

ESA 用 Microsoft Azure AD および Office 365 の設定方法

目次

[概要](#)

[前提条件](#)

[設定 認証 値](#)

[設定 Microsoft 紺碧 AD](#)

[カスタム Webアプリケーションを作成して下さい](#)

[カスタム Webアプリケーションを設定して下さい](#)

[明らかな作成して下さい](#)

[借用者 ID を見つけること](#)

[保存されるべき値の最終的なレビュー](#)

[ESA の設定 メールボックス設定](#)

概要

この資料に Microsoft 紺碧 AD およびオフィス 365 を Cisco E メール セキュリティ アプライアンス (ESA) を使用するためにセットアップおよび設定する方法を記述されています。

前提条件

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

• E メール セキュリティ 9.9.5-039 (ベッラージョ) 用の AsyncOS、またはより新しい。
この資料はまた次を必要とします:

- [オフィス 365 アカウント サブスクリプション](#) ([オフィス 365 アカウント サブスクリプション](#) が E-メールを送るためにアクセスが含まれている企業 E3 または企業 E5 アカウントのようなことを確かめて下さい。)
- [Microsoft 紺碧](#) アカウント
- オフィス 365 および Microsoft 両方紺碧 AD アカウントは `user@domain.com` アクティブな eメールアドレスにきちんと結ばれ、そのドメインおよびアカウントによって電子メールを送信し、受信できます。
- Windows サーバから通常管理される Windows PowerShell に、アクセスして下さい。
- 公共/私用 認証を作成するドメイン アクティブなパブリック/私用 認証に署名するのに使用される認証およびプライベートキーまたは認証に署名するのに使用されるプライベートキーを保存する機能および能力。

設定 認証 値

Windows にログインすれば、PowerShell を使用して `$keyid`、`$base64Thumbprint` および `$base64Value` をマッピングし、得る次のコマンドを完了して下さい:

1. \$cer = 新しいオブジェクト System.Security.Cryptography.X509Certificates.X509Certificate2
2. \$cer. インポート (「C:\path_to_cert\PEM_certificate.crt」)
3. \$bin = \$cer.GetRawCertData()
4. \$base64Value = [System.Convert]::ToBase64String(\$bin)
5. \$bin = \$cer.GetCertHash()
6. \$base64Thumbprint = [System.Convert]::ToBase64String(\$bin)
7. \$keyid = [System.Guid]::NewGuid().ToString()
8. エコー \$base64Value
9. エコー \$base64Thumbprint
10. エコー \$keyid

この資料の為に、設定例は「esatest.onmicrosoft.comに基づいています」。PowerShellによって実行されるようにコマンドは次の例に類似したではありません:

Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

```
PS C:\Users\Administrator> cd .\Desktop
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> $cer = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2
PS C:\Users\Administrator\Desktop>
$cer.Import('C:\Users\Administrator\Desktop\esatest.onmicrosoft.com_PEM.crt')
PS C:\Users\Administrator\Desktop> $bin = $cer.GetRawCertData()
PS C:\Users\Administrator\Desktop> $base64Value = [System.Convert]::ToBase64String($bin)
PS C:\Users\Administrator\Desktop> $bin = $cer.GetCertHash()
PS C:\Users\Administrator\Desktop> $base64Thumbprint = [System.Convert]::ToBase64String($bin)
PS C:\Users\Administrator\Desktop> $keyid = [System.Guid]::NewGuid().ToString()
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $base64Value
MIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwZcxzCzAJBgNVBAYTAlVTMRcwFQYDVQQLIEw50b3J0aCBDYXJv
bGluYTEEMMAoGAlUEBxMDU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGAlUECzMDVEF
DMSAwHgYDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnAY2lzy28uY29tMB4
XDTE2MDMyODE0NTYwMFoXDTE2MDMyODE0NTYwMFoZc2cxzCzAJBgNVBAYTAlVTMR
cwFQYDVQQLIEw50b3J0aCBDYXJvYXV0bGluYTEEMMAoGAlUEBxMDU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGAlUECzMDVEFDMSAwHg
YDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYSc
m9ic2hlcnAY2lzy28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzB6r/MtfKwG+86eHzdhyKlCdyT+j
/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
axulraQeZgY/dkyHkTE26vt6rpy5g611TLlotZGLF0nkzT5Gs+zLOuhPHat1DMU70LCXh8CHs2cLsczpdWfb20sHxTVlISVJ
qjdhYHYM7vc6VNfemYIYxAE90ZE19QH0dU5n7spPyxUP0fp8z8gHsQ7HhRTsCNg
WbFyYb0Ib1RTOznzmXaSONRKYaIpkLkOSwZurT0wyGJd+TZSw+RgsX1vKJNmKih/iilYlVMkyq+T7PjBPDwhU8uAGQIDAQA
Bo4HWMIHMTMAwGAlUEwQFMAMBAF8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGCcGCC
sGAQUFBwMBBggrBgEFBQcDQAgYIKwYBBQUHAwQCisGAQQBgjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgj
cKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQGA1UdeEQ9MDuCF2VzYXRlc
3Qub25taWVyb3NvZnQuY29tSByb2JzaGVyd0Blc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTANBgkqhkiG9w0BAQUFAAOCAQEAR
/F2tqxBrIYK8fEt0swLzQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625
f31o1kADPcK3ml0UarT35hH6f9abZSXm3mj3zMnuK5nW2ypDCVUiuA2C51+woEubSmvn980GHuSXOqfLMPtniUMTubp+SIDC
rtCse2l2GkE1OCRmxFlwtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Z
xg8NKtiyEzV990J6+DokMn1fQOXDBPkgHIlmzFmVQogUGDCVbvpsdlroT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj
l+guS0X0FMmhkDJOTyZWnAQ==
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $base64Thumbprint
3DLH9EgquMPdkMrUj/Faljxa+XU=
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $keyid
89ed56fc-7fae-4d10-ad63-7ddaeaf8e737
```

これらの値が作成の使用された以降この資料の明らかなセクションであるので、によって \$keyid のために表示される出力、\$base64Thumbprint および \$base64Value を保存して下さい。

\$base64Thumbprint は ESA 設定の間に使用されます。

注: 単一行であるために `$base64Value` が編集されるために必要となります。

認証 (.pem) にローカルで署名するのに使用される公開鍵 証明書 (.crt) およびプライベートキーを保存して下さい。 プライベートキーは ESA 設定の間に必要です。

設定 Microsoft 紺碧 AD

カスタム Webアプリケーションを作成して下さい

1. [Microsoft 紺碧](#) にログインして下さい。
2. **すべての ITEM** へのナビゲート。
3. ドメインのリソース名をクリックして下さい。
4. リソース名のためのツール タブから、『Applications』を選択して下さい。

Microsoft Azure | Check out the new port | CREDIT STATUS | @esatest.onmicrosoft.com

cisco tac (content security)

USERS | GROUPS | APPLICATIONS | DOMAINS | DIRECTORY INTEGRATION | CONFIGURE | REPORTS

LICENSES

Show Applications my company uses Search Application name or Client ID

NAME	PUBLISHER	TYPE	APP URL
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us...
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlo...
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/share...
Office 365 Yammer	Microsoft Corporation	Web application	https://products.office.com/yam...
Skype for Business Online (prev...	Microsoft Corporation	Web application	

+ NEW | ADD | VIEW ENDPOINTS | 1 ! ?

5. 一番下ツールバーから、『Add』を選択して下さい

:

+ NEW |  ADD | VIEW ENDPOINTS | 1 ! ?

6. 「何を示されたときしたいと思いませんか。」、**組織が開発しているアプリケーションを『Add』**を選択して下さい。
7. 適切な名前で作成し、**Webアプリケーションや Web API**として型を残し、続くために矢印をクリックして下さい:

Tell us about your application

NAME

ESA_Beta

Type

WEB APPLICATION AND/OR WEB API [?]

NATIVE CLIENT APPLICATION [?]



8. ドメインのためのカスタム Webアプリケーションを終わり、次の値を追加することを入力し終わるためにチェックをクリックするため: サインオン URL: `https://<your.domain.com>/ManualRegistration` APP ID URI: `https://<your.domain.com>`

App properties

SIGN-ON URL ?

APP ID URI ?



9. [アプリケーション ID URI](#) に関する Microsoft から、：「アプリケーション ID URI は論理的な識別子であるので、インターネット アドレスに解決する必要はありません。それはアプリケーションによって単一 サインオン 要求を紺碧 AD に送信 するとき示されます。紺碧 AD はアプリケーションを識別し、アプリケーション登録の間に提供された応答 URL へのサインオン応答 (SAML トークン) を返します。wtrealm プロパティ (WS フェデレーションのために) または発行元プロパティを設定 するのにアプリケーション ID URI 値を (SAML-P のために) サインイン要求を作った場合使用して下さい。 **アプリケーション ID URI は組織の紺碧 AD の固有の値である必要があります**」。

注：「外部ユーザ向けのアプリケーションを有効にした場合、アプリケーションのアプリケーション ID URI の値はディレクトリの確認されたドメインの 1 つのアドレスである必要があります。その結果、それは壺である場合もありません。この安全対策は他の組織が (規定することおよび) 組織に属する一意のプロパティを奪取 することを防ぎます。開発の間に、組織の最初のドメインの位置に (カスタム/虚栄心ドメインを確認しなかったら) App ID URI を変更でき、New 値これを使用するために app をアップデートします。最初のドメインは contoso.onmicrosoft.com のような参加する」。作成する 3 レベル ドメインです

設定カスタム Webアプリケーション

1. カスタム Webアプリケーションが作成されたら、カスタム Webアプリケーション自体に自動的にナビゲート されます。ここから、ツール タブで、『Configure』を選択 して下さい
：

Microsoft Azure | Check out the new port | CREDIT STATUS | @esatest.onmicrosoft.com

esa_beta

DASHBOARD USERS **CONFIGURE** OWNERS

Your app has been added!
Enable your app to integrate with Microsoft Azure AD
 Skip Quick Start the next time I visit

GET STARTED

- ▶ ENABLE USERS TO SIGN ON
- ▶ LEARN: MICROSOFT AZURE AD FEATURES FOR DEVELOPERS

CONFIGURE

- ▶ ACCESS WEB APIS IN OTHER APPLICATIONS
- ▶ EXPOSE WEB APIS TO OTHER APPLICATIONS
- ▶ CONFIGURE MULTI-TENANT APPLICATION

2. この画面から、作成されるようにサインオン URL および他のコンフィギュレーションの詳細を見ることができます。注: クライアントIDはこの画面にリストされています。この値は ESA 設定の間に必要です。

Microsoft Azure | Check out the new port | CREDIT STATUS | @esatest.onmicrosoft.com

esa_beta

DASHBOARD USERS CONFIGURE OWNERS

properties

NAME: ESA_Beta

SIGN-ON URL: https://esatest.onmicrosoft.com/ManualRegistration

LOGO: [Blue cube icon]

APPLICATION IS MULTI-TENANT: YES NO

CLIENT ID: 19d048bb-1c44-401b-b1fa-a61d67a9caca

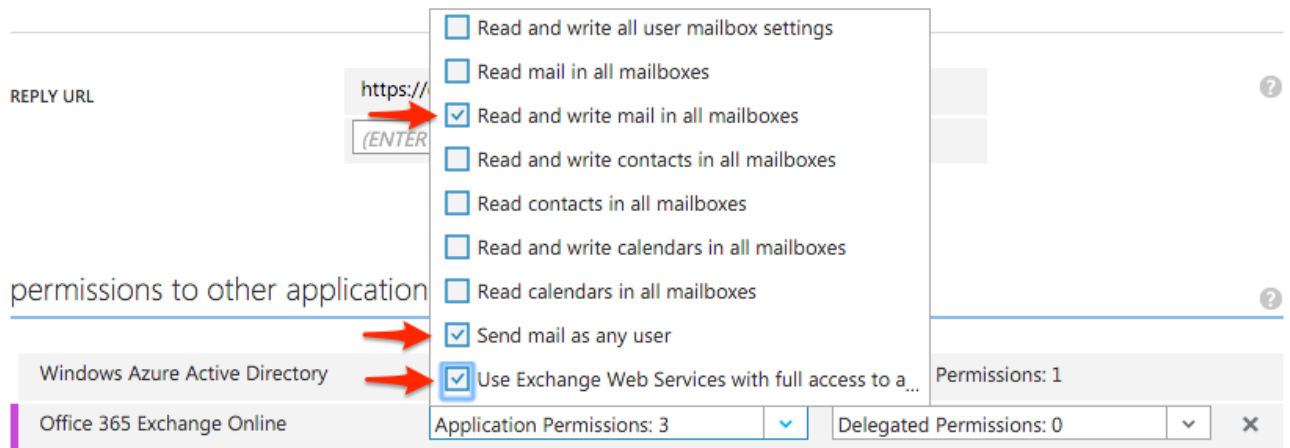
3. カスタム Webアプリケーション 設定のためのこの同じ画面から、下部のにスクロールし、アプリケーションを『Add』 をクリックして下さい

permissions to other applications

Windows Azure Active Directory	Application Permissions: 0	Delegated Permissions: 1
--------------------------------	----------------------------	--------------------------

Add application

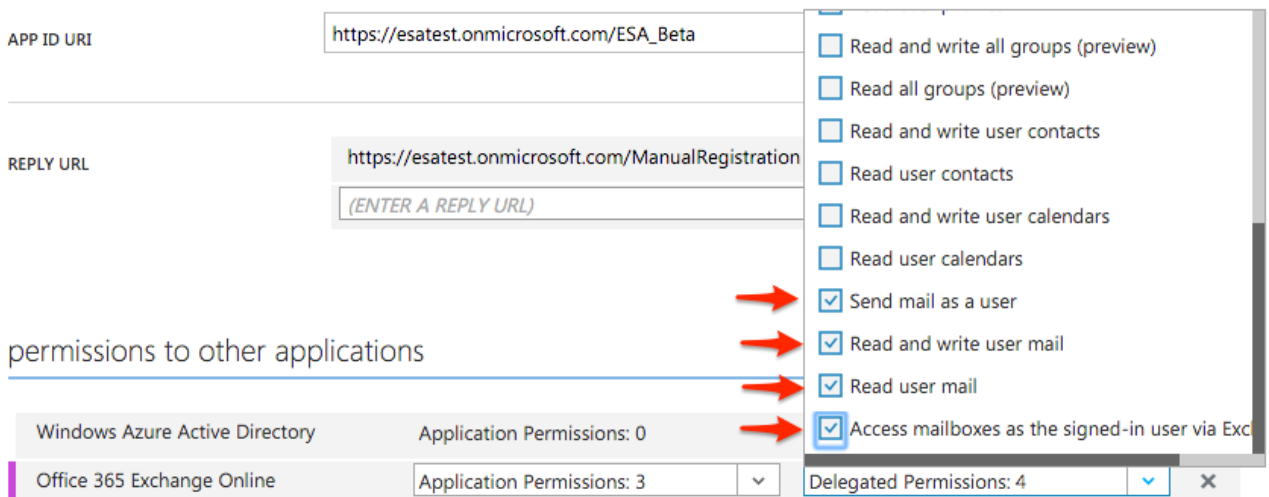
4. オフィス 365 Exchange オンラインを選択し、続くためにチェックをクリックして下さい。
5. オフィス 365 Exchange OnlineApplication 権限に関しては、読まれる選択し、すべてのメールボックスにあらゆるユーザとしてメール、メール送信、およびフルアクセスを用いる使用 Exchange Web サービスを...書いて下さい



Add application

6. オフィス 365 Exchange Online Delegated 権限に関しては、ユーザが、読み、ユーザ メールを書き、ユーザ メールを読み、ユーザ署名のとして Exchange によってメールボックスにアクセスするようにメールを『Send』を選択して下さい

:



Add application

7. カスタム Webアプリケーションのためのすべての作業および設定を保存するために一番下ツールバーから『SAVE』をクリックして下さい

:



明らかな作成して下さい

1. カスタム Webアプリケーションが保存およびアップデートを完了したら、明らか > 一番下ツールバーから明らかなダウンロード『Manage』をクリックして下さい

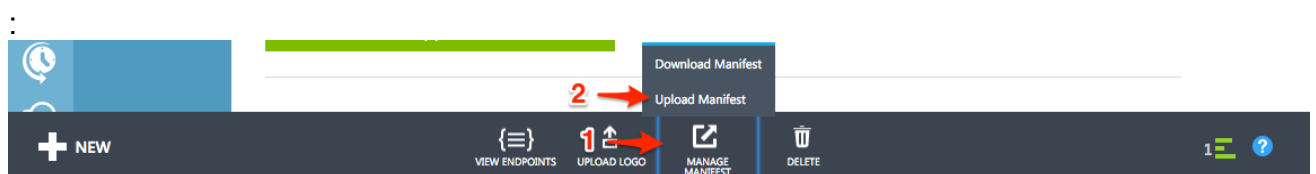
:



2. 応答によってナビゲートし、ローカル コンピュータに .json 形式で明らかな Webアプリケーションを保存して下さい。
3. この .json ファイルを見つけ、テキストエディタとこの .json ファイルを開いて下さい。
(望ましい Notepad++、原子、等)
4. 「keyCredentials」行を検索し、見つけて下さい。
5. 設定 認証 値 セクション (\$base64Thumbprint、\$keyid および \$base64Value) からのより早い識別された資格情報を使用して次の複数の回線が付いているこの単一行、およびカスタマイズを取り替えます:
6. "keyCredentials": [


```
{
        "customKeyIdentifier": "$base64Thumbprint",
        "keyId": "$keyid",
        "type": "AsymmetricX509Cert",
        "usage": "Verify",
        "value": "$base64Value"
      }
    ],
```
7. \$base64Value を入力した場合、これが単一行値であるために編集されるために必要となる、先に注意される。
8. この資料の初めから作成されるように例と続いて、修正された keyCredentials は次の通りです:
9. "keyCredentials": [


```
{
        "customKeyIdentifier": "3DLH9EqnuMPdkMrUj/Faljxa+XU=",
        "keyId": "89ed56fc-7fae-4d10-ad63-7ddaeaf8e737",
        "type": "AsymmetricX509Cert",
        "usage": "Verify",
        "value":
          "MIEEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwZcxXjBzEMMAoGAlUECwMDVEFDMSAwHgYDVQQDExdlc2F0Z
          XN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY2l2Y28uY29tMB4XDTE2MDMyODE0NTYw
          MFoXDTE2MDMyODE0NTYwMFowZcxXjBzEMMAoGAlUECwMDVEFDMSAwHgYDVQQDExdlc2F0ZGN0Lm9ubWljcm9zb2Z0LmNvbT
          EhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY2l2Y28uY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz
          B6r/MtFkKg+86eHzdYk1CdyT+j/j/+5yM6W9K8rqhW0FFT8et0vj402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
          axulraQeZgY/dkyHkTE26vt6rpy5g611TLloTZG1F0nkzT5Gs+zL0uhPHaT1DMU70LCXh8CHS2cLsczpdWfb20sHxTV
          lISVJqjdhYHYM7vC6VNfMYIYxAE90ZEL9QH0du5n7spPyxUP0fp8z8gHsQ7HhRTsCNgWbFyYb0Ib1RTOznmzMXaSon
          RKYaIpkLkOSwZurT0wyGJd+TZSw+RgsXlvKJNmKih/iilYLvMKYq+T7PJbPDwhU8uAGQIDAQABo4HWMHTMAwGAlUdE
          wQFMAMBAf8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAWQCisGAQQB
          gjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgjcKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQ
          GAlUdEQQ9MDuCF2VzYXRlc3Qub25taWVyb3NvZnQuY29tSByb2JzaGVyY29tY29tY29tY29tY29tY29tY29tY29tY29t
          ANBgkqhkiG9w0BAQUFAAOCAQEAR/F2tqxBrIYK8fEt0swLzQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625f
          31o1kADPcK3ml0UarT35hH6f9abZSxm3mj3zMnuK5nW2ypDCVUiuA2C5l+woEubSsmvn980GHuSXOqfLMPtniUMTubp+
          SICDrtCse2l2GkE1OCRmxF1wtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Zxg8NKtiyEzV990J6+DokMnlf
          QOXDBPkgHI1mzFmVQogUGDcVbvpsdlroT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqjl+guS0X0FMmhkDJOTyZ
          WnAQ=="
      }
    ],
```
10. .json ファイルをローカルで保存して下さい。
11. ブラウザおよび Microsoft 紺碧ポータルに戻って下さい。
12. 明らか > 明らかなアップロード 『Manage』 をクリックして下さい



13. 参照し、編集された .json ファイルを見つけ、アップロードを完了するためにチェックマ

クを選択して下さい。

借用者 ID を見つけること

1. Microsoft 紺碧 AD で統合エンドポイントを表示するために**エンドポイント**を『View』をクリックして下さい。
2. URL を使くと、各行の同じような値に、これによってが**借用者 ID**である "ed437e13-ba50-479e-b40d-8affa4f7e1d7," 注意して下さい。



App Endpoints

If you are developing an app that integrates with Microsoft Azure AD, update your code to use these endpoints for single sign-on and directory access.

FEDERATION METADATA DOCUMENT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



WS-FEDERATION SIGN-ON ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



SAML-P SIGN-ON ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



SAML-P SIGN-OUT ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



MICROSOFT AZURE AD GRAPH API ENDPOINT

<https://graph.windows.net/ed437e13-ba50-479e-b40d-8affa4f7e1d7>



OAuth 2.0 TOKEN ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



OAuth 2.0 AUTHORIZATION ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



これはアプリケーションおよび設定にユニークです。 ESA の後期コンフィギュレーションのこの値を記録して下さい。

保存されるべき値の最終的なレビュー

次の値は使用のための Microsoft 紺碧 AD 設定の間に ESA のメールボックス設定を行った場合記録する必要があります:

設定 認証 値から:

- プライベートキー 認証 (.pem)
- \$base64Thumbprint

設定カスタム Webアプリケーションから:

- クライアントID

借用者 ID を見つけることから:

- 借用者 ID

ESA の設定 メールボックス設定

完全な Microsoft 紺碧 AD 設定によって ESA を通信し、検証してもらって準備ができています。

1. GUI による ESA アプリアンスへのログイン。
2. システム 管理 > メールボックス設定の下のイネーブル オフィス 365 メールボックス設定。
3. ESA アプリケーションを認証の拇印及びプライベートキーと共に登録している間「イネーブル オフィス 365 メールボックス設定」チェックボックスを選択して下さい及び Microsoft 紺碧 AD を取得する Microsoft 紺碧 AD 詳細に (クライアントID 及び借用者 ID) 与えて下さい。
4. メールボックス設定への変更を保存するために『SUBMIT』をクリックして下さい。
5. 設定されるようにオフィス 365 ドメインのためのこの時に Microsoft 紺碧 AD への接続をテストする必要があります

:

Mailbox Settings

Success — The settings were configured successfully . You must test the connection.

Office 365 Mailbox Settings	
Azure AD Details:	Client ID: 19d048bb-1c44-401b-b1fa-a61d67a9caca Tenant ID: ed437e13-ba50-479e-b40d-8affa4f7e1d7 Thumbprint: 3DLH9EqnuMPdkMrUj/Fa1jxa+XU= Certificate Private Key: Successfully uploaded
Check Connection...	Edit Settings...

6. アクティブの使用すればアカウントの有効な eメールアドレスは、接続を『Test』をクリックします

Connection Check

Connection Parameters

Office 365 Email Address:

[Test Connection](#)



Connection Status

Connected to Azure AD.
Connection Successful.
Inbox count of Messages are 0

[Done](#)

- 接続ステータスが正常、接続チェックを完了するために『Done』をクリックして下さい。
- 最終的には、ESA ですべてのコンフィギュレーション変更を保存するために託しますをクリックして下さい。