Office 365 Exchange Assessment: Prerequisites and Configuration

This document explains the required steps to configure the Office 365 Exchange Assessment included with your Microsoft Azure Log Analytics Workspace and Microsoft Unified Support Solution Pack.

There are configuration and setup tasks to be completed prior to executing the assessment setup tasks in this document. For all pre-work, follow the Getting Started with On-Demand Assessments in the Services Hub Resource Center.

This document was last updated on August 27th, 2021. To ensure you have the latest version of this document, check here: https://go.microsoft.com/fwlink/?linkid=874965

Table of Contents

This document was last updated on August 27th, 2021. To ensure you have the latest version of this document, check here: https://go.microsoft.com/fwlink/?linkid=874965

System Requirements and Configuration at Glance

According to the scenario you want to use, review the following details to ensure that you meet the necessary requirements.

Supported Versions

- Office 365 tenant (AzureCloud, AzureChinaCloud, AzureGermanCloud, AzureUSGovernment)
- For Hybrid evaluation, Exchange Servers must run Exchange Server 2010, Exchange Server 2013, or Exchange Server 2016.

Environment Permissions

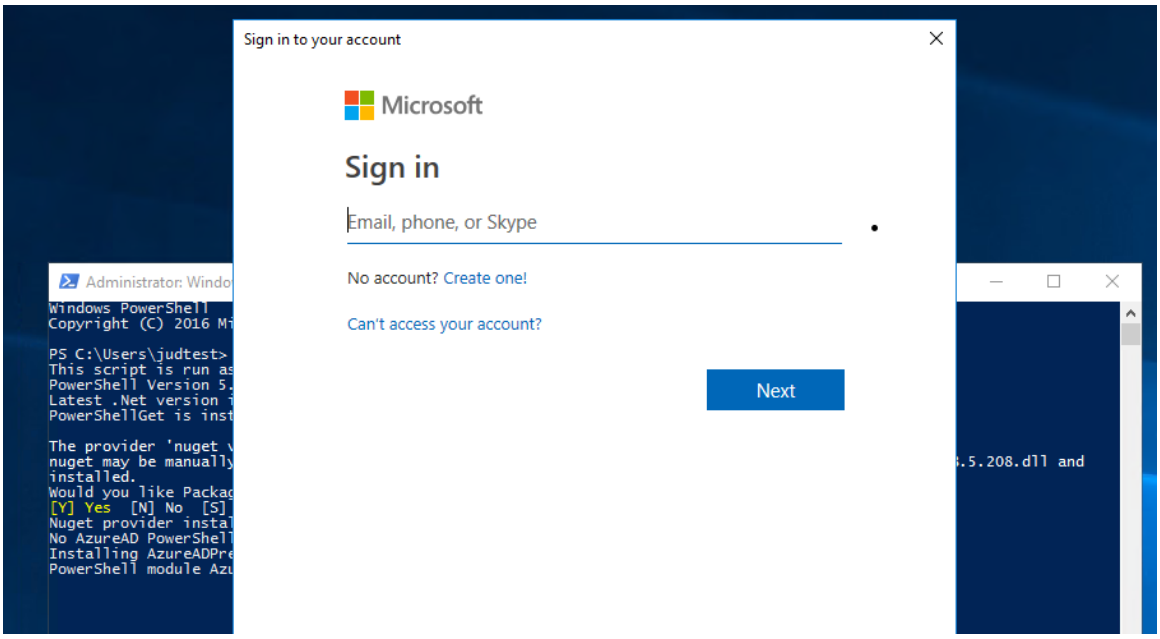
- **User account rights:**
    - A domain or local account with the following rights:
        - Local Admin access on the data collection machine
    - An Office 365 (Azure AD Account) with the following properties
        - Global Administrator for the Assessment Application setup (1-time setup)
        - Global Reader for data collection
        - Non-Federated
        - MFA is supported

Data Collection Machine

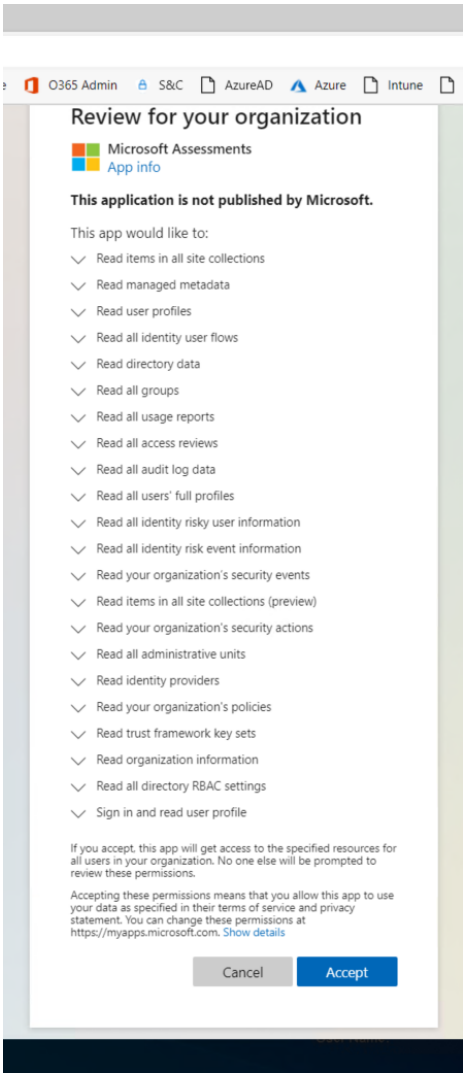
- A **data collection machine** running the Office 365 Exchange Assessment requires computers running Windows Server 2016 or Windows 10.
- The **data collection machine** can be joined to a domain or standalone
- **Data collection machine hardware:** Minimum 8 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 10 GB of free disk space.
- Microsoft .NET Framework 4.8 or newer installed
    - Download from: Download .NET Framework 4.8 | Free official downloads (microsoft.com)
- The CLR version on the data collection machine should be using .NET 4.0 or greater. This can be verified by running $PSVersionTable.CLRVersion in the PowerShell prompt
- Install the Exchange Online PowerShell module from https://aka.ms/exomodule
- Install MSOnline and CredentialManager PowerShell modules:

    1. Open a PowerShell session with Administrator privileges
    2. On the shell type the following command: *Install-Module MSOnline -Verbose -AllowClobber -Force*
    3. On the shell type the following command: *Install-Module CredentialManager*
    4. On the shell type the following command: *Import-Module MSOnline*

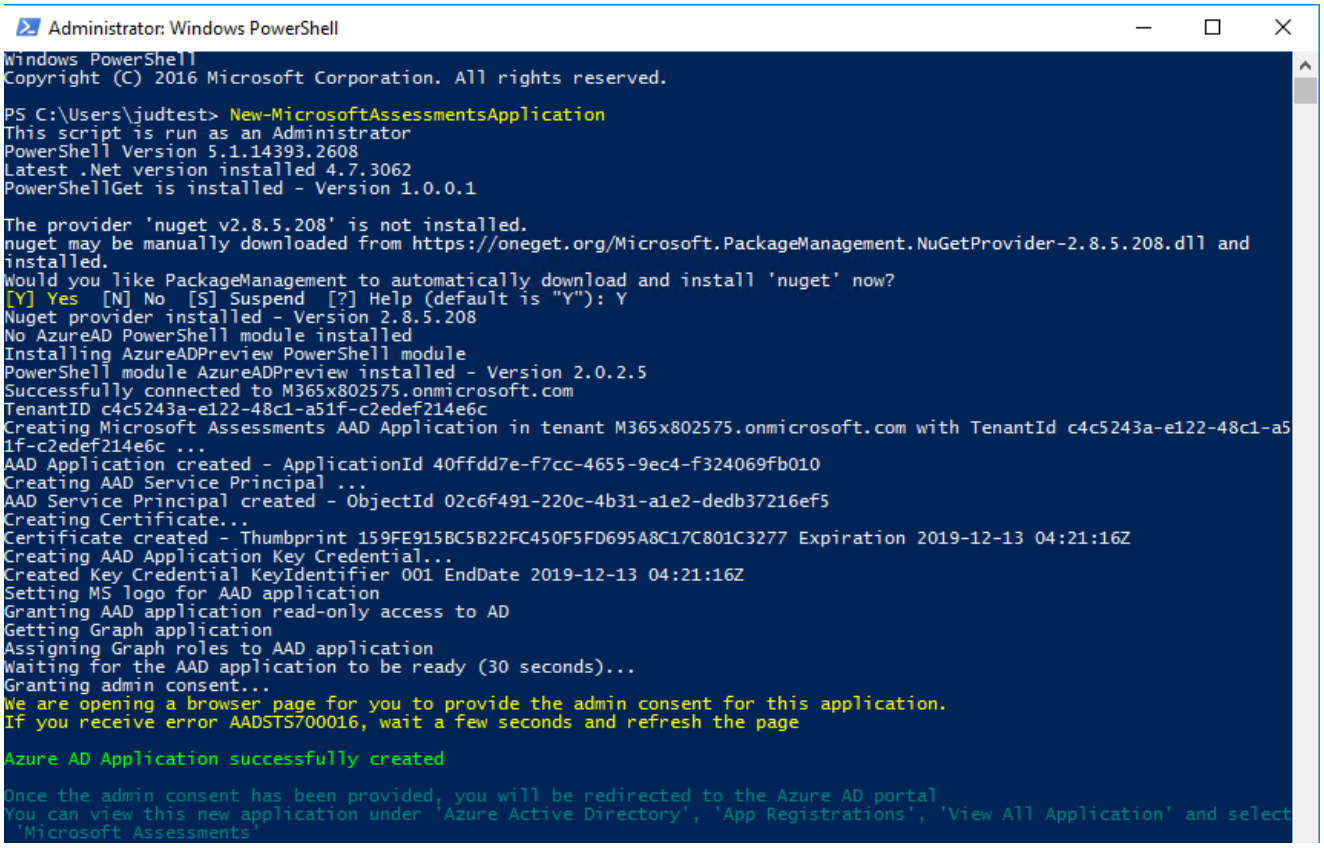
- Set up the Azure AD Application for Graph API authentication.
    1. Open a PowerShell session with Administrator privileges
    2. Ensure that running of scripts is permitted on the machine: *Set-ExecutionPolicy RemoteSigned*
    3. Run the following cmdlet: *New-MicrosoftAssessmentsApplication*
    4. This will prompt for Office 365 Administrator credentials (Global Administrator)



5. Enter the credentials for the Administrator account to be used to create the app in Azure
6. Once the credentials are entered the application will be created, the AzureAD Preview PowerShell module installed as well as other prerequisites verified.
7. There will be an admin consent prompt for a number of **read** permissions, accept these permissions for the app to continue.



8. Once everything is complete the Azure Portal will be opened and the PowerShell output will state that the Azure AD Application has been successfully created:



9. If you encounter issues with setting up the Assessment Application, for example if you do not receive an authentication prompt please refer to the troubleshooting section in the appendix.

- The **data collection machine** must be able to connect to the Internet using HTTPS to submit the collected data to your log analytics workspace. This connection can be direct, or via a proxy.

Setting up the Office 365 Exchange Assessment

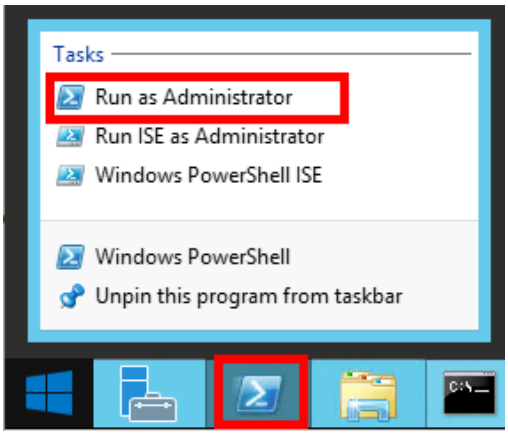
When you have finished the installation of the Microsoft Management Agent/OMS Gateway and completed the Microsoft Assessment Application setup, you are ready to setup the Office 365 Exchange Assessment

IMPORTANT: Although MFA is supported for the data collection account, when it is enabled automatic data collection cannot occur as an administrator would need to respond to the MFA prompts. If you choose to use MFA for the data collection account, you must manually collect data from Office 365 via a PowerShell script. See step 9 below for more information.

On the designated data collection machine, complete the following:

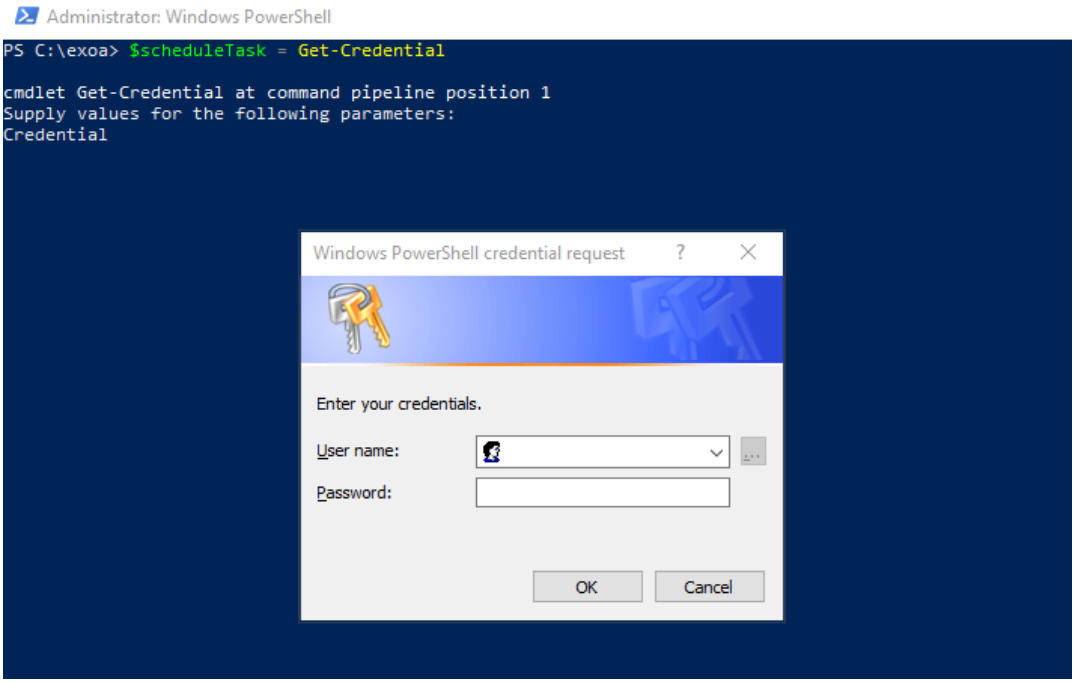
1. Note the following information
    - Credentials for scheduled task account (local admin account & the currently logged on user)
    - Credentials for Office 365 Tenant (Global Reader credentials on Office 365)
    - Create an Assessment Working directory, for example, C:\EXOA

2. Open the Windows PowerShell command prompt as an Administrator



3. Define the credentials for the assessment to use and the working directory by entering the following commands:

```
$scheduleTask = Get-Credential #Account to setup and Run Scheduled Task
$Office365EXOCred = Get-Credential #Account used to connect to Office 365
$dir = "C:\EXOA" #The location for the working directory e.g. "C:\EXOA"
```



Note: The credentials used for $ScheduleTask must be those of the current logged on user

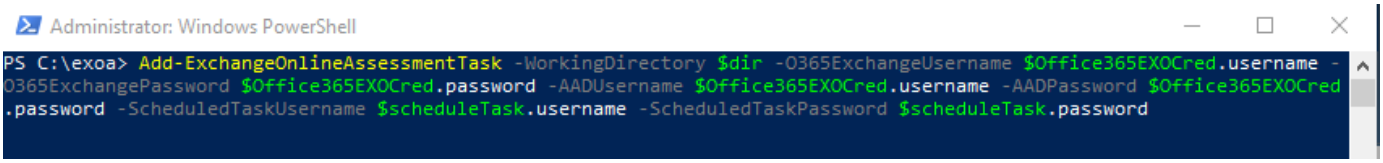
4. Depending on whether you are using MFA for the Global Reader account run the appropriate command below to add the assessment:

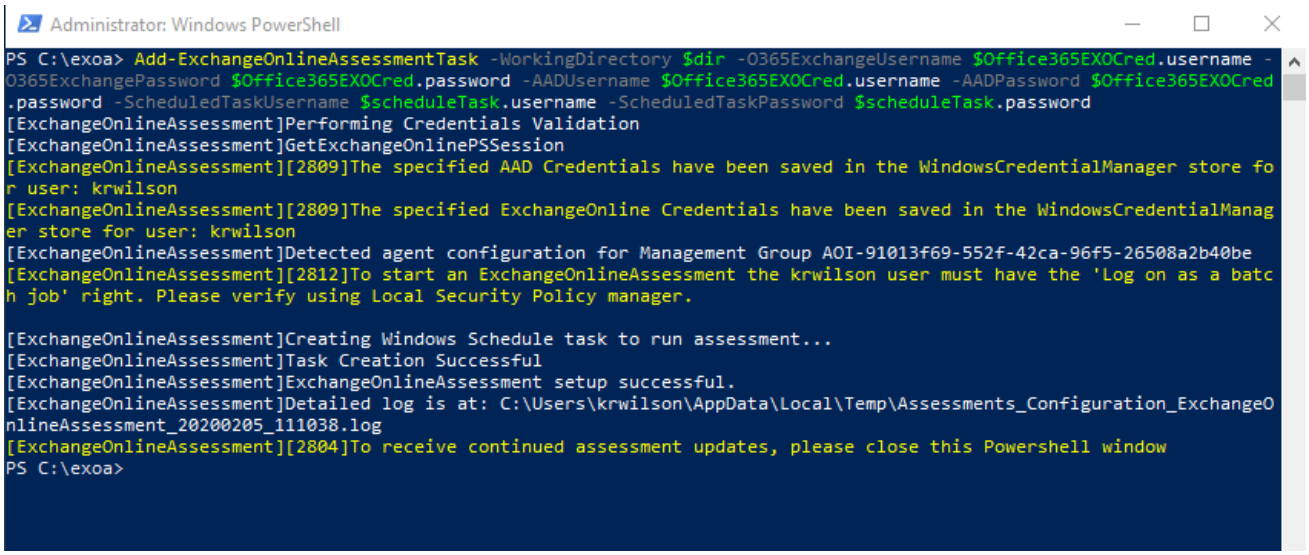
MFA Enabled

```
Add-ExchangeOnlineAssessmentTask –WorkingDirectory $dir -ScheduledTaskUsername $scheduleTask.username -ScheduledTaskPassword $scheduleTask.password
```

MFA Disabled

```
Add-ExchangeOnlineAssessmentTask –WorkingDirectory $dir -O365ExchangeUsername $Office365EXOCred.username -O365ExchangePassword $Office365EXOCred.password -AADUsername $Office365EXOCred.username -AADPassword $Office365EXOCred.password -ScheduledTaskUsername $scheduleTask.username -ScheduledTaskPassword $scheduleTask.password
```



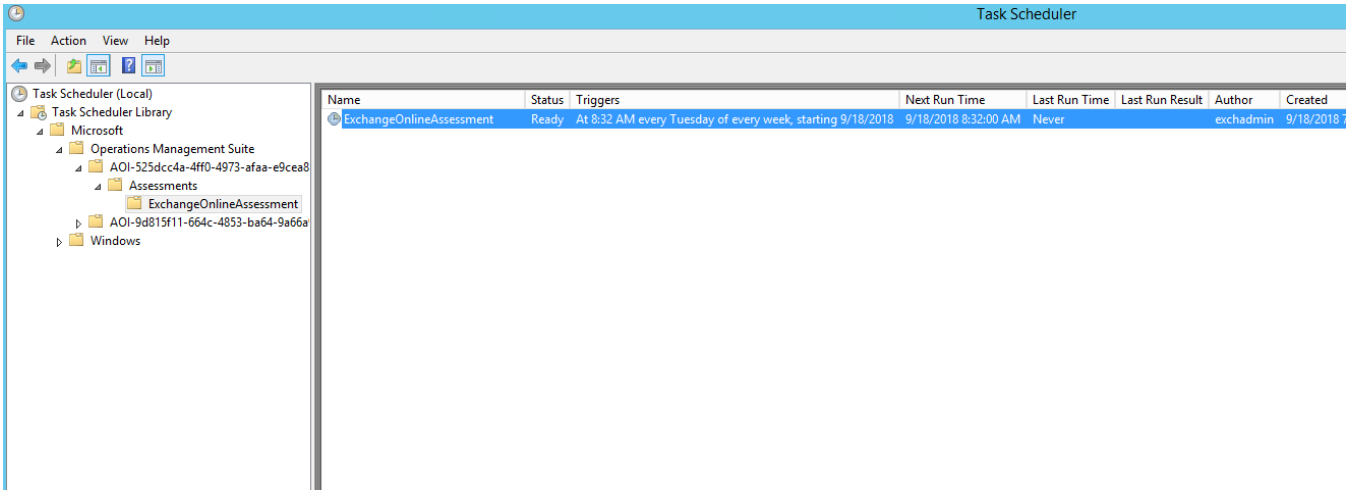


5. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

6. Add the On-Premises User to the local Security Policy to allow the user to log on as batch job
   - Open gpedit.msc
   - Navigate to *Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment*
   - Right click on "Log on as batch job" and select Properties
   - Click "Add User or Group" and include the relevant user.

7. Modify the User Profile Service Setting:
   - Open gpedit.msc
   - Navigate to *Computer Configuration->Administrative Templates->System-> User Profiles*
   - Open to setting "Do not forcefully unload the user registry at user logoff" and change from "Not Configured" to "Enabled"

8. Data collection is triggered by the **scheduled task** named **ExchangeOnlineAssessment** within an hour of running the previous script and then every 7 days. The task can be modified to run on a different date/time or even forced to run immediately.



For guidance and details on working with assessment results, visit Working with Assessment Results in the Services Hub Resource Center.

9. If MFA is in use for the data collection account, you must also manually collect data from Office 365 as often as you require. This collection is performed by running the following PowerShell script:

```
C:\EXOA
|-- ExchangeOnlineAssessment
    |-- [Numbered Folder]
        |-- Temp
            |-- Exchange.O365
                |-- EXO_Master.ps1
```

NOTE: This folder will only be available after the scheduled task has been run once.

You will need to enter the credentials for the Office 365 account and respond to the MFA prompt. Once the PowerShell script has completed rerun the Scheduled Task to refresh the collected data.

Appendix

Data Collection Methods

The **Office 365 Exchange Assessment** uses multiple data collection methods to collect information from your environment. This section describes the methods used to collect data from your environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

Data collection uses workflows and collectors. The collectors are:

Microsoft Graph API

Microsoft Exchange Online PowerShell

Microsoft Graph API

The Microsoft Graph API is used to get data pertaining to Office 365 Secure Score.

Microsoft Exchange Online PowerShell

PowerShell is used to collect data from both Azure AD and Office 365. PowerShell uses the cmdlets from Azure PowerShell, Exchange Online Management Shell and Patterns and Practices PnP) cmdlets to connect to and pull the required configuration settings pertaining to the tenant.

Office 365 Assessment – Authentication Model

The Office 365 Assessment collects data using 2 methods:

1. Microsoft Graph
2. PowerShell Cmdlets

Graph API

The assessment connects to and extracts data form Microsoft Graph using an App created in Azure. The App is granted read permissions using OAuth. The data collection machine will have a certificate which is used to connect to the Azure App, which in turns gets the data from Microsoft Graph. During the setup of the assessment, a Global Admin is required in order to create the App and grant it the relevant Read permissions so that it can query Microsoft Graph. Once the setup is completed this part of the assessment will collect data with the App via the certificate with no account requirement. The App has only read access, which helps collect data using a least privileged model.

PowerShell Cmdlets

The assessment also collects data from Office 365 using the following cmdlets:

- Azure AD cmdlets
- Exchange Online cmdlets

Whilst these cmdlets currently support modern authentication to login, they are designed to run manually. This means the support of Modern Authentication is handled for accounts with MFA by a prompt to handle the authentication. The assessment collects the data in an automated manner via a scheduled task. As this data collection is designed to run autonomously no prompts are generated. This causes an issue with account having MFA enabled, as when authenticating the account prompt for MFA does not appear and thus account cannot authenticate. We are currently working with the PG on cmdlets that will support OAuth. With cmdlets that fully support OAuth we can use the Azure App to authenticate the requests made from the cmdlets. In doing so this will remove the requirement to use a Global Admin account entirely, as well as the current requirement to manually collect the data when using an account that has MFA enabled

Troubleshooting Exchange Online Assessment Setup

General Troubleshooting OnDemand Assessment Guide

https://docs.microsoft.com/en-us/services-hub/health/assessments-troubleshooting

Office 365 URLs and IP address ranges

Office 365 requires connectivity to the Internet. The endpoints listed in the following article should be reachable

https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

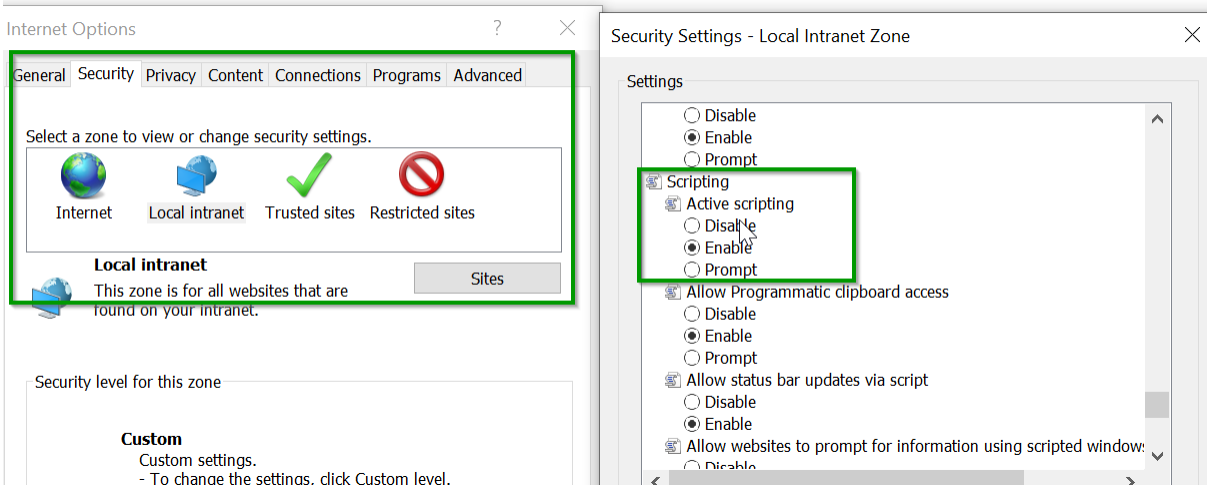
New-MicrosoftAssessmentApplication

If there are URL restrictions in place in order to correctly setup the Assessment Application you will need to ensure you whitelist the following URLs:

URLs
aadcdn.msauth.net:443
az818661.vo.msecnd.net:443
c.urs.microsoft.com:443
go.microsoft.com:443
iecvlist.microsoft.com:443
ieonline.microsoft.com:443
login.microsoftonline.com:443
oneget.org:443
psg-prod-eastus.azureedge.net:443
www.powershellgallery.com:443

Along with above URLs, ensure the following settings are enabled in Internet Explorer as JavaScript needs to run on the page.

Internet Options → Security Settings



While executing the New-MicrosoftAssessmentsApplication command, you may be prompted to add additional links to trusted sites to allow the authentication screen to display. These can be added by clicking the “Add” button shown on the popup.

Prerequisites Error

If you encounter any prerequisites errors, please check for any errors in Event Viewer as shown below: