

Impersonation and EWS in Exchange

📅 11/16/2014 ⌚ 2 minutes to read Contributors 🗨️ 👤

In this article

[Security considerations for impersonation](#)

[In this section](#)

[See also](#)

Learn how and when to use impersonation in your Exchange [service applications](#).

You can enable users to access other users' mailboxes in one of three ways:

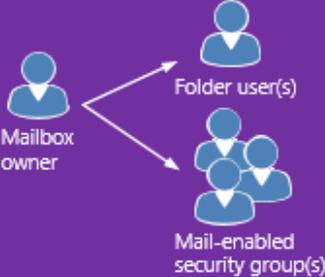
- By adding delegates and specifying permissions for each delegate.
- By modifying folder permissions directly.
- By using impersonation.

When should you choose impersonation over delegation or folder permissions? The following guidelines will help you decide:

- Use folder permissions when you want to provide a user access to a folder but do not want the user to have "send on behalf of" permissions.
- Use delegate access when you want to give one user permission to perform work on behalf of another user. Typically, this is a one-to-one or one-to-a-few permission - for example, a single administrative assistant managing the calendar for an administrator, or a single room scheduler managing the calendars for a group of meeting rooms.
- Use impersonation when you have a service application that needs to access multiple mailboxes and "act as" the mailbox owner.

Impersonation is the best choice when you're dealing with multiple mailboxes because you can easily grant one service account access to every mailbox in a database. Delegation and folder permissions are best when you're only granting access to a few users, because you have to add permissions individually to each mailbox. Figure 1 shows some of the differences between each type of access.

Figure 1. Ways to access other users' mailboxes

Mailbox access	Relationship	Type of permission
Delegation	 Mailbox owner → Delegate(s)	Send on behalf of
Delegation plus folder permissions		Send on behalf of plus custom folder permissions
Folder permissions	 Mailbox owner → Folder user(s) Mailbox owner → Mail-enabled security group(s)	Edit, delete, create folders and items No send permissions
Impersonation	 Mailbox owners → Service account	Send as

Impersonation is ideal for applications that connect to Exchange Online, Exchange Online as part of Office 365, and on-premises versions of Exchange and perform operations, such as archiving email, setting OOF automatically for users on vacation, or any other task that requires that the application act as the owner of a mailbox. When an application uses impersonation to send a message, the email appears to be sent from the mailbox owner. There is no way for the recipient to know the mail was sent by the service account. Delegation, on the other hand, gives another mailbox account permission to act on behalf of a mailbox owner. When an email message is sent by a delegate, the "from" value identifies the mailbox owner, and the "sender" value identifies the delegate that sent the mail.

Security considerations for impersonation

Impersonation enables a caller to impersonate a given user account. This enables the caller to perform operations by using the permissions that are associated with the impersonated account, instead of the permissions that are associated with the caller's account. For this reason, you should be aware of the following security considerations:

- Only accounts that have been granted the **ApplicationImpersonation** role by an Exchange server administrator can use impersonation.
- You should create a management scope that limits impersonation to a specified group of accounts. If you do not create a management scope, the **ApplicationImpersonation** role is granted to all accounts in an organization.

- Typically, the **ApplicationImpersonation** role is granted to a service account dedicated to a particular application or group of applications, rather than a user account. You can create as many or as few service accounts as you need.

You can read more about [configuring impersonation](#), but you should work with your Exchange administrator to ensure that the service accounts that you need are created with the [permissions and access](#) that meet the security requirements of your organization.

In this section

- [Configure impersonation](#)
- [Identify the account to impersonate](#)
- [Add appointments by using Exchange impersonation](#)

See also

- [Develop web service clients for Exchange](#)
- [Delegate access and EWS in Exchange](#)
- [Exchange 2013 Permissions](#)