

# Azure Active Directory Assessment: Prerequisites and Configuration

This document explains the required steps to configure the Azure Active Directory (AD) Assessment included with your Microsoft Azure Log Analytics Workspace and entitled Microsoft On-Demand assessment.

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.

## Table of Contents

<b>System Requirements and Configuration at Glance.....</b>	<b>2</b>
Supported Environments .....	2
Environment Permissions.....	2
Data Collection Machine.....	2
<b>Getting started with Microsoft Azure AD Assessment.....</b>	<b>3</b>
<b>Setup the Azure AD Application for Graph API authentication. ....</b>	<b>3</b>
<b>Setup the Azure AD Assessment.....</b>	<b>6</b>
Configure with MFA Enabled User Account .....	6
Configure with MFA Disabled User Account.....	7
Scheduled Task Details .....	8
<b>Appendix.....</b>	<b>9</b>
Data Collection Methods .....	9
Troubleshooting Azure AD Assessment Setup.....	9
General Troubleshooting OnDemand Assessment Guide.....	9
Azure datacenter IP address ranges.....	9
New-MicrosoftAssessmentApplication .....	9
Prerequisites Error .....	10

## 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 Environments

- Azure AD tenant (AzureCloud, AzureChinaCloud, AzureGermanCloud, AzureUSGovernment)

### Environment Permissions

- **Assessment account rights:**
  - An assessment scheduled task account with the following rights:
    - Administrative access to the data collection machine
    - Log on as a batch job privileges on the data collection machine
  - An Azure AD account for the setup of the Azure AD Registered Application with the following properties
    - Global Administrator
    - Non-Federated
  - An Azure AD account for assessment execution (can be separate account than above)
    - Global Reader
    - Non-Federated

**Note:** The Azure AD account for assessment execution is supported for MFA. The assessment setup and execution details will differ depending on which route is chosen; MFA enabled Azure AD account or MFA disabled Azure AD account.

### Data Collection Machine

- A **data collection machine** running the Azure AD Assessment requires computers running Windows Server 2016 or Windows Server 2019 or Windows 10.
- The **data collection machine** may be Azure AD joined, Active Directory joined, or Workgroup joined.
- The **data collection machine** must be able to connect to the Internet using HTTPS to successfully perform all steps detailed in this document. This connection can be direct, or via a proxy.
- **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: <https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-web-installer>
- 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
- Azure AD Preview Module for PowerShell needs to be installed (this will be installed automatically)
- MSONline Powershell module. Install MSONline PowerShell module:
  1. Open a PowerShell session with Administrator privileges
  2. On Start Menu type: PowerShell
  3. Right Click on the Icon and choose Run as Administrator
  4. On the shell type the following command: `Install-Module MSONline -Verbose -AllowClobber -Force`

- Microsoft.Graph Powershell module. Install Microsoft.Graph PowerShell module:
5. Open a PowerShell session with Administrator privileges
  6. On Start Menu type: PowerShell
  7. Right Click on the Icon and choose Run as Administrator
  8. On the shell type the following command: *Install-Module Microsoft.Graph -Verbose -AllowClobber -Force*

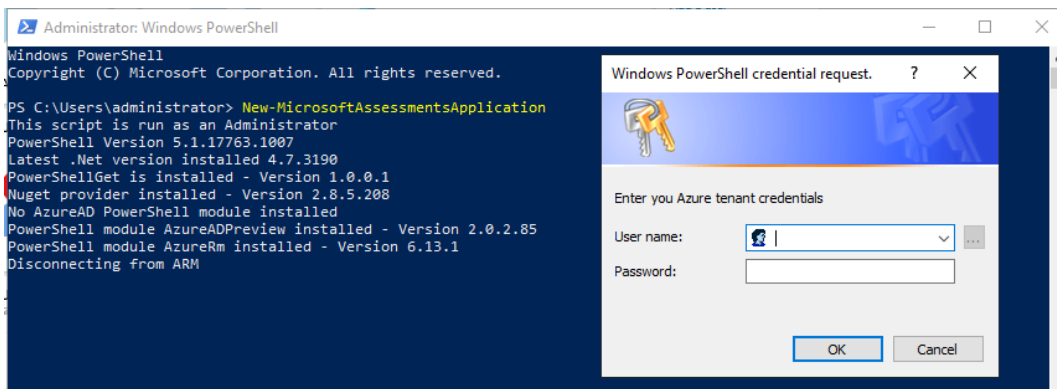
## Getting started with Microsoft Azure AD Assessment

Be sure to complete the steps in the following link before proceeding to assessment setup:

<https://docs.microsoft.com/en-us/services-hub/health/getting-started-azuread>

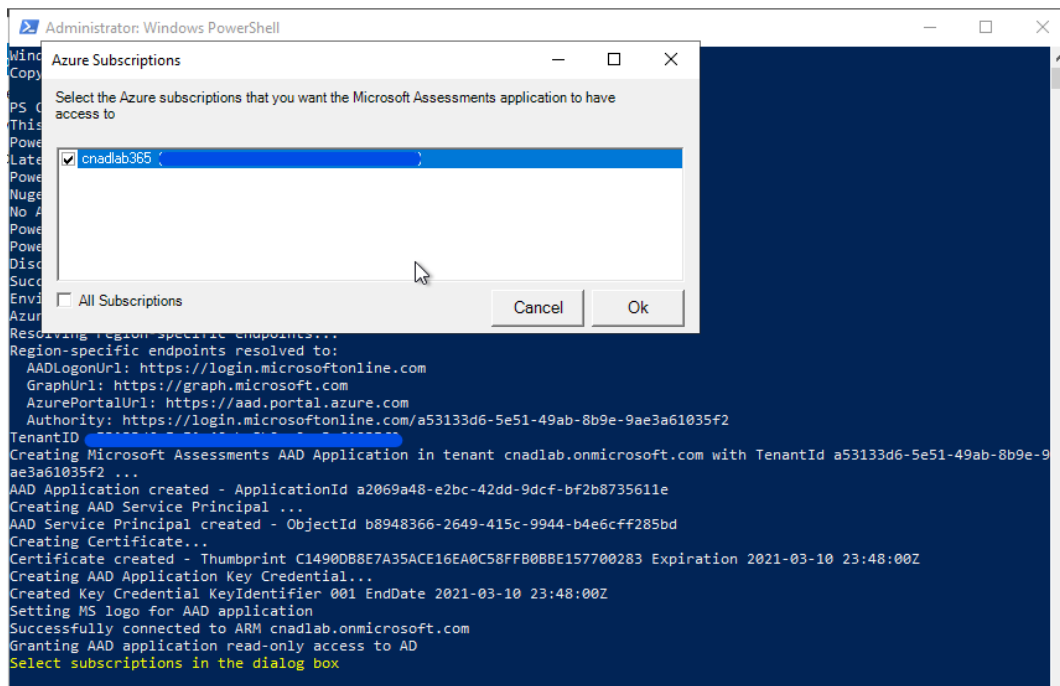
## Setup the Azure AD Application for Graph API authentication.

1. Open a PowerShell session on the data collection machine with Administrator privileges.
2. Ensure the running of scripts is permitted on the machine: *Set-ExecutionPolicy RemoteSigned*.
3. Run the following cmdlet: *New-MicrosoftAssessmentsApplication*.
4. This will prompt for Azure AD tenant Global administrator credentials:

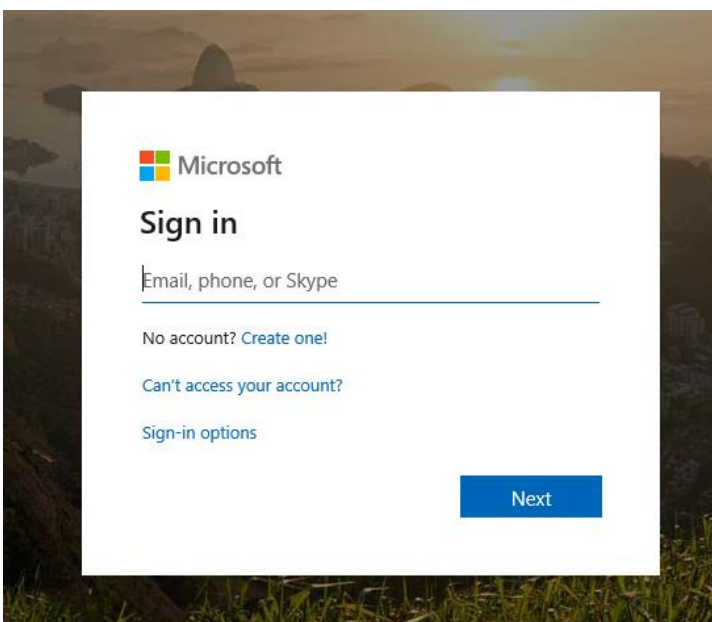


5. Enter the credentials for the Azure AD Tenant Global Administrator to be used to create the Azure application.
6. Once the credentials are entered the application will be created, the AzureAD Preview PowerShell module installed as well as other prerequisites verified.

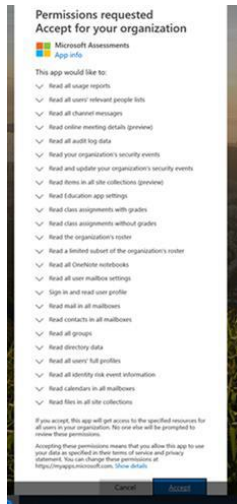
7. Select the Azure subscription that is in scope for the assessment:



8. An internet browser prompt will appear for Azure portal login with Global Administrator credentials:



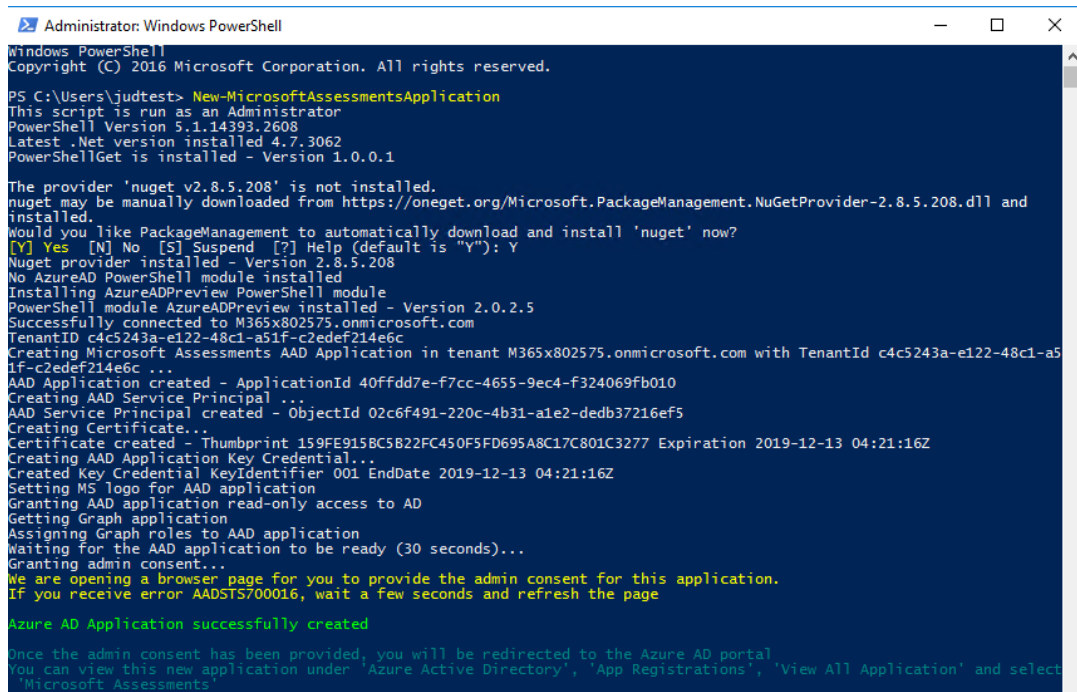
9. The required application consent **read** permissions will be displayed:



Select accept to complete the application registration.

Note: Please refer to [Permissions for Microsoft Azure AD Assessment Application](#) for consent details.

10. Once everything is complete, the application registration can be viewed in the Azure AD portal and the PowerShell output will state that the Azure AD Application has been successfully created:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\judtest> New-MicrosoftAssessmentsApplication
This script is run as an Administrator
PowerShell Version 5.1.14393.2608
Latest .Net version installed 4.7.3062
PowerShellGet is installed - Version 1.0.0.1

The provider 'nuget v2.8.5.208' is not installed.
nuget may be manually downloaded from https://oneget.org/Microsoft.PackageManagement.NuGetProvider-2.8.5.208.dll and
installed.
Would you like PackageManagement to automatically download and install 'nuget' now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
Nuget provider installed - Version 2.8.5.208
No AzureAD PowerShell module installed
Installing AzureADPreview PowerShell module
PowerShell module AzureADPreview installed - Version 2.0.2.5
Successfully connected to M365x802575.onmicrosoft.com
TenantID c4c5243a-e122-48c1-a51f-c2edef214e6c
Creating Microsoft Assessments AAD Application in tenant M365x802575.onmicrosoft.com with TenantId c4c5243a-e122-48c1-a51f-c2edef214e6c ...
AAD Application created - ApplicationId 40ffdd7e-f7cc-4655-9ec4-f324069fb010
Creating AAD Service Principal ...
AAD Service Principal created - ObjectID 02c6f491-220c-4b31-a1e2-dedb37216ef5
Creating Certificate...
Certificate created - Thumbprint 159FE915BC5822FC450F5FD695A8C17C801C3277 Expiration 2019-12-13 04:21:16Z
Creating AAD Application Key Credential...
Created Key Credential KeyIdentifier 001 EndDate 2019-12-13 04:21:16Z
Setting MS logo for AAD application
Granting AAD application read-only access to AD
Getting Graph application
Assigning Graph roles to AAD application
Waiting for the AAD application to be ready (30 seconds)...
Granting admin consent...
We are opening a browser page for you to provide the admin consent for this application.
If you receive error AADSTS700016, wait a few seconds and refresh the page

Azure AD Application successfully created

Once the admin consent has been provided, you will be redirected to the Azure AD portal.
You can view this new application under 'Azure Active Directory', 'App Registrations', 'View All Application' and select
'Microsoft Assessments'
```

11. 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.

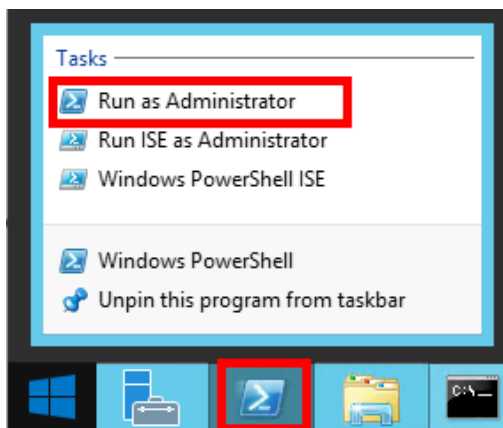
## Setup the Azure AD Assessment

When you have finished the installation of the Microsoft Management Agent/OMS Gateway, you are ready to setup the Azure AD Assessment. The assessment runs as a scheduled task and requires a user account for execution.

### Configure with MFA Enabled User Account

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator

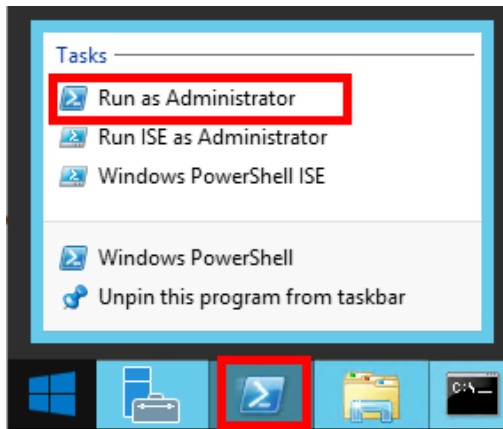


- Run the **Add-AzureAssessmentTask** command using the parameters below, replacing and **<AzureADUser>**, **<Directory>**, and **<AccountName>** with the Azure AD User account, an assessment working directory, and assessment scheduled task account name:  
*PS C:\OmsAssessment> Add-AzureAssessmentTask -AADUsername <AzureADUser> -WorkingDirectory <Directory> -ScheduledTaskUsername <accountname> -MFA \$true*

### Configure with MFA Disabled User Account

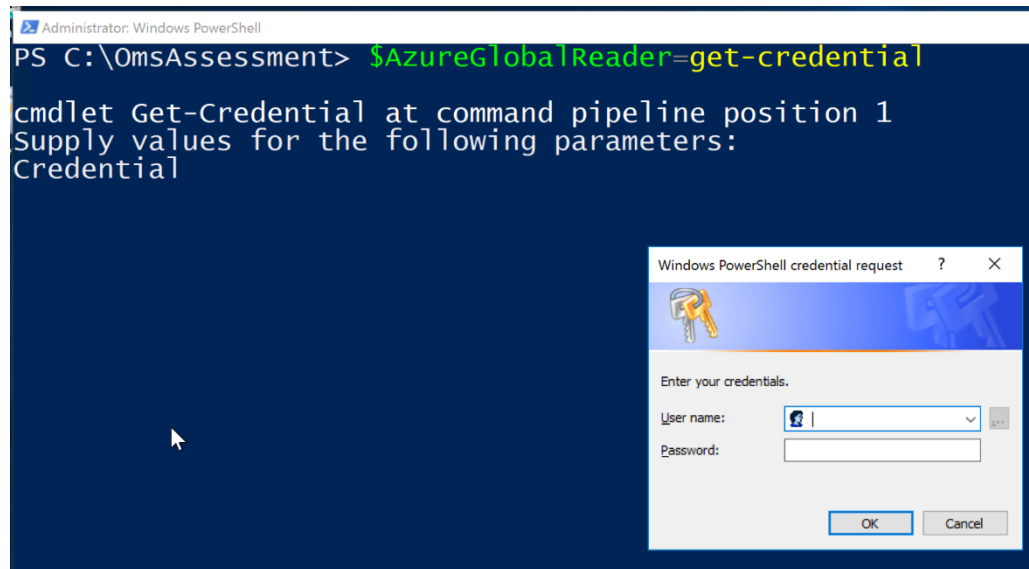
On the designated data collection machine, complete the following:

- Open the Windows PowerShell command prompt as an Administrator



- Define the credentials for the assessment to use:

- \$AzureGlobalReader = Get-Credential**



- Run the **Add-AzureAssessmentTask** command using the parameters below, replacing and **<Directory>** and **<AccountName>** with an assessment working directory and assessment scheduled task account name:  
*PS C:\OmsAssessment> Add-AzureAssessmentTask -AADUsername \$AzureGlobalReader.Username -AADPassword \$AzureGlobalReader.password -WorkingDirectory <Directory> -ScheduledTaskUsername <accountname>*

**Note.** If the command **Add-AzureAssessmentTask** is not available, the module is not yet found. It can take some time after installing the agent before it to show up.

```
Administrator: Windows PowerShell
PS C:\OMS> Add-AzureAssessmentTask -AADUsername $AzureGlobalReader.Username -AADPassword $AzureGlobalReader.password -WorkingDirectory c:\oms -ScheduledTaskUsername administrator

cmdlet Add-AzureAssessmentTask at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ScheduledTaskPassword: *****
[AzureAssessment]Performing Credentials Validation
[AzureAssessment][2859]The specified AAD Credentials have been saved in the WindowsCredentialManager store for user: administrator
[AzureAssessment]Agent is connected to multiple Management Group(s)/Workspace(s).
[AzureAssessment]1.AOI-463a9eea-1c05-42a0-8154-6d37fc0cb7b5
[AzureAssessment]2.AOI-c18d0e4c-cd0e-43ab-bec2-6428ac35ab2f
[AzureAssessment]Select the Management Group/Workspace to be used with AzureAssessment. (Enter the number corresponding to list item):
1
[AzureAssessment][2861]To start an AzureAssessment the administrator user must have the 'Log on as a batch job' right. Please verify using Local Security Policy manager.

[AzureAssessment]Creating Windows Schedule task to run assessment...
[AzureAssessment]Task Creation Successful
[AzureAssessment]AzureAssessment setup successful.
[AzureAssessment]Detailed log is at: C:\Users\administrator\AppData\Local\Temp\3\Assessments_Configuration_AzureAssessment_20200302_072643.log
[AzureAssessment][2852]To receive continued assessment updates, please close this Powershell window
```

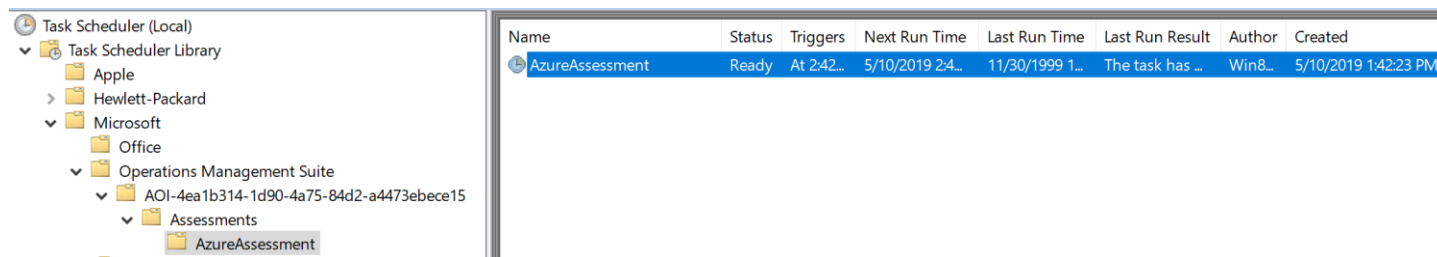
4. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

## Scheduled Task Details

Assessment execution triggering depends whether **-MFA \$true** parameter was used in **Add-AzureAssessmentTask**.

For an MFA enabled Azure AD user account; manually trigger the assessment through execution of the **AzureAssessment (MFA)** desktop shortcut or execution of the task from within **Task Scheduler**.

For an MFA disabled Azure AD user account; data collection is triggered by the **scheduled task** named **AzureAssessment** 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.



# Appendix

## Data Collection Methods

The **Azure AD Assessment** uses a couple data collection methods to collect information from the Azure AD tenant. This section describes the methods used to collect data from the environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

1. Windows PowerShell
2. Graph API

### 4. Windows PowerShell

PowerShell is used extensively in the Azure AD Assessment to gather configuration data. This includes scripts that directly call Graph API endpoints as well as cmdlets from MSOnline and AzureADPreview modules.

### 5. Graph API

Graph API is used to collect configuration and assessment data from Secure Score.

## Troubleshooting Azure AD Assessment Setup

### General Troubleshooting OnDemand Assessment Guide

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

### Azure datacenter IP address ranges

The Azure AD Assessment requires connectivity to the Internet from the data collection machine or proxy server. The endpoints listed in the following articles should be reachable from the data collection machine for successful assessment setup and execution. These are in addition to those required by Azure Log Analytics and the Microsoft Management Agent.

- Public: <https://www.microsoft.com/en-us/download/details.aspx?id=56519>
- US Gov (including DoD): <http://www.microsoft.com/en-us/download/details.aspx?id=57063>
- Germany: <http://www.microsoft.com/en-us/download/details.aspx?id=57064>
- China: <http://www.microsoft.com/en-us/download/details.aspx?id=57062>

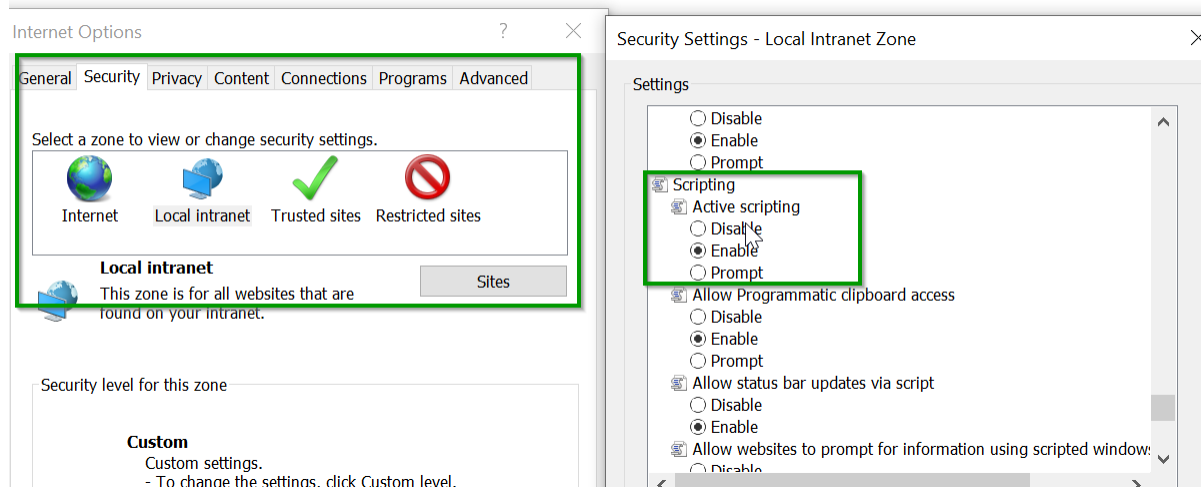
### New-MicrosoftAssessmentApplication

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
<a href="http://www.powershellgallery.com">www.powershellgallery.com</a> :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:

