

# Office 365 Exchange 評価：前提条件および構成

このドキュメントでは、Microsoft Azure Log Analytics ワークスペースと Microsoft Unified Support ソリューション パックに含まれている Office 365 Exchange 評価の構成に必要な手順を説明します。

このドキュメントには、評価のセットアップ タスクを実行する前に完了させる構成とセットアップのタスクがあります。すべての事前作業については、Services Hub リソース センターの[オンデマンド評価の概要](#)に従ってください。

## 目次

システム要件および構成の概要 .....	2
サポートされているバージョン .....	2
環境関連の許可 .....	2
データ収集マシン .....	2
Office 365 Exchange 評価の設定 .....	6
付録 .....	10
データ収集メソッド .....	10
Exchange Online 評価のセットアップのトラブルシューティング .....	11
オンデマンド評価のトラブルシューティング全般に関するガイド .....	11
Office 365 URL および IP アドレス範囲 .....	11
New-MicrosoftAssessmentApplication .....	11
前提条件のエラー .....	12

## システム要件および構成の概要

使用するシナリオに従って、次の詳細を確認し、必要な要件を満たしていることを確かめてください。

## サポートされているバージョン

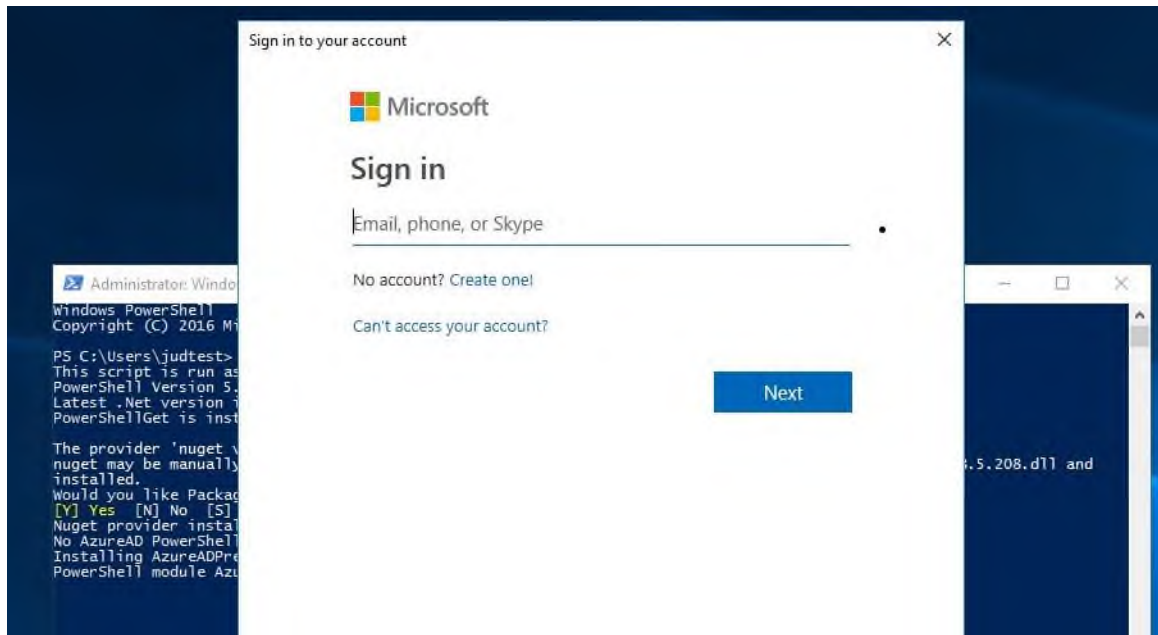
- Office 365 テナント (AzureCloud、AzureChinaCloud、AzureGermanCloud、AzureUSGovernment)
- ハイブリッドの評価については、Exchange Servers では、Exchange Server 2010、Exchange Server 2013、または Exchange Server 2016 を実行する必要があります。

## 環境関連の許可

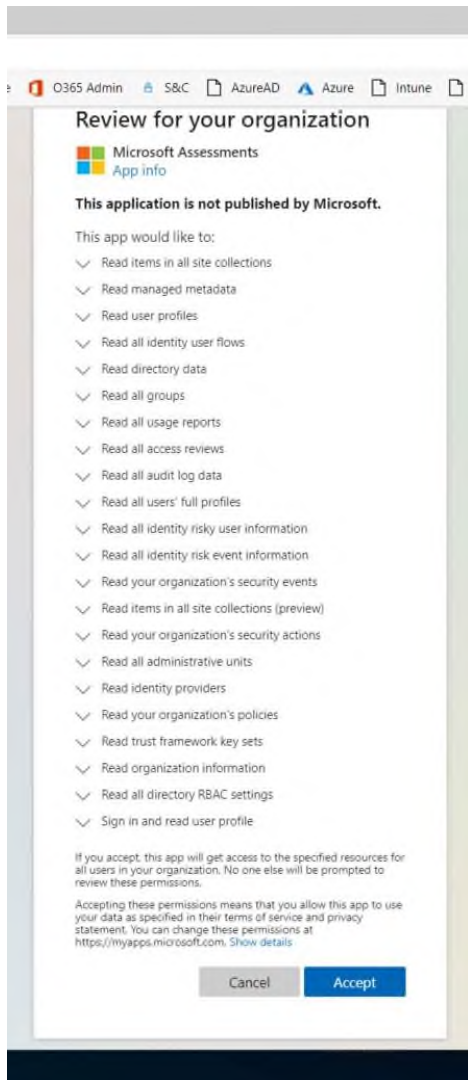
- **ユーザー アカウントの権利:**
  - 次の権利を持つ、ドメインまたはローカル アカウント:
    - データ収集マシンに対するローカル管理者のアクセス
  - 次のプロパティを持つ、Office 365 (Azure AD アカウント)
    - 評価アプリケーションのセットアップ (1 回のセットアップ) の Global Administrator
    - データ収集のグローバル閲覧者
    - 非フェデレーション
    - MFA がサポートされています

## データ収集マシン

- Office 365 Exchange 評価を実行している**データ収集マシン**では、Windows Server 2016 または Windows 10 を実行するコンピューターを必要とします。
- **データ収集マシン**は、ドメインに参加したりスタンドアロンで使用したりする場合があります
- **データ収集マシンのハードウェア:** 最小 8 ギガバイト (GB) の RAM、2 ギガヘルツ (GHz デュアル コア プロセッサ、最小 10 GB の空きディスク領域。
- Microsoft .NET Framework 4.6.2 以降をインストール済み
  - 次からダウンロードします: <https://dotnet.microsoft.com/download/dotnet-framework-runtime/net462>
- データ収集マシンの CLR バージョンでは、.NET 4.0 以上を使用する必要があります。PowerShell プロンプトで \$PSVersionTable.CLRVersion を実行すると、これを確認できます。
- <https://aka.ms/exomodule> から Exchange Online PowerShell モジュールをインストール
- MSOnline および CredentialManager PowerShell モジュールのインストール:
  1. 管理者特権で PowerShell セッションを開く
  2. シェルで次のコマンドを入力: Install-Module MSOnline -Verbose -AllowClobber -Force
  3. シェルで次のコマンドを入力します: Install-Module CredentialManager
  4. シェルで次のコマンドを入力します: Import-Module MSOnline
- Graph API 認証用の Azure AD アプリケーションをセットアップします。
  1. 管理者特権で PowerShell セッションを開く
  2. マシンでスクリプトの実行が許可されていることを確認します: Set-ExecutionPolicy RemoteSigned
  3. 次のコマンドレットを実行します: New-MicrosoftAssessmentsApplication
  4. これにより、Office 365 管理者の資格情報 (Global Administrator) の入力が必要になります



5. Azure でアプリを作成するために使用する管理者アカウントの資格情報を入力します
6. 資格情報が入力されると、アプリケーションが作成され、AzureAD Preview PowerShell モジュールがインストールされるとともに、他の前提条件が検証されます。
7. 複数の読み取りのアクセス許可に対する管理者の同意プロンプトが表示されたら、アプリに対するこれらのアクセス許可に同意し、続行します。



8. すべてを完了すると、Azure Portal が開かれ、PowerShell の出力により、Azure AD アプリケーションが正常に作成されたことが示されます：

```
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 159FE9158C5B22FC450F5FD695A8C17C801C3277 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'
```

9. 認証プロンプトを受信していないなど、評価アプリケーションの設定に関する問題が発生した場合は、付録のトラブルシューティングのセクションを参照してください。
- データ収集マシンは、HTTPS を使用してインターネットに接続し、収集データを Log Analytics ワークスペースに送信する必要があります。この接続は直接の場合、またはプロキシ経由の場合があります。

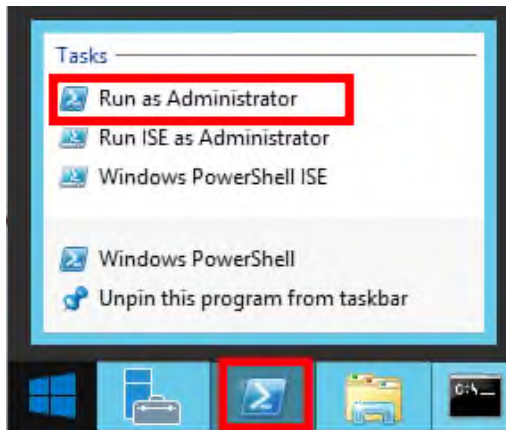
## Office 365 Exchange 評価の設定

Microsoft Management Agent/OMS Gateway のインストールを完了し、Microsoft 評価アプリケーションのセットアップを完了したら、Office 365 Exchange 評価をセットアップする準備が整っています

**重要:** MFA はデータ収集アカウントでサポートされていますが、それが有効になると、管理者が MFA プロンプトに応答する必要があるため、自動データ収集は発生しません。データ収集アカウントで MFA を使用する場合は、PowerShell スクリプトを介し、Office 365 から手動でデータを収集する必要があります。詳細については、以下の手順 9 をご確認ください。

指定されたデータ収集マシンで次の手順を実行します：

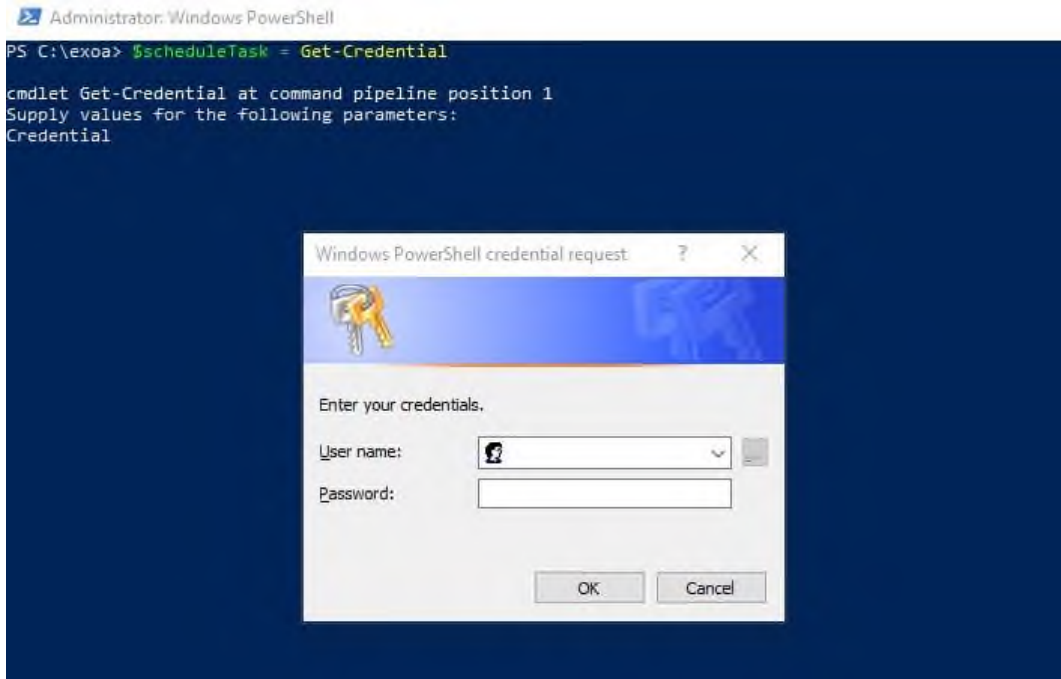
1. 次の情報に注意してください
  - スケジュールされたタスクのアカウントの資格情報（ローカル管理者アカウントと現在ログオンしているユーザー）
  - Office 365 テナントの資格情報（Office 365 のグローバル閲覧者の資格情報）
  - 例えば、C:\¥EXOA など、評価作業ディレクトリを作成します
2. Windows PowerShell コマンド プロンプトを管理者として開きます



3. 次のコマンドを使用して、使用する評価の資格情報と作業ディレクトリを定義します：

```
$scheduleTask = Get-Credential #スケジュールされたタスクをセットアップして実行するアカウント  
$Office365EXOCred = Get-Credential #Office 365 への接続に使用するアカウント  
$dir = "C:\¥EXOA" # "C:\¥EXOA" などの作業ディレクトリの場所
```





**注意:** \$ScheduleTask に使用される資格情報は、現在ログオンしているユーザーのものである必要があります

4. グローバル閲覧者のアカウントで MFA を使用しているかに応じて、下の該当するコマンドを実行して評価を追加します:

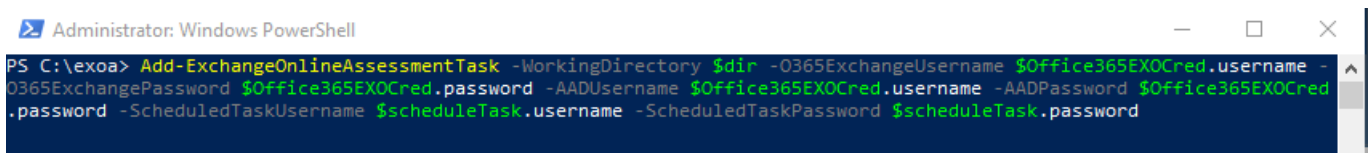
#### MFA が有効

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

#### MFA が無効

```
Add-ExchangeOnlineAssessmentTask -WorkingDirectory $dir -0365ExchangeUsername
$Office365EXOCred.username -0365ExchangePassword $Office365EXOCred.password -AADUsername $Office365EXOCred.username
-AADPassword $Office365EXOCred.password -
ScheduledTaskUsername $ScheduleTask.username -ScheduledTaskPassword
```

```
$ScheduleTask.password
```

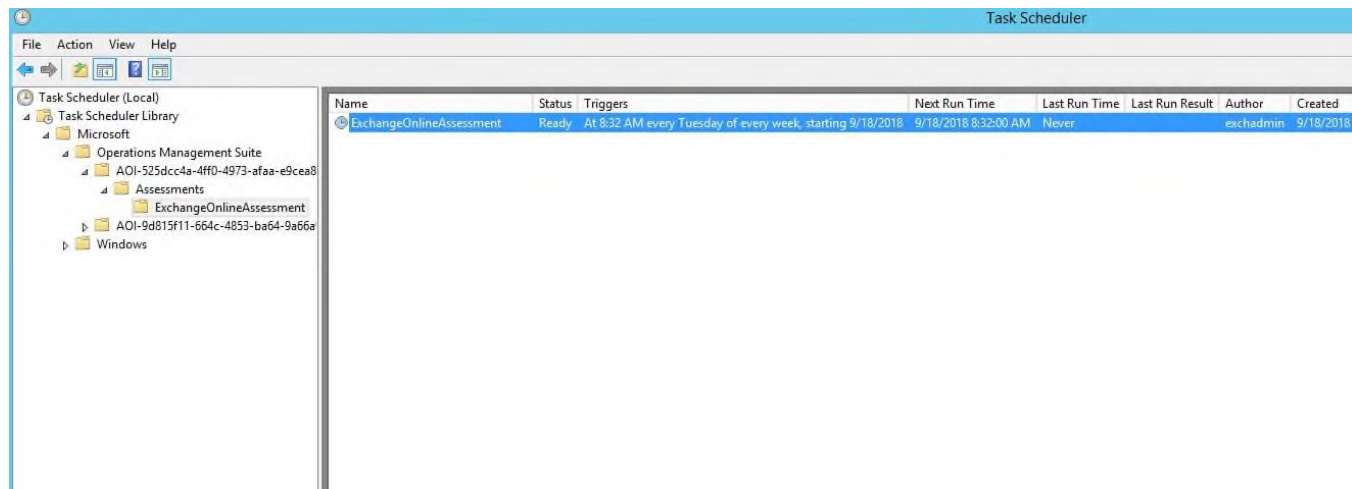


```
Administrator: Windows PowerShell
PS C:\exoa> Add-ExchangeOnlineAssessmentTask -WorkingDirectory $dir -O365ExchangeUsername $Office365EXOCred.username -
O365ExchangePassword $Office365EXOCred.password -AADUsername $Office365EXOCred.username -AADPassword $Office365EXOCred
.password -ScheduledTaskUsername $scheduleTask.username -ScheduledTaskPassword $scheduleTask.password
[ExchangeOnlineAssessment]Performing Credentials Validation
[ExchangeOnlineAssessment]GetExchangeOnlinePSSession
[ExchangeOnlineAssessment][2809]The specified AAD Credentials have been saved in the WindowsCredentialManager store fo
r user: krwilson
[ExchangeOnlineAssessment][2809]The specified ExchangeOnline Credentials have been saved in the WindowsCredentialManag
er store for user: krwilson
[ExchangeOnlineAssessment]Detected agent configuration for Management Group AOI-91013f69-552f-42ca-96f5-26508a2b40be
[ExchangeOnlineAssessment][2812]To start an ExchangeOnlineAssessment the krwilson user must have the 'Log on as a batc
h job' right. Please verify using Local Security Policy manager.

[ExchangeOnlineAssessment]Creating Windows Schedule task to run assessment...
[ExchangeOnlineAssessment]Task Creation Successful
[ExchangeOnlineAssessment]ExchangeOnlineAssessment setup successful.
[ExchangeOnlineAssessment]Detailed log is at: C:\Users\krwilson\AppData\Local\Temp\Assessments_Configuration_ExchangeO
nlineAssessment_20200205_111038.log
[ExchangeOnlineAssessment][2804]To receive continued assessment updates, please close this Powershell window
PS C:\exoa>
```

5. 必要な構成に基づいてスクリプトが続行されます。データ収集をトリガーするスケジュールされたタスクが作成されます。
6. オンプレミスのユーザーをローカルのセキュリティ ポリシーに追加し、ユーザーがバッチ ジョブとしてログオンできるようにします
  - gpedit.msc を開きます
  - コンピューターの構成¥Windows の設定¥セキュリティの設定¥ローカル ポリシー¥ユーザー権利の割り当てに移動します
  - “バッチ ジョブとしてログオン” を右クリックし、プロパティを選択します
  - [ユーザーまたはグループの追加] をクリックし、関連するユーザーを含めます。
7. ユーザー プロファイルのユーザー設定の変更:
  - gpedit.msc を開きます
  - [コンピューターの構成]->[管理用テンプレート]->[システム]-> [ユーザー プロファイル] の順に移動します
  - [ユーザーのログオフ時にユーザー レジストリを強制的にアンロードしない] の設定を開き、[未構成] から [有効] に変更します
8. データ収集は、名前 ExchangeOnlineAssessment のスケジュールされたタスクにより、前のスクリプトの実行後 1 時間以内、それから 7 日ごとにトリガーされます。タスクは、別の日時に実行するように変更できます。また強制的に即実行することもできます。





評価結果での作業のガイダンスと詳細については、Services Hub リソース センターの[評価結果での作業](#)にアクセスしてください。

9. データ収集のアカウントで MFA を使用している場合もまた、必要な回数だけ Office 365 から手動でデータを収集する必要があります。このコレクションは、次の PowerShell スクリプトを実行することにより、実行されます：

C:\¥EXOA

```
|-- ExchangeOnlineAssessment
```

```
    |-- [番号付きのフォルダー]
```

```
        |-- Temp
```

```
            |-- Exchange.0365
```

```
                |-- EXO_Master.ps1
```

**注意：** このフォルダーは、スケジュールされたタスクが一度実行されてからのみ、利用できます。

Office 365 アカунツの資格情報を入力し、MFA のプロンプツに応答する必要があります。PowerShell スクリプトが完了したら、スケジュールされたタスクを再実行し、収集されたデータを更新します。

## 付録

### データ収集メソッド

Office 365 Exchange 評価では、複数のデータ収集メソッドを使用し、環境から情報を収集します。このセクションでは、環境からデータを収集するために使用されるメソッドについて説明します。データ収集に Microsoft Visual Basic (VB) のスクリプトは使用していません。

データ収集ではワークフローとコレクターを使用します。コレクターは次のとおりです：

Microsoft Graph API

Microsoft Exchange Online PowerShell

#### Microsoft Graph API

Microsoft Graph API は、Office 365 セキュア スコアに関するデータを取得するために使用されます。

#### Microsoft Exchange Online PowerShell

PowerShell は、Azure AD と Office 365 の両方のデータを収集するために使用されます。PowerShell では、Azure PowerShell からのコマンドレット、Exchange Online Management Shell とパターンとプラクティス (PnP) コマンドレットを使用し、テナントに関する必要な構成設定に接続してプルします。

### Office 365 評価 - 認証モデル

Office 365 評価では、次の 2 つのメソッドを使用してデータを収集します：

1. Microsoft Graph
2. PowerShell コマンドレット

#### Graph API

評価では、Azure で作成したアプリを使用して、Microsoft Graph に接続し、そこからデータを抽出します。アプリへの読み取りのアクセス許可が OAuth を使用して付与されています。データ収集マシンには、Microsoft Graph から順番にデータを取得する Azure アプリに接続するために使用される証明書が与えられています。評価のセットアップ中に、アプリを作成し、それに関連する読み取りのアクセス許可を付与し、Microsoft Graph に対してクエリを実行できるようにするためには、グローバル管理者が必要です。セットアップが完了したら、この部分の評価では、アカウントの要求なしで、証明書を介してアプリでデータを収集します。アプリには、特権モデルを使用してデータ収集するのに役立つ、読み取りアクセス権のみ与えられています。

#### PowerShell コマンドレット

また、この評価では、次のコマンドレットを使用して Office 365 からデータを収集します：

- Azure AD コマンドレット
- Exchange Online コマンドレット

現在、これらのコマンドレットは、手動で実行するために設計された、ログインの先進認証をサポートしています。これは、認証要求を処理するよう求めるプロンプトにより、MFA を使用するアカウントに対して先進認証のサポートが行われるということです。この評価では、スケジュールされたタスクを介して自動化された方法で、データを収集します。このようなデータ収集は、プロンプトが生成されることなく、自立的に実行されるように設計されています。これは、認証中に MFA のアカウントのプロンプトが表示されないためにアカウントが認証できない場合、MFA が有効なアカウントに関する問題を引き起こします。現在、OAuth をサポートするコマンドレットでは、PG を使用しています。OAuth を完全にサポートするコマンドレットを使用すると、Azure アプリを使用し、コマンドレットからの要求を認証できるようになります。その際、この操作により、MFA が有効なアカウントの使用時に手動でデータを収集するための現在の要求と、Global Admin アカウント全体を使用するための要求が削除されます。

### Exchange Online 評価のセットアップのトラブルシューティング

オンデマンド評価のトラブルシューティング全般に関するガイド

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

Office 365 URL および IP アドレス範囲

Office 365 にはインターネットへの接続が必要です。次の記事に一覧表示されているエンドポイントに到達できる必要があります

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

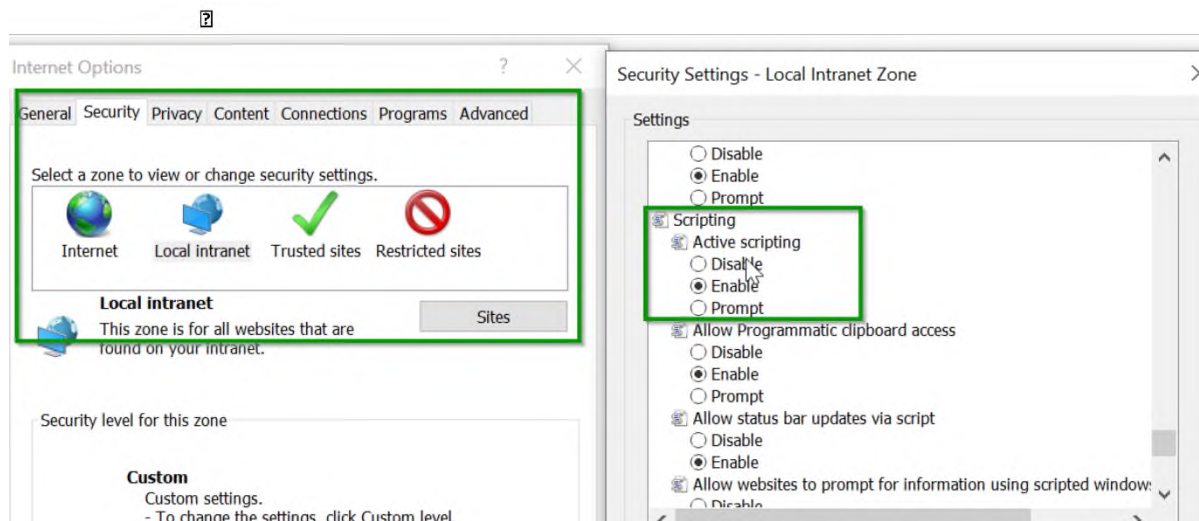
### New-MicrosoftAssessmentApplication

評価アプリケーションを正しくセットアップするために、所定の場所に URL 制限がある場合は、次の URL をホワイトリストに登録していることを確かめる必要があります：

URL
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:443">www.powershellgallery.com:443</a>

上記の URL と共に、以下の設定が、ページ上で実行するために必要な JavaScript として Internet Explorer で有効になっていることを確認してください。

### インターネット オプション セキュリティの設定



New-MicrosoftAssessmentsApplication コマンドの実行中に、認証画面を表示できるように信頼済みのサイトに追加のリンクを追加するようメッセージが表示されることがあります。これは、ポップアップに表示される [追加] ボタンをクリックして、追加することができます。

### 前提条件のエラー

前提条件のエラーが発生した場合は、以下に示すように、イベント ビューアーでエラーを確認してください：

