Please Note: We no longer support local Outlook client configurations on remote systems for anyone outside our domain. We have experienced various sync issues with these setups and users (i.e. clergy, etc.) at the various parishes have a hard time troubleshooting them for one reason or another. Should you choose to try and configure a local Outlook client to connect to an arch e-mail account from a remote location, please beware we will not be able to offer any troubleshooting support or guidance and recommend accessing the account remotely only by the options below

We are still an on-prem Exchange environment. When attempting to setup access to an arch e-mail account using a local Outlook client for a remote user (i.e. parish clergy, etc.), the following information is needed. We now recommend accessing the AoA email accounts via webmail or a mobile device. Below are some helpful links should you choose to go that route.

Outlook Client Settings (ex: John Doe):

User name format: AOA-INT\jdoe

Sever: webmail.archatl.com

Email address: jdoe@archatl.com

Outlook Web App:

https://support.archatl.com/index.php?/Knowledgebase/Article/View/3/2/using-the-outlook-web-app

AoA Email Account setup for Mobile Devices:

https://support.archatl.com/index.php?/Knowledgebase/Article/View/15/2/windows-email-setup-for-mobile

It is recommended that if your user name and password for your AoA account is stored in Windows Credential Manager, delete all instances of it then setup the Outlook client from scratch.

Lastly, if a password reset is needed, we can provide a new password for the AoA account (which may involve our department needing to work directly with the end user for verification purposes). If necessary, the user may need to provide us with a phone number that the Archbishop's office has on file and we will contact him via phone at a convenient date and time. It is also recommended that if a new password is needed, all instances of this account be removed from all mobile devices and anywhere else the credentials may be stored BEFORE we reset the password. This must happen or the devices with the old password will continually try to authenticate using the old credentials and will lock out the account after several incorrect attempts to connect.