Exchange Connector 5.0.0 (Impersonation Connector)

Overview

Our past Exchange connector product experienced throttling issues when deployed in Exchange Online and Exchange 2010(or newer) on-premises environments. The throttling has resulted in RoomWizards intermittently showing Connector communication losses which result in the RoomWizard being unable to show bookings and Users being unable to update or end meetings.

Overall, the RoomWizard experience has been diminished substantially for customers using Exchange Online and Exchange 2010(or newer).

Why Throttling Affects the Exchange Connector

The Exchange Connector leverages Microsoft's EWS Managed API, which ultimately makes outbound requests (connections) to Exchange Web Services. In order to make requests to an Exchange Web Service, the requests must be authenticated and made on behalf of an Exchange User.

The connector is configured with an Exchange User – which has been historically called a "service user" – that has read/write access to an organization's Resources.

In the event that the Service User is making outbound requests to multiple Resource Mailboxes at approximately the same time, it is likely that the Service User will be throttled by the web service resulting in temporary loss of communication between our Connector and the RoomWizard.

The fundamental issue is that our current connector does not scale effectively, because it is bounded by a throttling limitation of open connections by Exchange.

Application Impersonation

By using the Impersonation Connector, there is the potential that access may be granted to personal information beyond the scope of RoomWizard. As a result, Room Names used to reflect the RoomWizards must be validated as part of the setup process. This validation needs to ensure that only Rooms supported by the RoomWizard are included in the csv file used to import the names of the rooms when installing and configuring the Connector. Please see Installation and Configuration Guide for further details on the csv file and importation steps.

If an individual is listed in error in the csv file, RoomWizard will in turn be granted the access to impersonate that individual. Proper validation of the csv will remove the risk of an individual being impersonated by RoomWizard.

The only way to get around the current connection limitation is to utilize Exchange's *Application Impersonation* that enables an account to make outbound connections on-behalf of a different User or Resource within Exchange.

Leveraging *Impersonation* ensures that throttling quotas are not counted against the User or Resource being impersonated instead the Service User. For example; if there are multiple resources that are being queried and individual Exchange throttling limits would normally be exceeded, the Service User now actually counts as only one connection as far as Exchange is concerned but can represent "Impersonation" of ~~the~~ multiple resources and avoid the throttling limit.

Microsoft's point of view on Impersonation and EWS in Exchange

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.

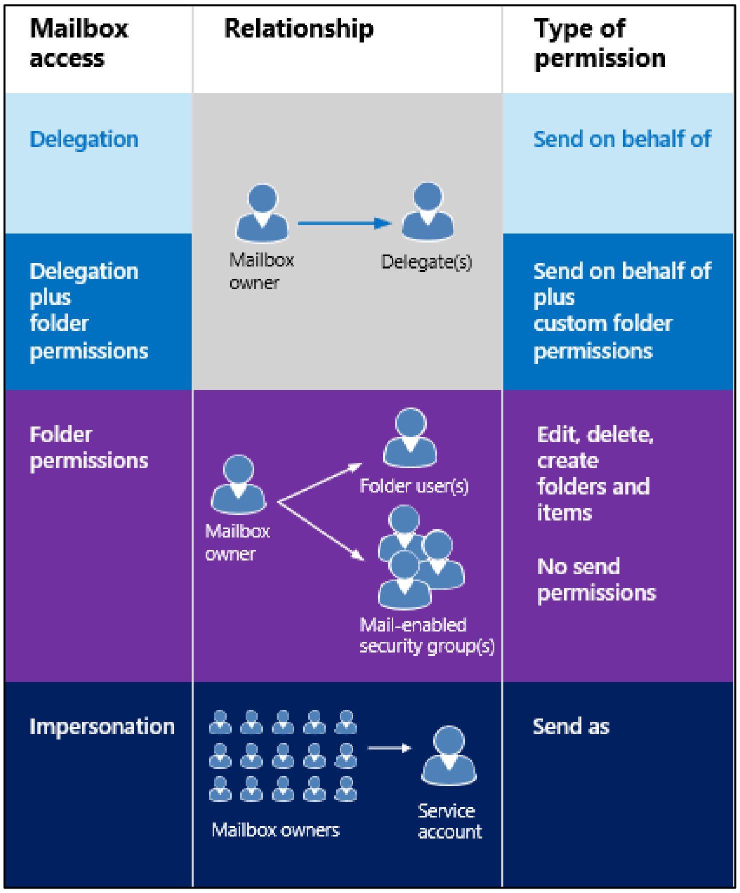
When should you choose impersonation over delegation or folder permissions? The following guidelines will help you decide:

- 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.

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) 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 to 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 application impersonation

While unlimited *Application Impersonation* can be used, some sites might find that they are more comfortable restricting the scope of the Resources that can be "Impersonated". A means to do this is provided by creating a Scoped Impersonation based on Naming Pattern. More information on this is provided in the installation instructions for this connector.

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. Read more at: https://msdn.microsoft.com/en-us/library/office/dn722377(v=exchg.150).aspx