MoxiWorks

MoxiEngage Integration Process using Exchange 2016

Introduction

Don't panic! This setup has been completed by hundreds of individuals with no previous experience in setting up email accounts and/or credentials. This document includes screenshots of of the entire process, step-by-step. You got this!

Use the links below to jump to a particular MoxiEngage integration set-up step:

If you have questions or concerns, please check out our Tips and Further Info!

Overview

MoxiEngage integrates directly with your brokerage's Exchange 2016 account to provide your agents and support staff with consistent and convenient access to their information, while eliminating any need to enter the same information multiple times.

MoxiEngage relies upon Exchange application impersonation access to synchronize data and perform actions on behalf of individual users. Each MoxiEngage user account has an email address that corresponds to a mailbox on your Exchange 2016 account. All integration actions are performed within the context of a single given mailbox. MoxiEngage never requires administrative access to your Exchange 2016 account.

Contacts

MoxiEngage continually synchronizes a user's contacts and contact details with the Exchange 2016 mailbox. Contacts created in Exchange 2016 will appear in MoxiEngage. Contacts created in MoxiEngage are synchronized back to the Exchange 2016 mailbox.

Calendar

MoxiEngage displays the user's calendar events and appointments. Calendar events and appointments can also be added through MoxiEngage and are synchronized to the Exchange 2016 mailbox.

Email

MoxiEngage sends certain email messages through user's mailbox. These email messages will appear in the Sent mail folder and will be delivered to the recipient from the mailbox just as if the user had sent the email from Exchange 2016 directly. MoxiEngage does not synchronize or inspect incoming email messages.

MoxiWorks

Service Account Setup

MoxiEngage is designed to utilize service account credentials for organizations that use Exchange 2016 for administration of the company's email functions.

An email administrator in your company organization will need to perform steps to create a service account and obtain the necessary credentials for MoxiEngage to use.

Refer to Exchange 2016 Setup Instructions for Administrators in this document and follow the step-by-step instructions to set up a service account with application impersonation using basic authentication and a password that will not expire.

You will need to provide the service account email address and non-expiring password, along with a regular user email address that we can use for testing.

Information Gathering

To enable configuration of the MoxiEngage integration, we will need to gather some key information and credentials from you, including the service account credentials created by following the steps in the Exchange 2016 Setup Instructions for Administrators section of this document.

Next Steps

Verification of Credentials

MoxiWorks staff will begin the next step of the integration process. We will test the credentials you provided to verify that the service account is able to connect to your email service and perform a synchronization for the test email address you supplied.

Outcome: Credentials Cannot be Verified

If your entered credentials cannot be verified, we will contact you. Your email administrator will need to resolve the issue and then you will provide us with the updated information.

Outcome: Credentials are Verified Successfully

If your credentials are verified successfully, we will store the credentials securely. Congratulations! This is a key milestone that enables us to continue the process of getting MoxiEngage enabled for your brokerage.

Security

MoxiWorks requires the use of a single username/mailbox on your Exchange 2016 instance, configured as a service account with the Application Impersonation role. All interactions between the MoxiWorks system and your user's mailboxes happens through this designated impersonation account. MoxiEngage never requires administrative access to your Exchange 2016 instance.

Network Access

MoxiWorks systems communicate directly with Exchange 2016 servers over secure HTTPS/SSL connections.

MoxiWorks

Managing Shared Secrets and Credentials

For automated access, MoxiWorks makes use of methods native to our configuration management software. Credentials are stored in encrypted objects accessible only to servers with the relevant service role and environment. These credentials are pulled and decrypted during software deployment. Server identity is validated via pre-shared public/private key. Credentials are managed through a commercial password manager and any non-automated access is limited to the MoxiWorks Technical Operations team and, with customer approval, limited support personnel on an as-needed basis. See also:

https://docs.chef.io/secrets.html#encrypt-a-data-bag-item

https://www.lastpass.com/en/enterprise

Communications Policy for Security Breaches

In the unlikely event of a security breach where client data such as account credentials for registrar management, impersonation credentials, and the like may have been compromised, MoxiWorks Technical Operations and/or Account Management staff will notify affected clients. If the client is aware of a potential security breach, they should notify MoxiWorks immediately so that we may contain and mitigate potential risk in a timely manner. In either case, a change to Impersonation account credentials will be coordinated between both parties.

Exchange 2016 Setup Instructions for Administrators

The following steps describe the recommended process for creating a service account in Exchange 2016 with the Application Impersonation role for use with your brokerage's MoxiWorks integration. Special consideration must be given to ensure the service account user has a password that never expires. The service account user must also be allowed to connect to Microsoft Web Services and Auto Discovery in your Exchange 2016 instance using basic authentication.

Note

If your Exchange 2016 instance is hosted by a third-party vendor (i.e., GoDaddy, etc.), your Admin user interface may not match the instructions provided here. Please contact your email vendor for assistance. Feel free to provide a copy of this document to your vendor as a guide and explanation of what is required.

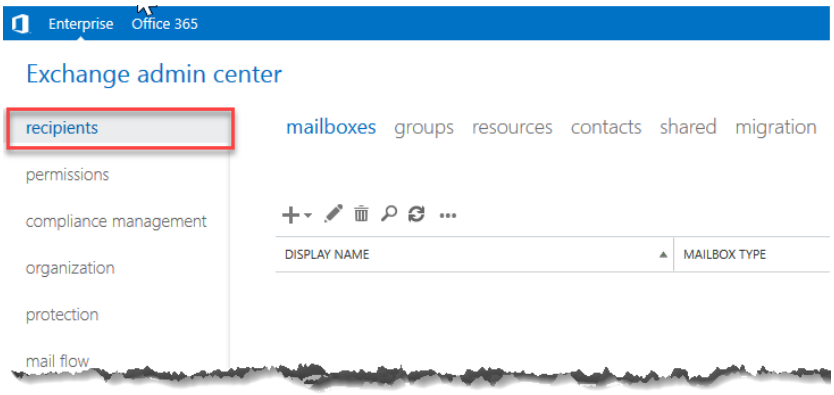
Exchange 2016 menu structure and user interface is subject to change. Steps provided in this document were performed from a computer running Windows 10 Pro against a Exchange 2016 instance created in July 2021.

The instructions provided in this guide are not intended to provide security advice for configuring your Exchange 2016 instance. The documented steps represent the most direct approach available at the time of this writing to achieve the necessary access required by MoxiWorks products. Other methods of configuration may be available.

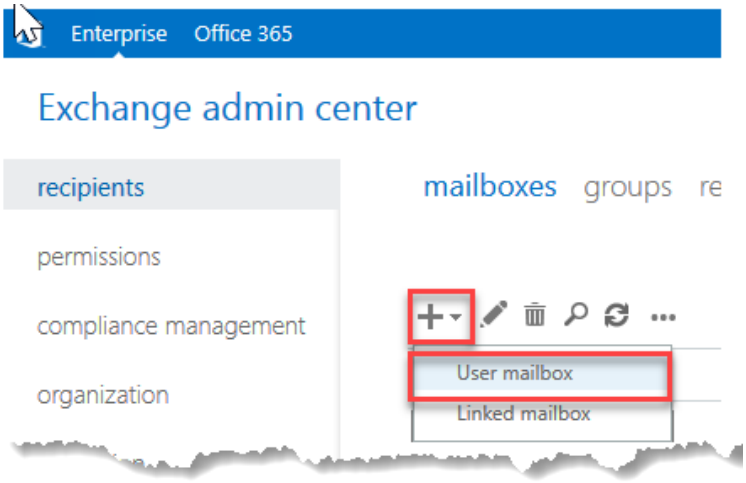
MoxiWorks

Create a Service Account User

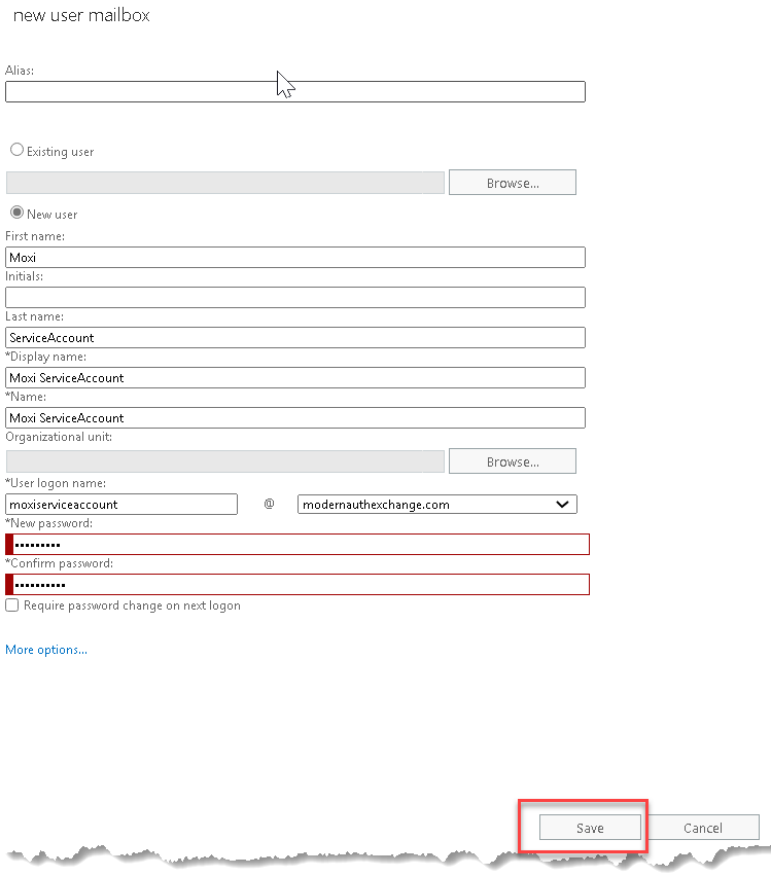
1. Login to your Exchange 2016 Admin Center.
2. Open the Exchange Admin Center and click on ‘recipients’ in the navigation panel. You should see something similar to the screenshot below.



3. Click the + and select the ‘User mailbox’ option to create the new service account. **The service account MUST have a mailbox.**



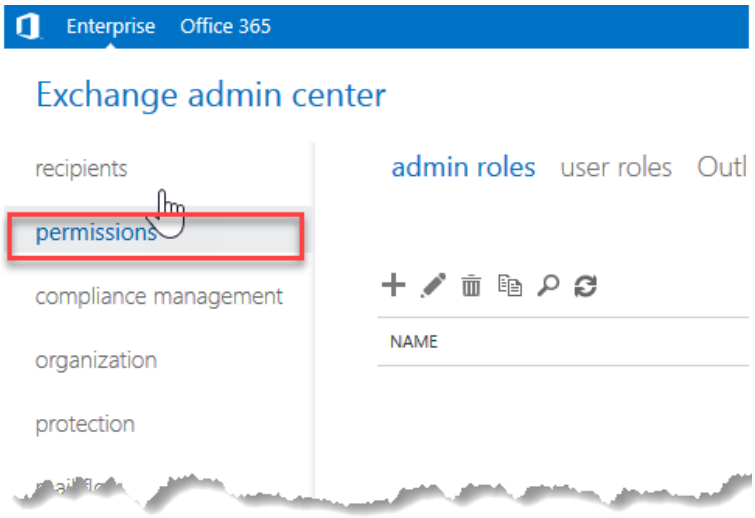
4. Once the form is completed click the ‘Save’ button



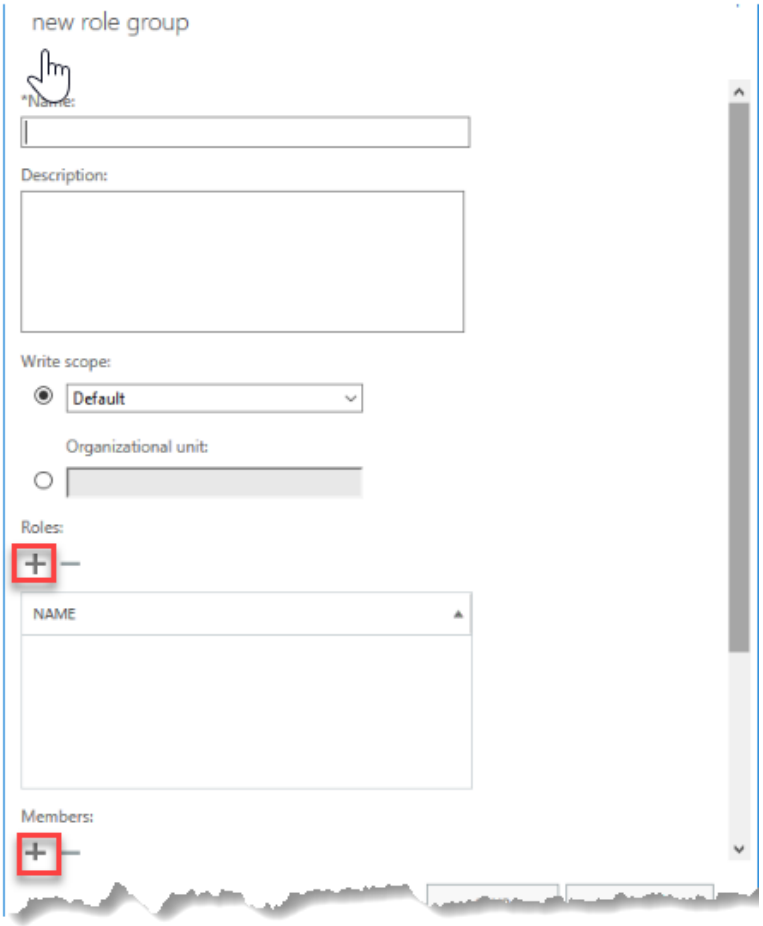
MoxiWorks

Grant Application Impersonation to the Service Account User

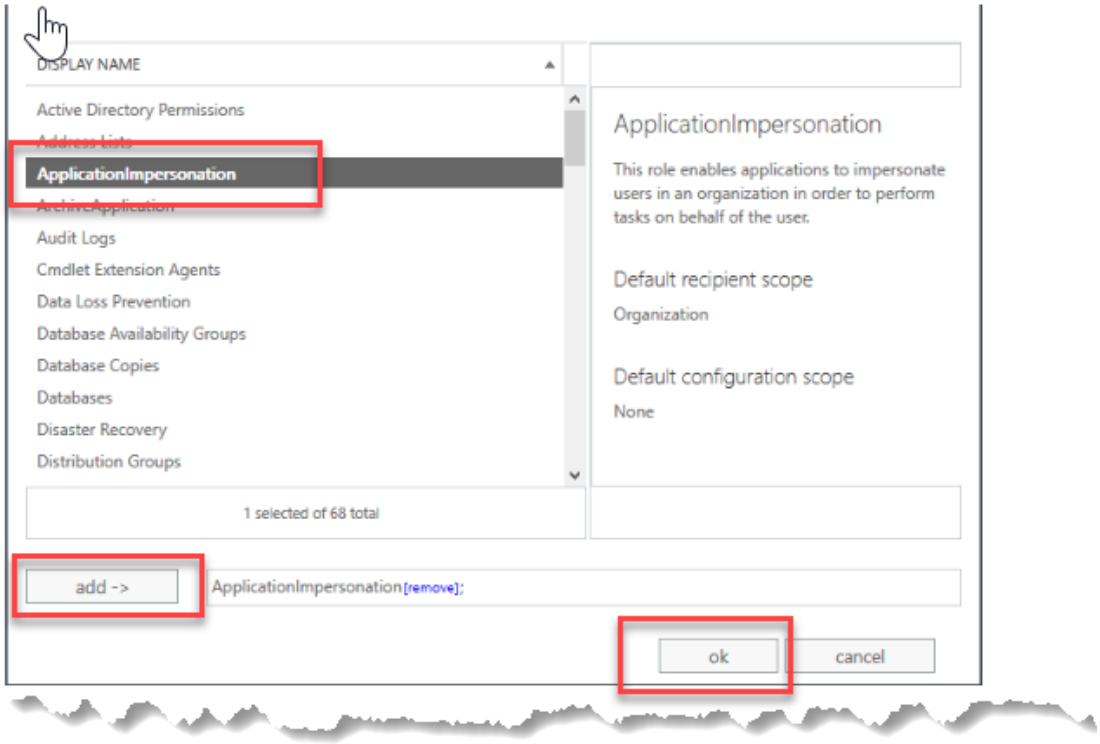
1. Open the Exchange Admin Center and select the ‘permissions’ node as shown in the screenshot below.



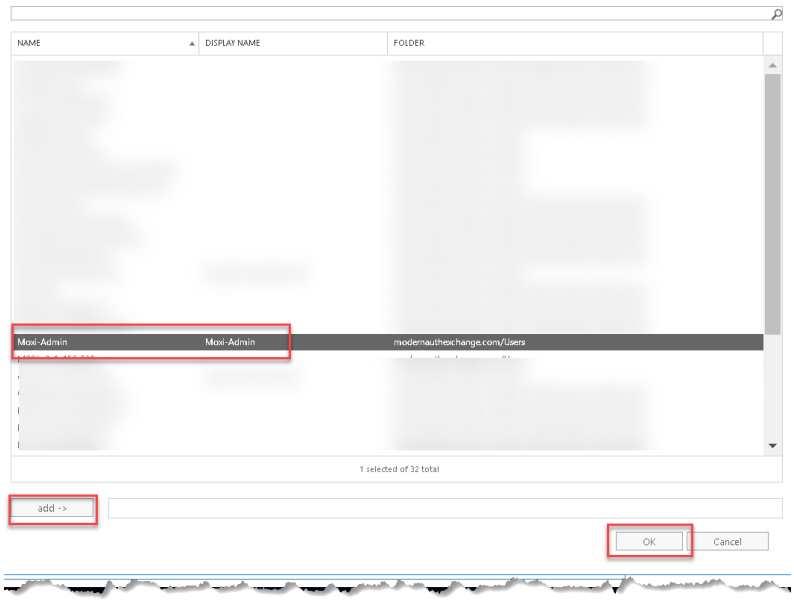
2. Click the + to add a new Role Group. Enter a value for Name and Description. Leave the ‘Write scope’ value set to ‘Default’.



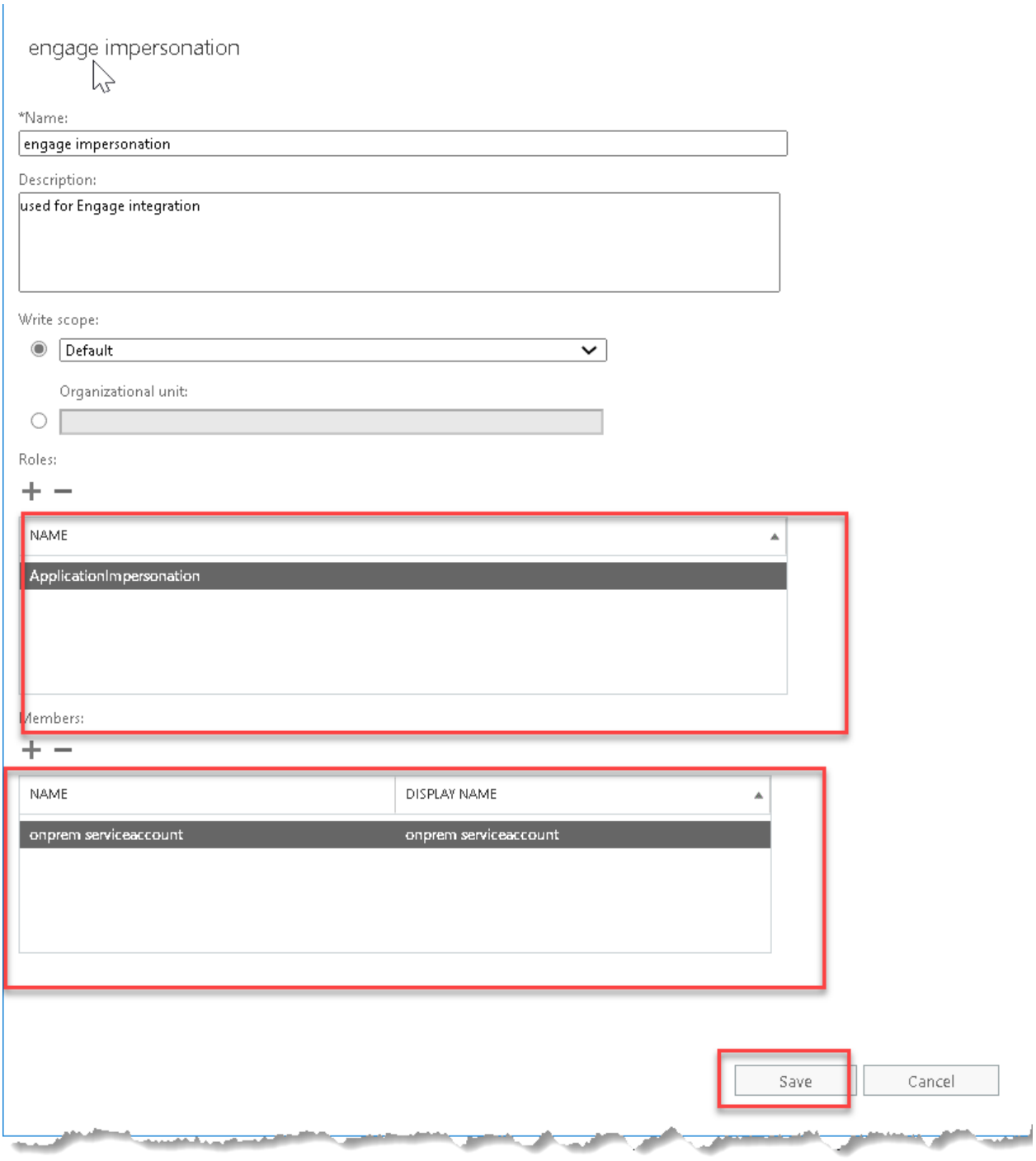
3. Click the + under ‘Roles’ and add ‘ApplicationImpersonation’ as shown below. Click ‘OK’ once it has been added to the list..



4. Click the + under ‘Members’ and add the service account you created in Step 1. Click ‘OK’ once it has been added to the list. Note that unless "all users" or the service account are added to the manged group, the configuration will fail. **This is true even if the Service Account is the owner of the group.** This is because when you add a service account, it tests its ability to impersonate by testing against itself..



5. After completing the form click the ‘Save’ button and the new Role Group should be added to your list.

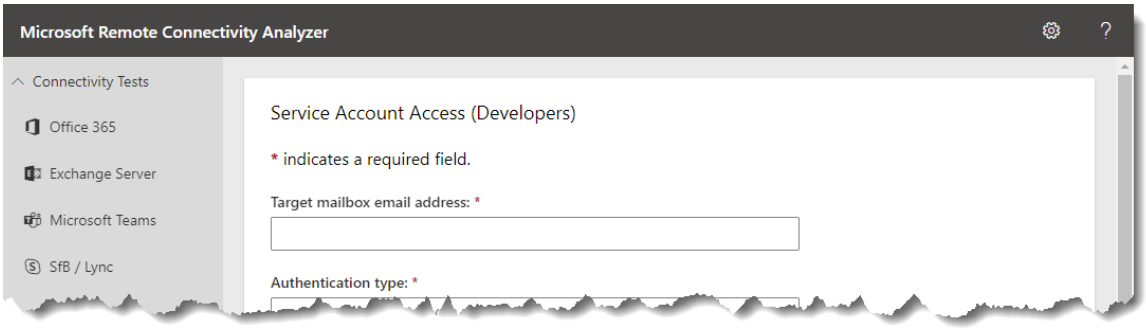


MoxiWorks

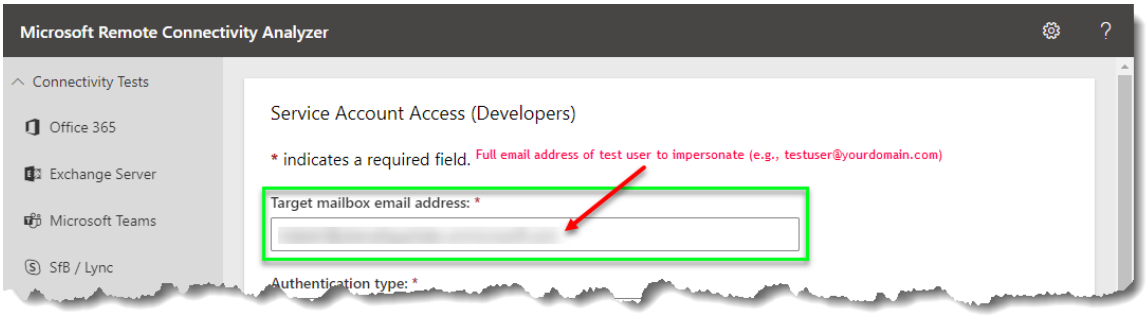
Test Service Account Impersonation for MoxiEngage

It is best practice to test the impersonation role of your MoxiEngage service account before you provide the service account credentials to MoxiWorks. This will prevent delays in your onboarding process. If the impersonation testing fails, additional configuration steps may be required.

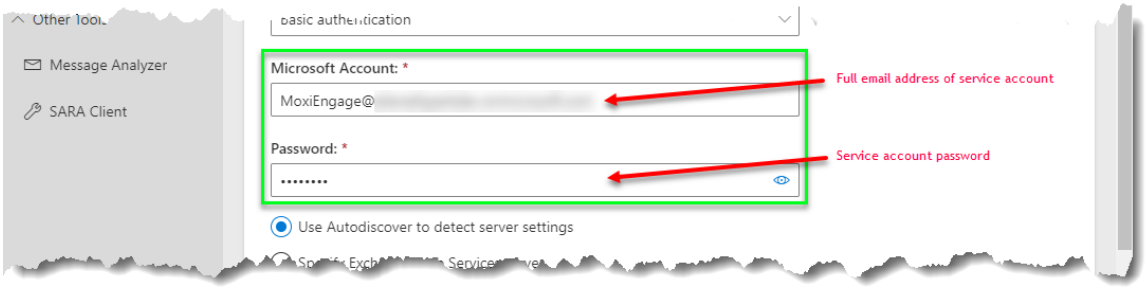
1. Identify a regular (non-administrator) email address in your Exchange 2016 instance. The test will attempt to use the service account to impersonate this user. Be sure that the selected user has logged into Exchange 2016 and accessed Outlook at least one time.
2. In your web browser, navigate to the Microsoft Remote Connectivity Analyzer.



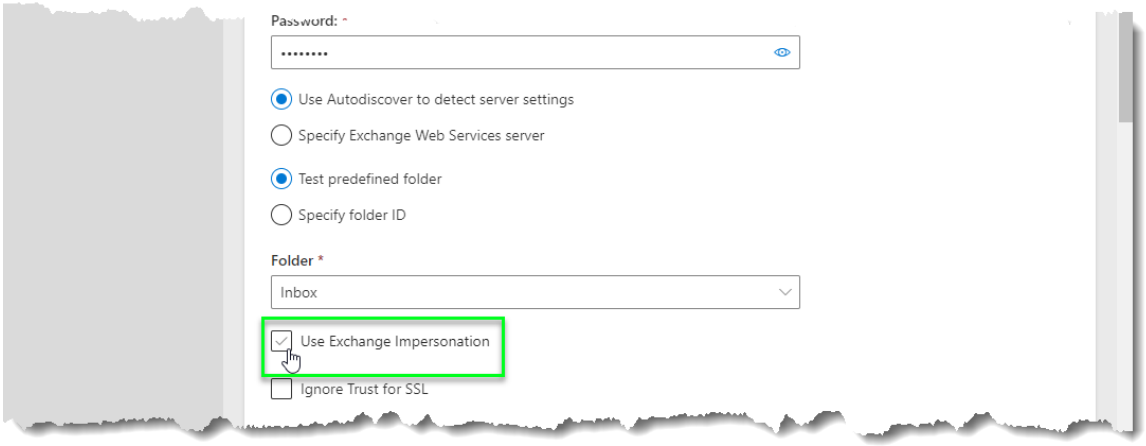
3. Enter the test email address in the “Target mailbox email address” box of the form.



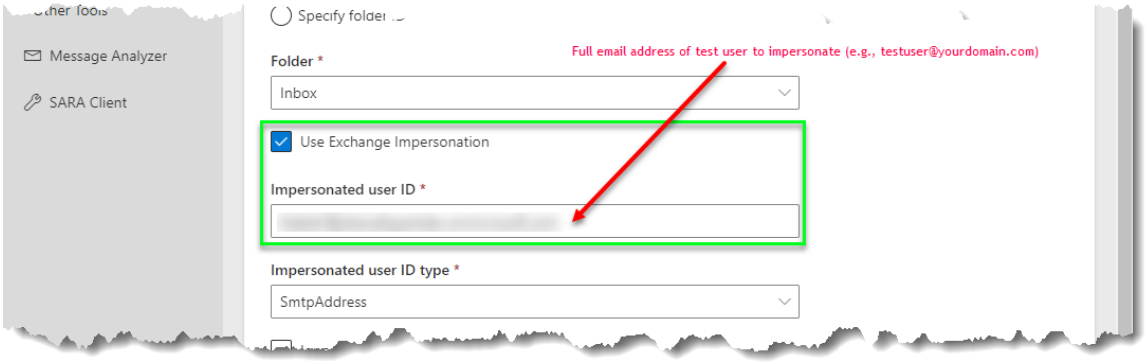
4. Enter the email address of the service account you created for MoxiEngage in the “Microsoft Account” box of the form, then enter the associated password in the “Password” box.



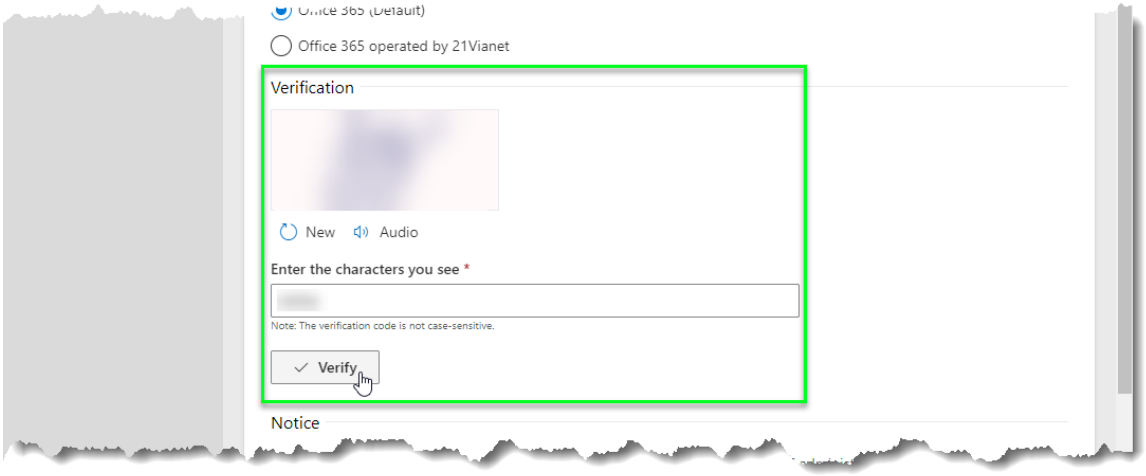
5. Mark the checkbox next to the “Use Exchange Impersonation” label.



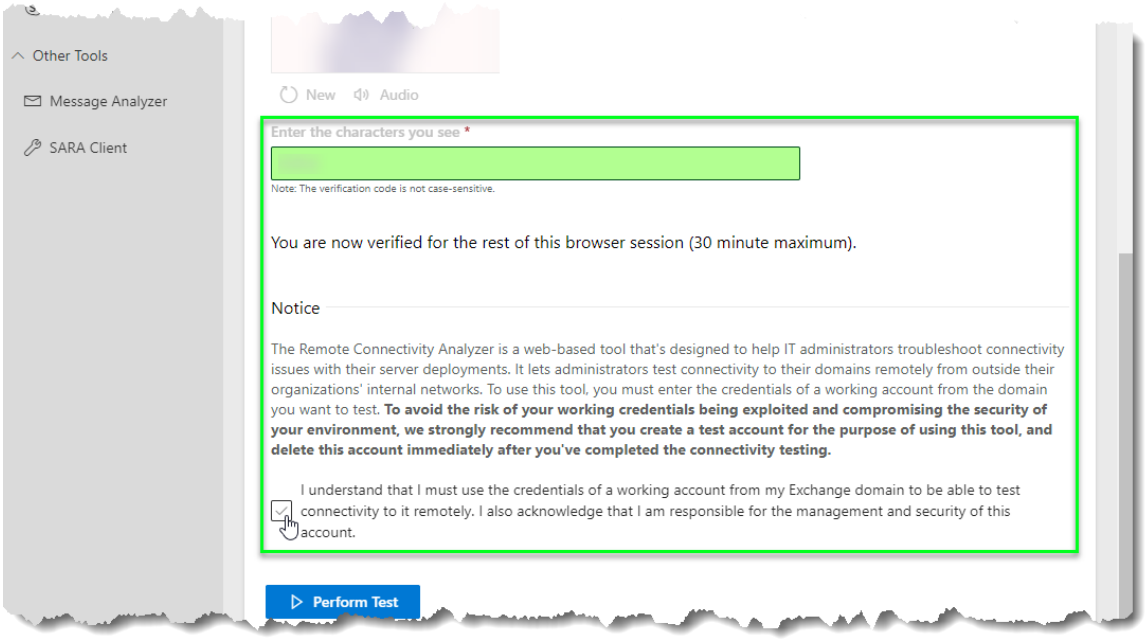
6. Enter the test email address in the “Target mailbox email address” box of the form. (This should be the same email address entered in the “Target mailbox email address” box.)



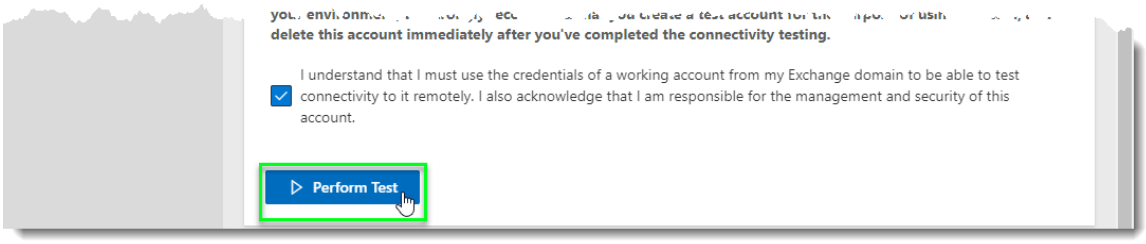
7. Enter the displayed Verification code in the “Enter the characters you see” box of the form, then click on the “Verify” button.



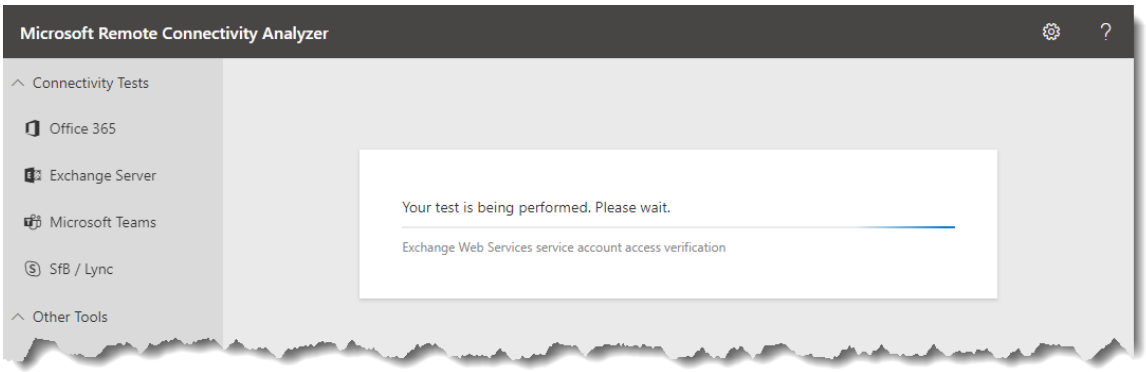
8. Observe that your verification code was accepted for the browser session, then mark the checkbox next to the acknowledgement statement.



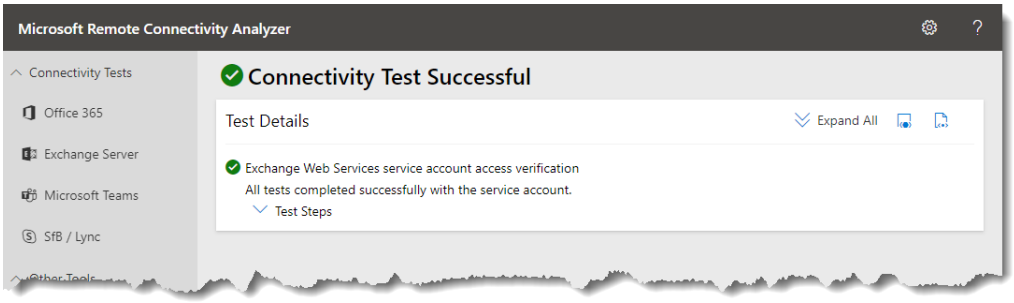
9. Click on the “Perform Test” button.



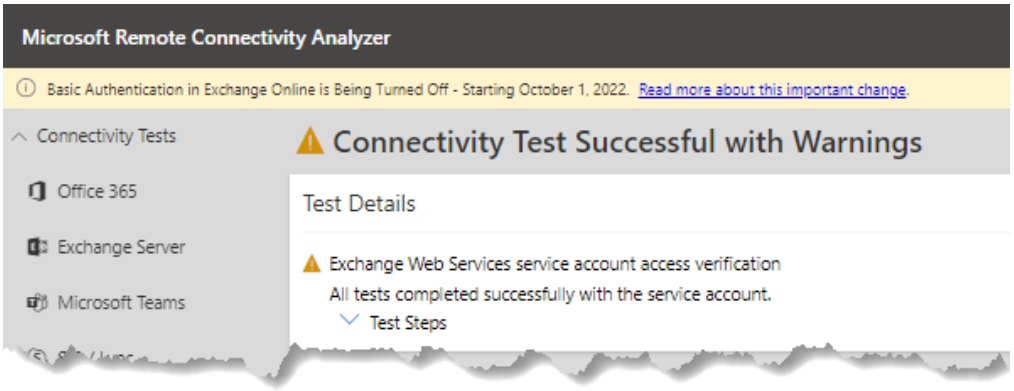
10. Wait while the test is performed.

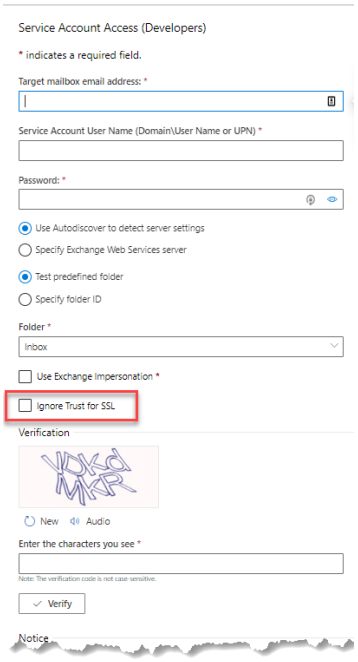


11. Observe the results of the test.
    a. If the test was successful, no further configuration of the service account is required. Provide the service account email address and password in the secure online form.



    b. Connectivity Test Successful with warnings. Please ensure that you have checked “Ignore Trust for SSL. If this tests success its due to no SSL in place for your domain, we recommend you set up an SSL.





MoxiWorks

Submit Credentials to MoxiEngage

Once the above process is completed, please submit your credentials to us through this Cognito form.

Tips and Further Information

- Why is this process necessary for Engage to function for our agents?
    - Engage functions through a sync between itself and an agent's email. Without an email to sync to Engage cannot work.
    - Engage can sync to an office-provided MS365 or Google Workspace account, provided that your office completes the Integration Process.
    - Integration process can only be completed by someone with admin credentials to the office email tenant.
    - Once you've completed the process you must submit those credentials to us here: https://www.cognitoforms.com/MoxiWorks2/moxiworksrealogyengagecredentialsform
    - If you do not have an office provided email or prefer not to do this process for any reason, your agents will always have the option to sync using a Free Gmail account. No further action is required by your office in this case.

- Notes about known issues and what to do:
    - 3rd Party Provided Email - Offices with email accounts purchased through third party companies such as Go-Daddy may not be able to complete process due to limitations they place on admin access. Your agents will still be able to sync with Free Gmail.
    - Access / Permissions - If you do not have admin privileges to your email tenant you must escalate to someone who does or reach out to your email provider. Moxi cannot assist you with your permissions in your email tenant.
    - Stuck? - If you are stuck on a step of the process, compare your screen to the screenshot shown for that step and ensure they look the same. Additionally, each section of the process includes a time stamp and link to a video going through the process step by step.
    - Failed Submission – If you have submitted credentials and have subsequently been notified that your submission failed, we recommend redoing the setup process entirely. During this new setup, do not use anything created in the previous attempt, instead

create a new service account with a new name, etc. If you use any previously created accounts, permissions, etc you will likely experience the same issue.

- Most offices that have resubmitted credentials after failing their first submission passed on their 2nd attempt.
- When redoing the process, it is critical that any field where you name something is filled in differently that your previous attempt. If you reuse names from a previous attempt this will likely cause an issue, even if you have deleted the previously created account / permission. We recommend putting a number at the end of the name that reflects the attempt # (i.e. MoxiEngage2 & Impersonation2).
- If you continue to have issues we recommend reaching out to your email provider and requesting assistance.

Related Resources

Google Workspace Support

Microsoft Office Support
The following resources may provide additional information you need to perform the requisite tasks:

Compare Active Directory to Azure Active Directory

Azure AD PowerShell Module

Connect to Microsoft 365 with PowerShell

Set an individual user's password to never expire