# ESA の Azure AD およびオフィス 365 メールボックスの設定方法設定

## 目次


はじめに
前提条件
要件
背景説明
ESA の Azure AD およびオフィス 365 メールボックスの設定方法設定
Azure の新規アプリケーションを登録して下さい
アプリケーションのための必要なアクセス許可を設定して下さい
アプリケーションの明らかの準備をして下さい
明らか編集して下さい
（オプション）明らかのダウンロードして下さい
（オプション）明らかのアップロードして下さい
アプリケーションのためのクライアントID を得て下さい
アプリケーションの借用者 ID 値を取得して下さい
必要な値を確認して下さい
ESA を設定して下さい
ESA のトラブルシューティング
Azure AD のトラブルシューティング
（オプション）標準的なポータルを使用して Azure のアプリケーションを作成し設定する方法を
アプリケーションを追加して下さい
アプリケーションを設定して下さい
明らかの管理して下さい
借用者 ID を見つけること
関連情報


## 概要

この資料は Windows Azure の新規アプリケーションを登録し、Cisco E メール セキュリティ アプライアンス（ESA）のオフィス 365 メールボックス設定のための設定を完了するために必要な値を得るためにステップバイステップ「ハウツー」を、提供したものです。 ESA 管理者が ESA のメール ポリシー設定の Advanced Malware Protection （アンペア）のためのメールボックス オート治療（3 月）を設定するときこれが必要となります。

## 前提条件

### 関連製品

この資料は次に適用します:

- すべての ESA、ハードウェアおよびバーチャル実行 10.x およびより新しい

- 10.x を実行するすべてのクラウド E メール セキュリティ（CES）ESA およびより新しい

## 要件

この資料は次を必要とします:

- オフィス 365 アカウント サブスクリプションが企業 E3 または企業 E5 アカウントのような Exchange へのアクセスが、含まれていることをオフィス 365 アカウント サブスクリプション（確かめて下さい。）
- Microsoft Azure アカウント
- オフィス 365 および Microsoft Azure AD アカウントは両方 *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メールを送信し、受信できます。
- から通常 Windows ホストかサーバを管理される Windows PowerShell に、アクセスして下さい。
- 公共/私用証明書を作成するドメイン アクティブなパブリック/私用証明書に署名するのに使用される証明書およびプライベートキーまたは証明書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。

Azure AD に戻って ESA メールボックス コネクタを設定するために次の 4 つの値を作成します:

1. クライアントID
2. 借用者 ID
3. 拇印
4. .pem フォーマットの証明書 プライベートキー

これらの必要な値を構築するために、この資料のステップを完了する必要があります。 開始する前に、Windows Powershell で次を実行する必要があります:

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**

**注:** #2 に関しては、証明書にパス**によって「C:\path _to_cert \ PEM_certificate.crt」を**取り替えて下さい。

$base64Thumbprint = *拇印*。 必要な値の前提条件リストにこの値を追加して下さい。

**ヒント**： それらがコンフィギュレーションのステップの必要とされた以降であるので、出力を *$base64Value*、*$base64Thumbprint* および *$keyid* のためにローカルで保存して下さい。 現時点で、証明書の .crt が完了します。 コンピュータの利用可能な、ローカル フォルダで証明書の関連する .pem を持って下さい。

# 背景説明

Microsoft は紺碧ポータルの 2 つのバージョンへのアクセスを許可します:

- https://manage.windowsazure.com （標準的なポータル）
- https://portal.azure.com （新しいポータル）

左手ツールバーによって新しいポータルから「標準的なポータル」にアクセス選択します「Azure Active Directory」を > 標準的なポータルできます

この資料の目的で、アプリケーションの登録および設定は新しいポータルで行われます。 「標準的なポータル」の使用へのステップはこの資料の終わりに含まれています。 （標準的な紺碧ポータルを無効に することを Microsoft はいつかで選択するかもしれません。）

# ESA の Azure AD およびオフィス 365 メールボックスの設定方法設定

## Azure の新規アプリケーションを登録して下さい

1. 紺碧ユーザインターフェイスにアクセスして下さい: https://portal.azure.com/
2. 左メニューバーは、**サービス > SECURITY + 識別を**『More』 をクリック します: **アプリケーション登録**
3. アプリケーション登録ペインから、**+Add を**クリックして下さい
4. アプリケーションの名前を作成して下さい
5. アプリケ- ションタイプに関しては、**Web app/API** として去って下さい
6. サインオン URL に関しては、次の形式を使用して下さい: https://*<company_domain.com>/ManualRegistration***注:** *<company_domain.com> は*ドメイン ユーザがサインイン O365 ドメインにアクセスするためにできる O365 のドメイン *であり。*
7. 『Create』 をクリック して下さい

## アプリケーションのための必要なアクセス許可を設定して下さい

1. ちょうど登録したアプリケーションのために関連付けられる「表示名」をクリックして下さい
2. 設定ペインでは、API アクセスのために、**必要なアクセス許可を**クリックして下さい
3. **+Add を**クリックして下さい
4. 「API アクセス」ペインで、『SELECT』 をクリック します **API を**追加して下さい
5. 「選択すれば API」ペインで、クリックして下さい **Office 365 Exchange Online （Microsoft Exchange）を**
6. ページの一番下に『SELECT』 をクリック して下さい
7. アプリケーション権限に関しては選択して下さい:
   - すべてのメールボックスにフルアクセスと Exchange Web サービスを利用して下さい
   - ユーザとしてメール送信
   - すべてのメールボックスにメールを読み、書いて下さい
8. delegated 権限に関しては選択して下さい:
   - ユーザとしてメール送信
   - ユーザ メールを読み、書いて下さい
   - ユーザ メールを読んで下さい

• Exchange Web サービスによってユーザ署名のとしてメールボックスにアクセスして下さい
9. ページの一番下に、これ閉じます「選択します API」ペインを『SELECT』 をクリック して下さい
10. ページの一番下に、これ閉じます「追加します API アクセス」ペインを『Done』 をクリック して下さい
11. **アクセス許可権限を**クリックして下さい
12. 「プロンプト表示されたときワーキング ディレクトリのすべてのアカウントの myESA のために下記の権限を与えたいと思うためにか。 この操作はこのアプリケーションが既に下記にリストされているものを一致するならない既存の権限をアップデートします。」、『Yes』 をクリック して下さい

今 2 API 「Windows Azure Active Directory」および「Office 365 Exchange Online」をリストしてもらうはずです。

次の セクションを続行するために登録されていたアプリケーション ペインに戻る必要があります:

1. 「必要なアクセス許可」ペインを閉じるために「X」クリックして下さい
2. 「設定」ペインを閉じるために「X をクリックして下さい

登録されていたアプリケーション ペインに今あります。

## アプリケーションの明らかの準備をして下さい

### 明らか編集して下さい

1. 登録されていたアプリケーション ペインから、ツールバーの明らかクリックして下さい
2. エディタで完全の明示します示されます。 exisiting 「keyCredentials」行を見つけて下さい。 次と「keyCredentials だけ」取り替えます:

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

3. 値と $base64Thumbprint、$keyid および $base64Value を取り替える必要があります 示されているようにすべての値のまわりで引用符 ( "" ) を、残して下さい各値がたった 1 つの行であること $base64Thumbprint を含む特別な注意を、注意して下さい
4. アプリケーションをアップデートするために『SAVE』 をクリック して下さい。 ツールバー エリアの「更新済みのアプリケーション」表記を正常に見るはずです。

次の セクションを続行するために登録されていたアプリケーション ペインに戻る必要があります:

「閉じるために編集します明らかな」ペインを"X"を クリックする。

### ( オプション ) 明らかのダウンロードして下さい

**ヒント**： 明らかののために内部 Azure エディタを使用正常にできた場合明らかなダウンロードをスキップし、明らかアップロードすることができます。 そうでなかったら、手動で明らかの編集する必要があり続行して下さい。

1. 登録されていたアプリケーション ペインから、ツールバーの明らかクリックして下さい
2. 編集明らかなメニューで『Download』 をクリック して下さい
3. 証明書が含まれているディレクトリに明らかの保存して下さい。 これはコンピュータに .json 形式の明らかのローカルで保存します。
4. ローカル エディタ ( Wordpad++、原子、等 ) を使用する、からの完全なステップ 2 および 3 は「この資料の明らかな」セクションを編集します
5. 明らかな .json ファイルをローカルで保存して下さい

### ( オプション ) 明らかのアップロードして下さい

ダウンロードすることを選択し、明らかの手動で編集した場合、編集された明らかのアップロードする必要があります:

1. ブラウザおよび Azure ポータルに戻って下さい
2. から「編集します明らかな」ペインを『Upload』 をクリック して下さい

次の セクションを続行するために登録されていたアプリケーション ペインに戻る必要があります :

「閉じるために編集します明らかな」ペインを"X"を クリックする。

## アプリケーションのためのクライアントID を得て下さい

1. 登録されていたアプリケーションから見つけて下さい「アプリケーション ID」を
2. コピーして下さいアプリケーション ID ( アプリケーション ID = *クライアントID* ) を
3. 必要な値の前提条件リストにこの値を追加して下さい。

## アプリケーションの借用者 ID 値を取得して下さい

1. 「アプリケーション登録」ペインから、「エンド ポイント」をクリックし、フェデレーション メタデータ ドキュメントに最初の行を選択して下さい
2. 外部エディタに行をコピー アンド ペーストして下さい
3. 「https://login.windows.net/」の後に IDストリングである *借用者 ID* を取得したいと思います
4. 必要な値の前提条件リストにこの値を追加して下さい。

例：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

この例に関しては、借用者 ID は "ed437e13-ba50-479e-b40d-8affa4f7e1d7" 才です。

### 必要な値を確認して下さい

値は今完了します。 次の値を記入できるはずです:

- クライアントID
- 借用者 ID
- 拇印（前提条件を参照して下さい）
- .pem フォーマットの証明書 プライベートキー（前提条件を参照して下さい）

ESA のこれらの値の設定によってオフィス 365 メールボックス設定を完了して準備ができています。

### ESA を設定して下さい

1. ESA GUI: **システム 管理 > メールボックス設定 > Edit 設定…**
2. 入力して下さい前のセクション（クライアントID、借用者 ID、拇印）からで値
3. ロードして下さい保存された証明書（.pem）を
4. [Submit] をクリックします。
5. 「設定がうまく行われたことを見ます。 変更を保存し、接続をテストして下さい」。
6. 上部右上隅から、**保存しますテスト**する前に**変更を**クリックして下さい
7. "Check Connection…"を クリックする そして O365 ドメインと関連付けられる既知よい、はたらく e メールアドレスで入力して下さい
8. "Test Connection"を クリックする

接続ステータスという結果に終ります成功を受け取る必要があります:

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

# ESA のトラブルシューティング

接続ステータスのための正常な結果はテストすることを見なければ、Azure AD から実行されたアプリケーション登録を検討したい場合もあります。

ESA から、3 月ログをトレース レベルに設定し、接続を再検査して下さい。

不成功な接続に関しては、ログは類似したをへの示すかもしれません:

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
```

```
],
```
（借用者 ID と同じである）アプリケーション ID、ディレクトリ ID、または Azure AD のアプリケーションのログからの他の関連する識別名を確認して下さい。 値の不確実である場合、アプリケーションを門脈 Azure AD から削除し、開始して下さい。

接続の成功に関しては、ログは類似したにであるはずです:

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

# Azure AD のトラブルシューティング

> **注:** Cisco TAC および Ciscoサポートは Microsoft Exchange、Microsoft Azure AD、またはオフィス 365 で加入者宅側問題を解決するために資格を与えられません。

加入者宅側に関しては Microsoft Azure AD においての、マイクロソフトのサポートを実行する必要があります発行します。 Microsoft Azure ダッシュボードからの「ヘルプ + サポート」オプションを参照して下さい。 ダッシュボードからのマイクロソフトのサポートに直接支援要求を開けますかもしれません。

# （オプション）標準的なポータルを使用して Azure のアプリケーションを作成し設定する方法を

> **注:** 正常に https://portal.azure.com （新しいポータル）にアクセスして Azure ポータルを使用できた場合これを完了する必要はありません。 これは紺碧管理者のためにだけ参照されますまだ「標準的なポータル」を使用するために選択する。 Azure AD ポータルのこのバージョンを使用したい場合必要な値を完了するための次のステップバイステップの説明を見つけて下さい:

## アプリケーションを追加して下さい

1. Microsoft Azure にログインして下さい。
2. 左メニューバーから、**すべての ITEM** にナビゲート して下さい
3. ドメインのリソース名をクリックして下さい
4. リソース名の下のツール タブから、『Applications』 を選択 して下さい
5. 一番下ツールバー エリアから、『Add』 をクリック して下さい
6. *「何を示されたときしたいと思いますか。」*、**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. 「*言いますアプリケーションについて私達に*」情報を記入して下さい: アプリケーションの名前を作成して下さいアプリケ– ションタイプに関しては、**Webアプリケーションや Web API** として去って下さい続くために矢印をクリックして下さい

8. アプリケーション プロパティを完了して下さい: サインオン URL に関しては、次の形式を使用して下さい: https:// *<Office365_assigned_company_domain.com>/ManualRegistration***注**: *<company_domain.com> は*ドメイン ユーザがサインイン O365 ドメインにアクセスするためにできる O365 のドメイン*であり*。APP ID URI に関しては、次の形式を使用して下さい:
   https:// < *Office365_assigend_company_domain.com* >完了するためにチェックマークをクリックして下さい

## アプリケーションを設定して下さい

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
2. **クライアントID はこの画面にリストされています。** 必要な値の前提条件リストにこの値をコピーし、追加して下さい。
3. 「他のアプリケーションへの権限」を見るためにスクリーンの一番下にスクロールして下さい。
4. **アプリケーションを**『Add』 をクリック して下さい **Office 365 Exchange Online を**選択し、続くためにチェックをクリックして下さい**アプリケーション権限**に関しては、選り抜き: **すべてのメールボックスにメールを読み、書いて下さいユーザとしてメール送信利用して下さいフルアクセスと Exchange Web サービスを…**delegated 権限に関しては、選り抜き: **ユーザとしてメール送信ユーザ メールを読み、書いて下さいユーザ メールを読んで下さい Exchange によってユーザ署名のとしてメールボックスにアクセスして下さい**
5. 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

## 明らかの管理して下さい

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. ローカルで、.json ファイルを見つけ、テキストエディタと開いて下さい。 （望ましい Notepad++、原子、等）
4. 「keyCredentials」行を検索し、見つけて下さい
5. *$base64Thumbprint*、*$keyid* および *$base64Value* *の*使用によってカスタマイズする次の複数の回線が付いているこの単一 行を置き換えます:
```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```
6. *$base64Value* *を*入力するとき、これが単一 行値に編集されるために必要となります
7. .json ファイルをローカルで保存して下さい
8. ブラウザおよび Microsoft Azure ポータルに戻って下さい
9. **明らか > 明らかなアップロード**『Manage』 をクリック して下さい
10. 編集された .json ファイルを参照し、見つけて下さい

11. アップロードを完了するためにチェックマークを選択して下さい

### 借用者 ID を見つけること

1. 一番下ツールバーから、Microsoft Azure 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. フェデレーション メタデータ ドキュメントに最初の行を選択して下さい
3. 外部エディタに行をコピー アンド ペーストして下さい
4. 「https://login.windows.net/」の後に IDストリングである *借用者 ID* を取得したいと思います
5. 必要な値の前提条件リストにこの値を追加して下さい

例：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

この例に関しては、借用者 ID は "ed437e13-ba50-479e-b40d-8affa4f7e1d7" 才です。

## 関連情報

- Cisco E メール セキュリティ アプライアンス-製品サポート
- Cisco E メール セキュリティ アプライアンス-リリース ノート
- **Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド**