversary can utilize any other account in the tenant to maintain persistence to the target user’s mail folders.(Citation: Mandiant Defend UNC2452 White Paper)

This may be used in persistent threat incidents as well as BEC (Business Email Compromise) incidents where an adversary can add [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003) to the accounts they wish to compromise. This may further enable use of additional techniques for gaining access to systems. For example, compromised business accounts are often used to send messages to other accounts in the network of the target business while creating inbox rules (ex: [Internal Spearphishing](https://attack.mitre.org/techniques/T1534)), so the messages evade spam/phishing detection mechanisms.(Citation: Bienstock, D. - Defending O365 - 2019)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

## APTs (Intrusion Sets)

* APT28
* APT29
* Magic Hound