

SMAIL/ Microsoft Office 365 SMTP OAuth2 認証の利用・設定

2021/06/22 初版

2021/09/10 1 版

2024/08/04 2 版

— 目次 —

| | |
|---|----|
| 1. 概要 | |
| 1) 準備 | 3 |
| 2) 設定 | 3 |
| 3) 動作確認 | 3 |
| 2. 詳細 | |
| ①Azure Active Director で OAuth 2.0 クライアント用の[クライアント ID]および [クライアントシークレット]の取得 | 4 |
| 1) 新ナビゲーションメニューから「Azure Active Directory」を表示します | 4 |
| 2) ナビゲーションメニューから[アプリの登録]-[+新規登録] | 4 |
| 3) 「アプリケーションの登録」画面で、アプリケーションの名前(任意の文字列)登録 | 5 |
| 4) [認証] - [+プラットフォームを追加] -[WEB]を選択します | 5 |
| 5) リダイレクト URI を入力し[構成]ボタンをクリックします | 6 |
| 6) ナビゲーションメニューから[証明書とシークレット]-[+新しいクライアント] | 7 |
| 7) ナビゲーションメニューから[API のアクセス許可]-[+アクセス許可の追加] | 8 |
| 8) [委任されたアクセス許可]を選択、アクセス許可 | 8 |
| 9) 概要でクライアント ID の確認 | 10 |
| ②Azure Active Director で[リフレッシュトークン]を取得 | 10 |
| 1) SmailRefreshToken.exe を起動させます | 12 |
| 2) ブラウザーでログイン許可設定をします | 12 |
| ③SmailRefreshToken.exe で正しくリフレッシュトークンが取得できれば、 実行フォルダーに、smail_refreshtoken.ini が生成されます | 12 |
| ④smail_refreshtoken.ini を smail.exe と同じフォルダーにコピーし、smail.exe を起動して、 smtp 認証に OAUTH-XOAUTH2 を選択すれば利用できます | 12 |
| 3. 動作確認 | 15 |
| 4. OAUTH 関連エラー例 | 17 |

1. 概要

Azure Active Directory は Microsoft Entra ID にサービス名が変更になりました。(2024/03/05)

本文中の Azure Active Directory は Microsoft Entra ID に読み替えてください。

1) 準備

Microsoft クラウド サービス | Microsoft Azure のアカウントが必要です。

(本参考例は MSDN の付属の Microsoft Azure を使用しております。)

※実際の設定方法は2. 詳細を参照して下さい。

① Azure Active Directory で OAuth 2.0 クライアント用の[クライアント ID]と[クライアントシークレット]の取得をブラウザアクセスで行います。

② Azure Active Directory で[リフレッシュトークン]を取得
付属の SmailRefreshToken.exe で行います。認証はデフォルトのブラウザが起動します。

ここまでで、SMAIL で OAuth2 認証を利用するための各種情報が取得できます。

この操作は一度のみです。ただし、クライアントシークレットの期限切れ等が発生した場合はリフレッシュトークンの再取得(SmailGmailRefreshToken.exe)が必要です。

2) 設定

③ SmailRefreshToken.exe で正しくリフレッシュトークンが取得できれば、実行フォルダーに、smail_refreshtoken.ini が生成されます。

④ smail_refreshtoken.ini を smail.exe と同じフォルダーにコピーし、smail.exe を起動して、smtp 認証に OAUTH-XOAUTH2 を選択すれば利用できます。

※SMTP ユーザ ID,SMTP パスワードを設定していても無視されます。(OAUTH-XOAUTH2 では必要が無いため)

3) 動作確認

以降、SMAIL は、リフレッシュトークンを利用してアクセストークンを自動で取得し、OAuth 2.0 認証でメールを送信できるようになります。

OAuth 2.0 認証の動作 OS:

| OS | Windows Server 2008 sp2 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2016 | Windows xp | Windows 7 pro | Windows 8.1 | Windows 10 pro |
|--------------|-------------------------|------------------------|---------------------|---------------------|------------|---------------|-------------|----------------|
| OAuth 2.0 認証 | △(*1) | ○ | ○ | ○ | × | ○ | ○ | ○ |

(*1)

KB4019276 パッチを利用し、TLS1.2 を利用可にすれば動作可能です。(Windows Server 2008 sp2 64BIT 版検証済み)

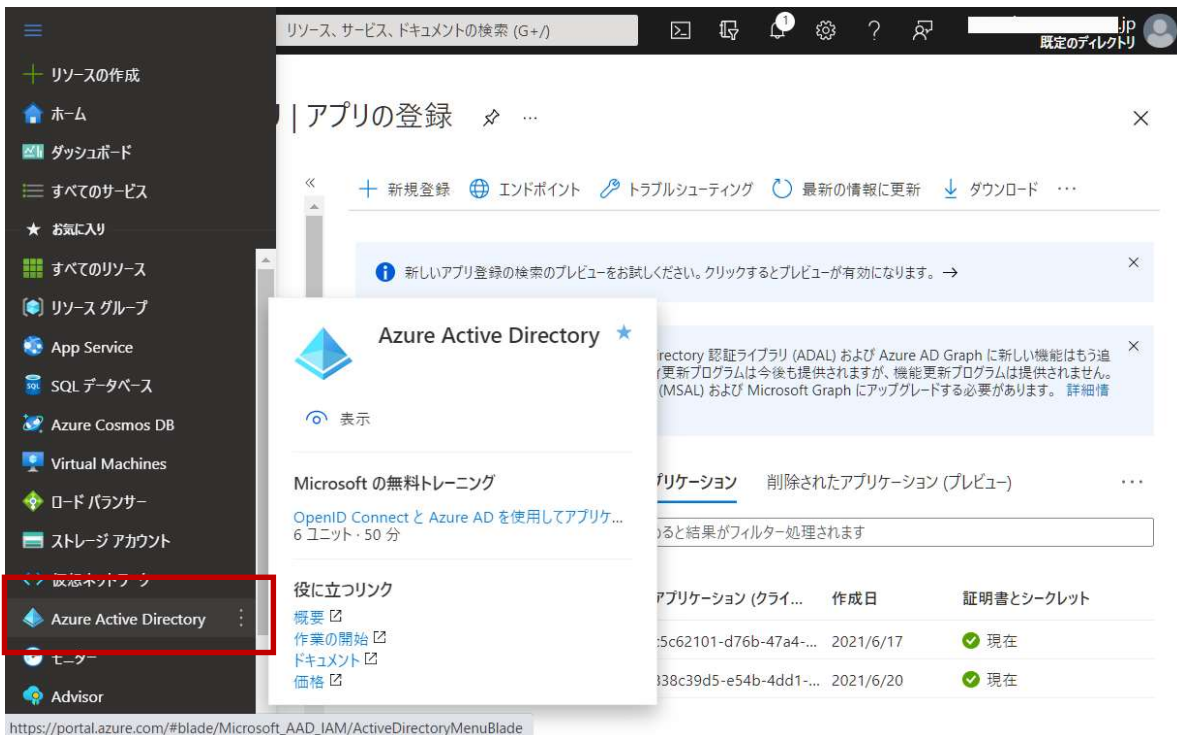
<https://support.microsoft.com/ja-jp/help/4074621/add-rds-support-for-tls-1-1-and-tls-1-2-in-windows-server-2008-sp2>

2. 詳細 (実際の取得方法)

① Azure Active Director で OAuth 2.0 クライアント用の[クライアント ID]および[クライアントシークレット]の取得

Azure Active Directory を操作できる管理者アカウントで Azure Portal(<https://portal.azure.com/>)にログインする。
(本参考例は MSDN の付属の Microsoft Azure を使用しております。)

1) ナビゲーションメニューから「Azure Active Directory」を表示します。



2) ナビゲーションメニューから[アプリの登録]-[+新規登録]をクリックします。



3) 「アプリケーションの登録」画面で、アプリケーションの名前(任意の文字列)を入力し登録して下さい。

例では smail-common とします。

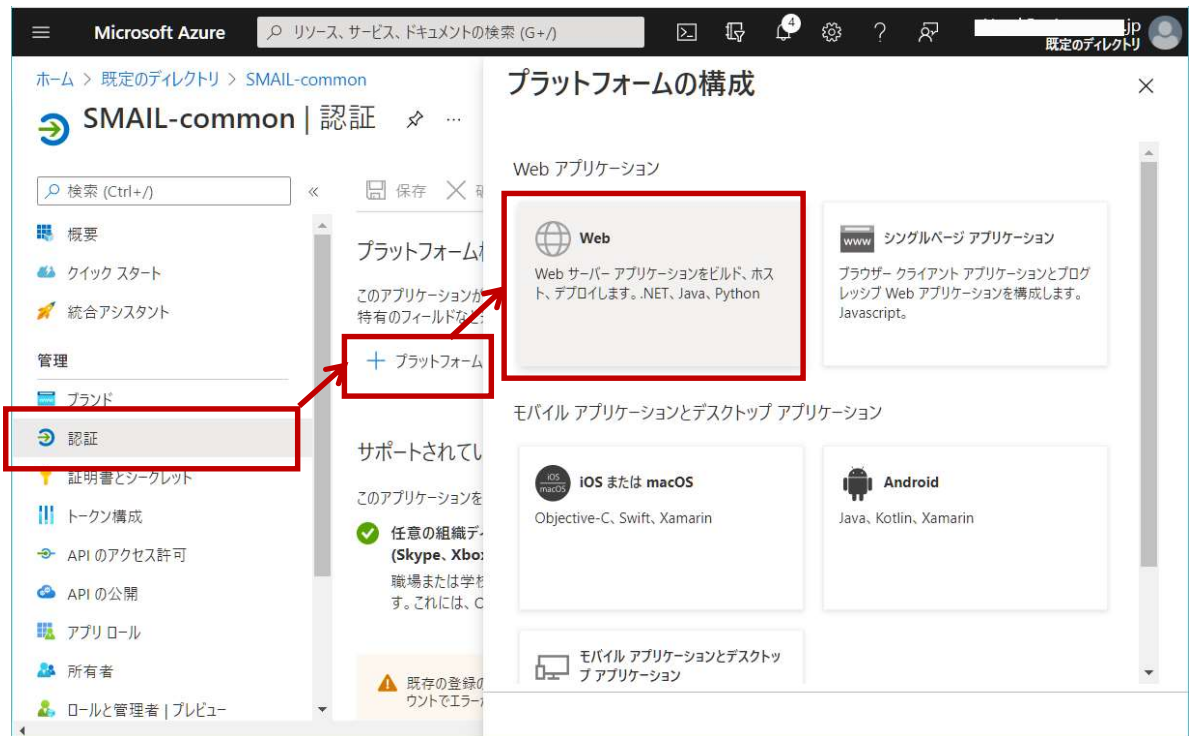
アカウントの種類は、**任意の組織ディレクトリ内のアカウントと個人の Microsoft アカウント**を選択して下さい。



※smail は”**任意の組織ディレクトリ内のアカウントと個人の Microsoft アカウント**“をデフォルトでサポートしておりますのでかかわらずこれを選択して下さい。

これにより各種エンドポイントの[tenant]の値の URI が異なってきます。この場合、[tenant]=common となります。

4) [認証] - [+プラットフォームを追加] -[WEB]を選択します。



5) リダイレクト URI を入力し[構成]ボタンをクリックします。

<http://localhost:8001/myapp/>

と入力します。(必ずこの URL)



詳細設定

Live SDK サポート

Microsoft アカウント サービス (login.live.com) と直接統合できるようにします。Microsoft アカウント SDK (Xbox や Bing Ads など) との統合に必要です。

はい

いいえ

パブリッククライアント フローを許可する

次のモバイルとデスクトップのフローを有効にする:

はい

いいえ

Live SDK は必要なので”いいえ”を選択

SmailRefreshToken.exe は、<http://localhost:8001/myapp/> で待ち受けます。ポート 8001 を使用しますので、後で SmailRefreshToken.exe を実行する時に、お使いの PC でポート 8001 のサービスを使っている場合はそのサービスを停止するか、他の PC で行って下さい。

(通常の PC ではバッティングはありません。ウイルスソフトで内部的に proxy で 8001 を使用している場合があるかもしれません。)

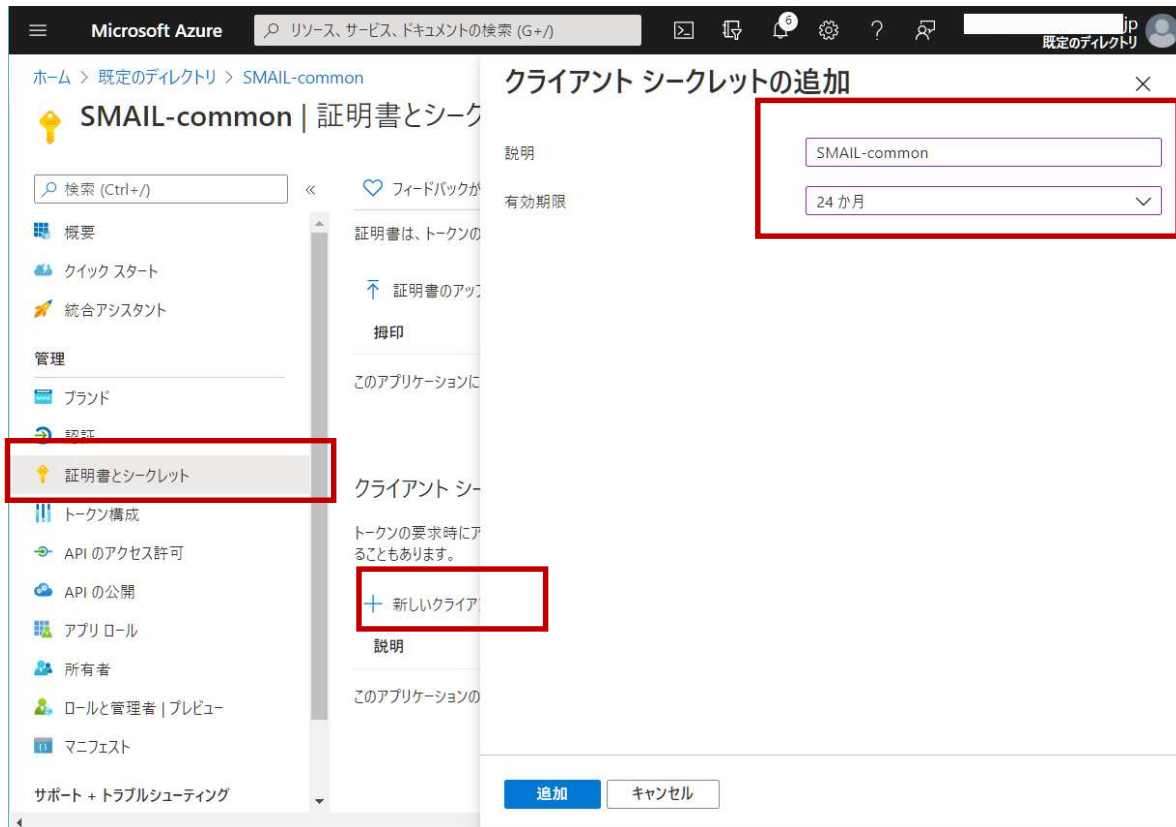
[参考]

Google API の場合は、リダイレクト URI に動的生成で SmailRefreshToken.exe の方から自動的に空きポートを選択して指定しておりますので、上記のような制約はありません。

6) ナビゲーションメニューから[証明書とシークレット]-[+新しいクライアント]をクリックします。

説明(任意の文字列:ここでは SMAIL-common とします)

有効期限を選択して下さい。

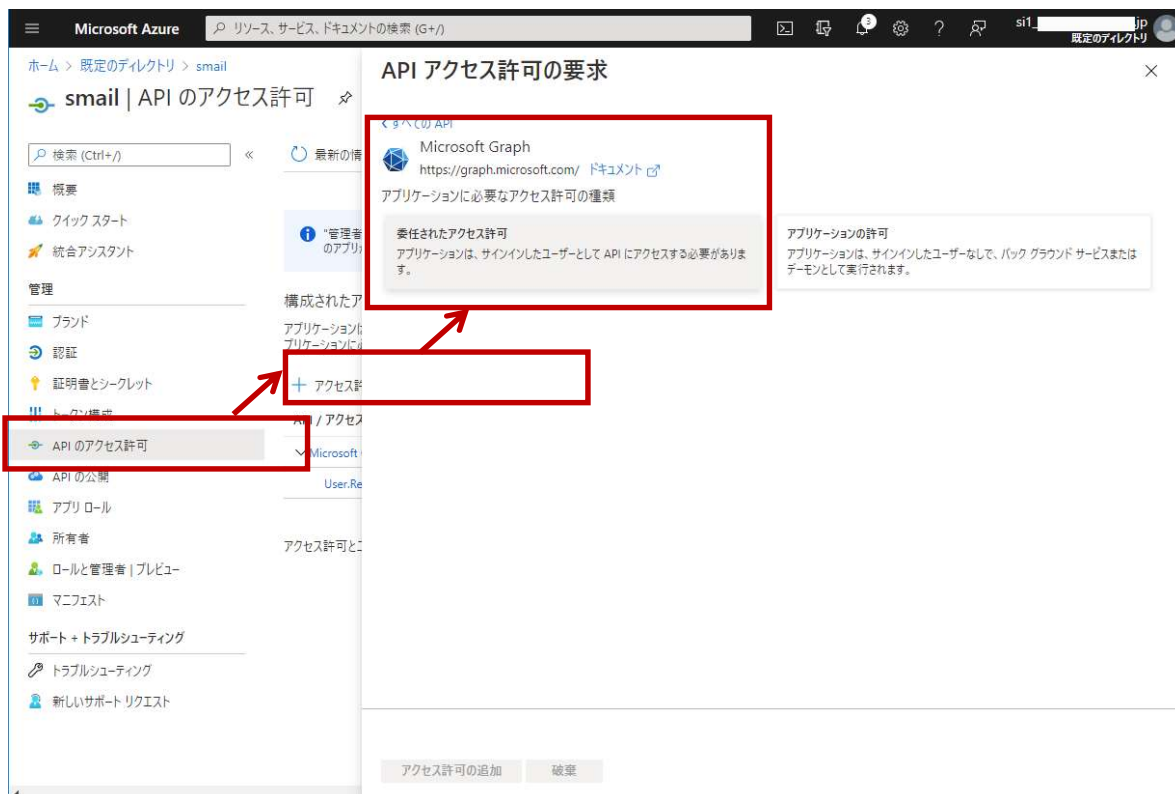


利用したい月数を選択。無期限があればそちらを選択して下さい。期限切れになった場合は、再度6)を実行します。

[追加]をクリックするとシークレット値が得られますので、ここでかみならず、クリップボードに保管してメモ帳等に記録しておいて下さい。この画面を離れるシークレット値はコピー & ペーストできなくなります。もし、そうなった場合は再度、追加でシークレット値を再作成して下さい。



- 7) ナビゲーションメニューから[API のアクセス許可]-[+アクセス許可の追加]をクリックします。「API アクセス許可の要求」画面をスクロールし、「Microsoft Graph」を選択します。

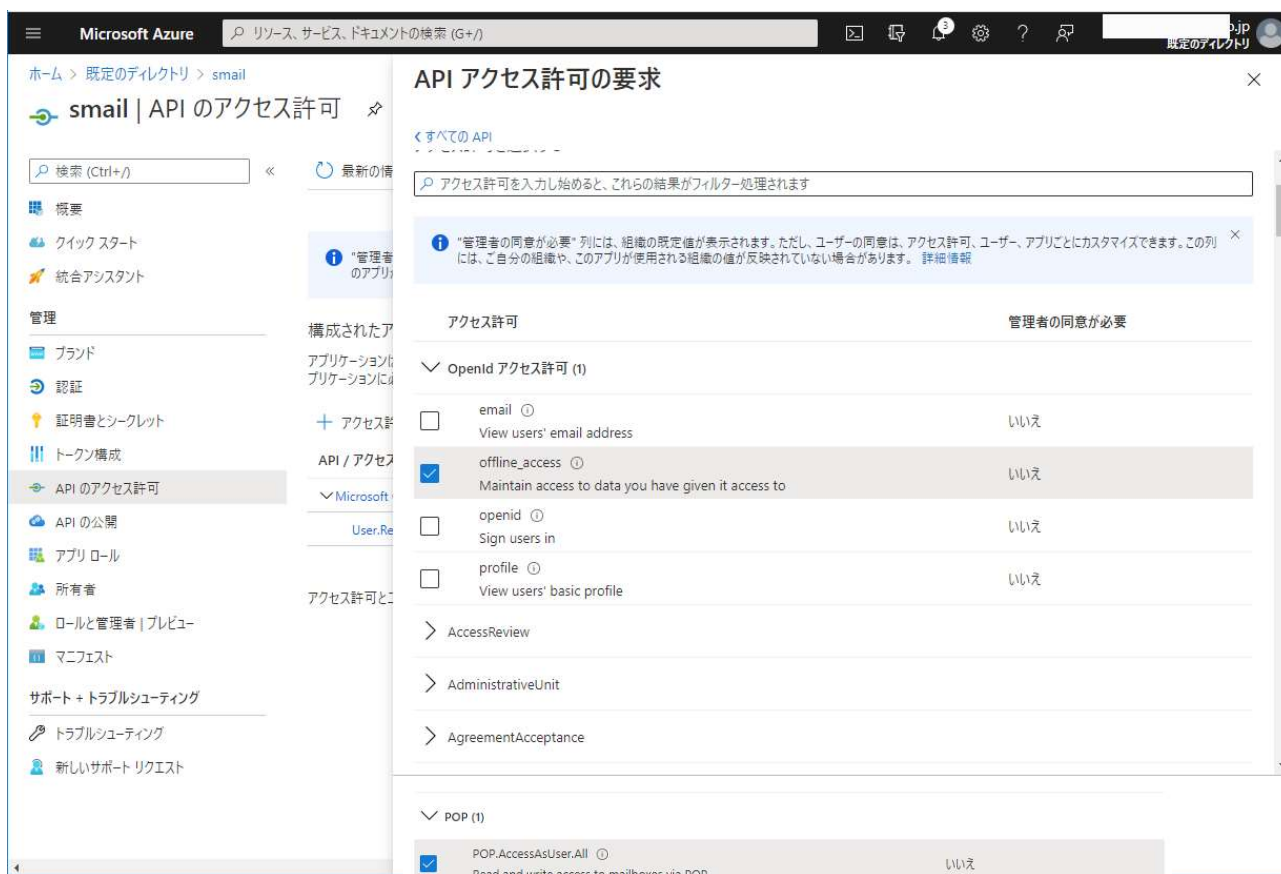


- 8) [委任されたアクセス許可]を選択し、次のアクセス許可をすべて選択します。

POP.AccessAsUser.All

SMTP.Send

offline_access





設定内容を確認し、[アクセス許可の追加]をクリックします

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

ホーム > 既定のディレクトリ > smail

smail | API のアクセス許可

検索 (Ctrl+F) | 最新の情報に更新 | フィードバックがある場合

概要
クイックスタート
統合アシスタント

管理
ブランド
認証
証明書とシークレット
トークン構成
API のアクセス許可
API の公開
アプリ ロール
所有者
ロールと管理者 | プレビュー
マニフェスト
サポート + トラブルシューティング
トラブルシューティング
新しいサポート リクエスト

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 | 既定のディレクトリに管理者の同意を与えます

| API / アクセス許可の名前 | 種類 | 説明 | 管理者の同意が必要 | 状態 |
|----------------------|------|---|-----------|-----|
| Microsoft Graph (4) | | | | ... |
| offline_access | 委任済み | Maintain access to data you have given it access to | いいえ | ... |
| POP.AccessAsUser.All | 委任済み | Read and write access to mailboxes via POP. | いいえ | ... |
| SMTP.Send | 委任済み | Send emails from mailboxes using SMTP AUTH. | いいえ | ... |
| User.Read | 委任済み | Sign in and read user profile | いいえ | ... |

アクセス許可とユーザーの同意を表示および管理するために、エンタープライズ アプリケーションをお試しください。

User.Read は必要ありませんが、デフォルトで設定されていました。削除しても良いです。

9) 概要でクライアント ID の確認

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Overview' page for an application named 'SMAIL-common'. The 'Application (Client) ID' is highlighted with a red box. The page also shows a search bar, navigation menu, and various informational messages.

| 項目 | 値 | 詳細 |
|----------------------|--------------|--|
| 表示名 | SMAIL-common | クライアントの資格情報 0 証明書、1 シークレット |
| アプリケーション (クライアント) ID |2b | リダイレクト URI 1 個の Web、0 個の SPA、0 個のパブリック クライアント |
| オブジェクト ID | 8 | アプリケーション ID の URI アプリケーション ID URI の追加 |
| ディレクトリ (テナント) ID | f | ローカル ディレクトリでのマネージド アプリケーション SMAIL-common |

クライアント ID をコピー & ペーストし、メモ帳に記録して下さい。

(クライアント ID と 6) のシークレット値の 2 つで、SmailRefreshToken.exe からリフレッシュトークンを取得できるようになります)

② Azure Active Director OAuth API で[リフレッシュトークン]を取得

1) SmailRefreshToken.exe を起動させます。

OAuth2.0 プロバイダーは Microsoft Azure を選択します。

連携したいメールアドレスと取得したクライアント ID、シークレット値を入力します。

The screenshot shows the 'Smail OAuth リフレッシュトークン取得 Ver 1.1' application window. The 'OAuth 2.0 Provider' is set to 'Microsoft Azure', the 'Sending Email' is '@outlook.com', and the 'Client ID' and 'Secret Value' fields are filled with values and highlighted with a red box.

| 項目 | 値 |
|------------------|--|
| OAuth 2.0 プロバイダー | Microsoft Azure |
| 送信メール(必須) | @outlook.com |
| クライアントID(必須) | 31c5c0a..... |
| シークレット値(必須) | se..... |
| トークンURI | https://login.microsoftonline.com/common/oauth2/v2.0/token |
| 承認URI | https://login.microsoftonline.com/common/oauth2/v2.0/authorize |

Smail OAuth リフレッシュトークン取得 Ver. 1.1

OAuth 2.0プロバイダー: Microsoft Azure

送信メール(必須): @outlook.com

クライアントID(必須): [input field]

シークレット値(必須): [input field]

トークンURI: https://login.microsoftonline.com/common/oauth2/v2.0/token

承認URI: https://login.microsoftonline.com/common/oauth2/v2.0/authorize

リフレッシュトークンの作成 (highlighted)

終了

[リフレッシュトークンの作成] をクリックします。

(このボタンを押下することで、Microsoft Azure サーバへ承認接続し、リフレッシュトークンを取得します。)

確認ダイアログが表示されますので、[OK] ボタンをクリックして下さい。(リクエストのメールアドレスは正しいか、再確認して下さい)

EMail Autorization

リクエストメールアドレス: 1@outlook.com

デフォルトブラウザが開きますのでログインしてアクセスして下さい。
別のアカウントで認証したい場合は一度ログアウトする必要があります。

OK (highlighted) キャンセル

Microsoft

サインイン

@outlook.com

アカウントをお持ちではない場合、作成できます。

アカウントにアクセスできない場合

戻る 次へ (highlighted)

Microsoft

1@outlook.com

パスワードの入力

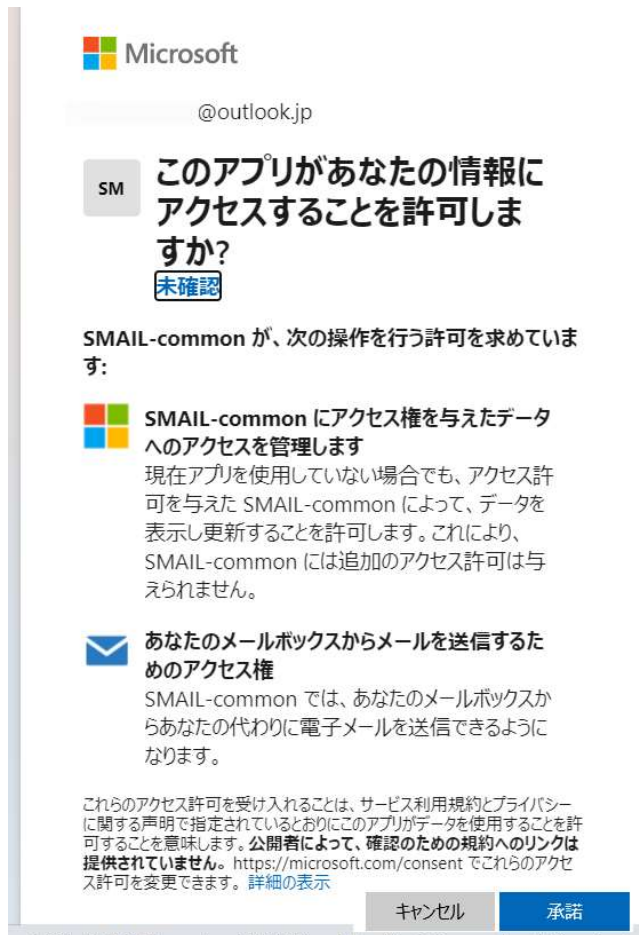
.....

サインインしたままにする

パスワードを忘れた場合

サインイン (highlighted)

デフォルトのブラウザが起動し、マイクロソフトのログイン画面が表示されます。複数アカウントが表示される場合は、今回連携するメールアドレスを選択するか、別ログインして下さい。



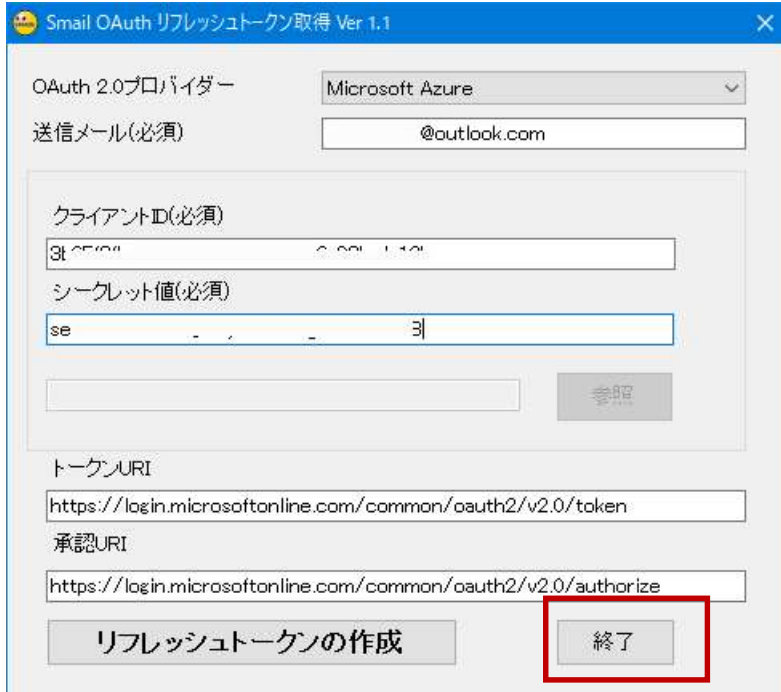
上のような承諾画面が表示されますので、[承諾]をクリックして下さい。

③ **SmailRefreshToken.exe** で正しくリフレッシュトークンが取得できれば、**実行フォルダー**に、**smail_refreshtoken.ini** が生成されます。

- ・成功するとデフォルトのブラウザに以下のように表示されます。



- ・ **SmailRefreshToken.exe** 以下のダイアログメッセージが表示されます。
[OK]を押して[終了]させてください。



※リフレッシュトークンの再取得が必要な時はこの操作をします。

通常は一度だけ取得すれば OK ですが、期限切れの時は再取得が必要となります。

尚、ここまでの操作は **SMAIL** を動作させない PC 上で行っても問題ありません。

④smail_refresh_token.ini を **smail.exe** と同じフォルダーにコピーし、**smail.exe** を起動して、**smtp 認証に OAUTH-XOAUTH2** を選択すれば利用できます。

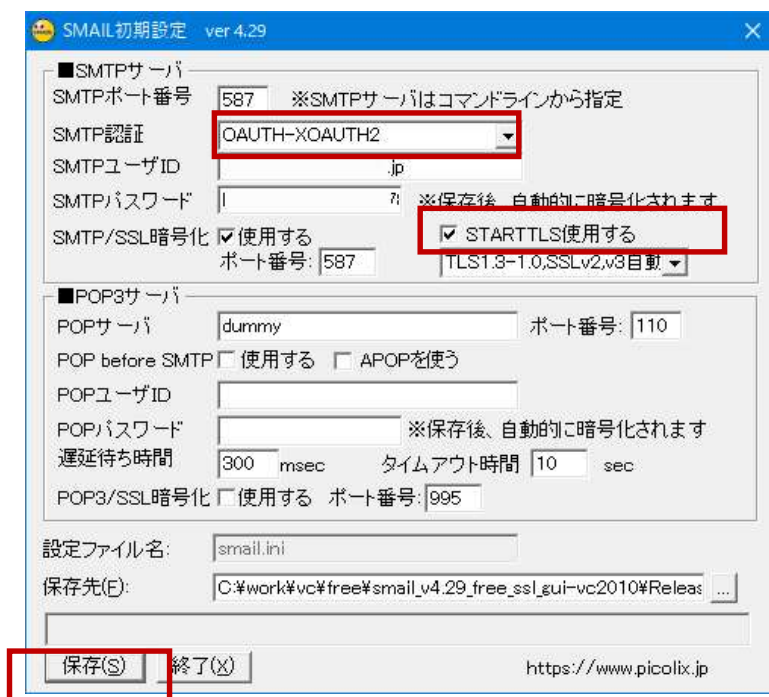
- 1) 実行フォルダーにリフレッシュトークン等が記載された INI ファイル、**smail_refresh_token.ini** が生成されていますので、**smail.exe** または **smail.ini** のあるフォルダーにコピーして下さい。

以後、**smail_refresh_token.ini** のファイルが **SMAIL** を実行する PC に必要です。

例) **smail_refresh_token.ini**

```
[OAUTH2]
UserID=xxxxxxxxxxxxx@outlook.com
ClientID=3bxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
ClientSecret=se4xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
RefreshToken=M.R3_BAY.-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TokenURI=https://login.microsoftonline.com/common/oauth2/v2.0/token
OuthURI=https://login.microsoftonline.com/common/oauth2/v2.0/authorize
OAUTH2_TIME_OUT=30
Provider=1
```

- 2) SMAIL.exe を起動し SMTP 認証：OAUTH-XOAUTH2 を選択して保存して下さい。
office365 は、STARTTLS のチェックが必要です。



[保存]して終了して下さい。

refresh token.ini が見つからない場合は以下の警告が出ます。正しく INI ファイルを作製して下さい。



smail.ini に設定が保存されます。(既存の smail.ini に引き継がれます)

以上で、全ての事前準備が終わりです。smail で Microsoft office365 のメール送信が可能になります。

3. 動作確認

例) c>smail -hsmtp.office365.com -s"TEST MAIL" -fxxxxxxxxxxx@outlook.com xxx@xxxxxx.xx -d -i

```
#----- SMAIL 4.29 Information By Eva -----
#設定ファイル      : [C:\work\vc\free\smail_v4.29_free_ssl_gui-vc2010\Release\smail.ini]
#POP before SMTP  : 使わない
#APOP              : 使わない
#SMTP 認証        : 使う AUTH XOAUTH2 を利用
#設定ファイル(OAUTH用) : [C:\work\vc\free\smail_v4.29_free_ssl_gui-vc2010\Release\smail_refresh_token.ini]
#API アカウント   : [xxxxxxxx@xxxxxx.jp]
#SMTP アカウント  : xxxxxxxx@outlook.com
#SMTPS (SMTP over SSL) : 使う [OpenSSL 1.1.1k]
#SSL 方式         : TLS1.3-1.0, SSLv2, v3 自動
#STARTTLS        : 使う
#本文ファイル     : なし
#添付ファイル     : なし
#メールサーバ     : smtp.office365.com
#メール送り元     : xxxxxxxx@outlook.com
#メール送り先     : xxx@xxxxxxxx.jp
#サブジェクト内容 : TEST MAIL
#キャラクターセット : ISO-2022-JP
#エンコーディング : 7bit
Recv:[111 bytes] 220 OS3PR01CA0017.outlook.office365.com Microsoft ESMTPL MAIL Service ready at Tue, 22 Jun 2021 05:13:49 +0000
Send: EHLO xxxxxxxxx
Recv:[63 bytes] 250-OS3PR01CA0017.outlook.office365.com Hello [xxx.xxx.xxx.xxx]
Recv:[142 bytes] 250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250-SMTPUTF8
[250 message2 ok!]
Send: STARTTLS
Recv:[29 bytes] 220 2.0.0 SMTP server ready
SSL connection using ECDHE-RSA-AES256-GCM-SHA384 - TLSv1.2
X509 subject_name: /C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/CN=outlook.com
X509 issuer_name: /C=US/O=DigiCert Inc/CN=DigiCert Cloud Services CA-1
Send: EHLO xxxxxxxxx
Recv:[215 bytes] 250-OS3PR01CA0017.outlook.office365.com Hello [219.75.132.65]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-AUTH LOGIN XOAUTH2
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250-SMTPUTF8
[250 message ok!]
[Try get access token from https://login.microsoftonline.com/common/oauth2/v2.0/token]
[access_token=EwA4A+I3BAAU0+FyEzrG...] ; 認証サーバにアクセストークン要求
Send: AUTH XOAUTH2 ***** ; アクセストークン取得
Recv:[37 bytes] 235 2.7.0 Authentication successful ; XOAUTH2 で接続要求
Send: MAIL FROM:<xxxxxxxx@outlook.com> ; 認証成功
Recv:[21 bytes] 250 2.1.0 Sender OK
Send: RCPT TO:<xxx@xxxxxx.xx>
Recv:[24 bytes] 250 2.1.5 Recipient OK
```

```

Send: DATA
Recv:[46 bytes] 354 Start mail input; end with <CRLF>.<CRLF>
Send: From: xxxxxx1@outlook.com
To: xxxxxx@xxxxxxxx.jp
Subject: TEST MAIL
X-Mailer: SMAIL 4.29
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-2022-JP
Content-Transfer-Encoding: 7bit
Date: Tue, 22 Jun 2021 14:13:50 +0900
Send:
#//メールヘッダー送信完了 (2.640sec)....
Send:
.
Recv:[146 bytes] 250 2.0.0 OK <S12PR03MB5291274D9C18E46A7FBCEC25C0099@S12PR03MB5291.apcprd03.prod.outlook.com> [Hostname=S12PR03MB5291.apcprd03.prod.outlook.com]
Send: QUIT
Recv:[48 bytes] 221 2.0.0 Service closing transmission channel

C:¥work¥vc¥free¥smail_v4.29_free_ssl_gui-vc2010¥Release>

```

・SMTPはSSL通信にOPENSSLライブラリーを使っていますが、OAUTHのアクセストークン取得部分のみ、googleへのhttpsプロトコルは、標準Windows関数を使用しております。従って、使用端末がtls1.2以降をサポートしている必要があります。

OAuth 2.0 認証の動作 OS:

| OS | Windows Server 2008 sp2 | Windows Server 2008 R2 | Windows Server 2012 | Windows Server 2016 | Windows xp | Windows 7 pro | Windows 8.1 | Windows 10 pro |
|--------------|-------------------------|------------------------|---------------------|---------------------|------------|---------------|-------------|----------------|
| OAuth 2.0 認証 | △(*1) | ○ | ○ | ○ | × | ○ | ○ | ○ |

(*1)

KB4019276 パッチを利用し、TLS1.2 を利用可にすれば動作可能です。(Windows Server 2008 sp2 64BIT 版検証済み)

<https://support.microsoft.com/ja-jp/help/4074621/add-rds-support-for-tls-1-1-and-tls-1-2-in-windows-server-2008-sp2>

・プロキシ対応です。httpsアクセスに端末のプロキシ情報を利用しています。

4. OAUTH 関連エラー例

エラー番号 28 が発生した時は、オプションに `-d` を付けて通信内容をコンソールに表示して詳細なエラーを取得して下さい。

1. Error HttpSendRequest [12157]

```
[250 message ok!]  
[Try get access token from https://oauth2.googleapis.com/token]  
Error HttpSendRequest [12157]  
ERR-0028:OAUTH 認証サーバからアクセストークンが取得できませんでした。
```

12157 セキュリティ・チャネル・エラー

SSL ライブラリのロード中に、アプリケーションに内部エラーが発生しました

2. Error HttpSendRequest [12045]

```
[250 message ok!]  
[Try get access token from https://oauth2.googleapis.com/token]  
Error HttpSendRequest [12045]  
ERR-0028:OAUTH 認証サーバからアクセストークンが取得できませんでした。
```

12045 無効な認証局です

サーバーSSL 証明書は、未知または無効な認証局から発行されたものです。

PC が TLS1.2 をサポートしていない場合のエラーです。

3. Error HttpSendRequest [12029]

```
[250 message ok!]  
[Try get access token from https://oauth2.googleapis.com/token]  
Error HttpSendRequest [12029]  
ERR-0028:OAUTH 認証サーバからアクセストークンが取得できませんでした。
```

12029 サーバー接続の試みに失敗しました

プロキシ設定が間違っており接続できない場合もこのエラーが出ます。

4. Error InternetCrackUrl [12006]

```
[250 message ok!]  
[Try get access token from https://oauth2.googleapis.com/token]  
Error InternetCrackUrl [12006]  
ERR-0028:OAUTH 認証サーバからアクセストークンが取得できませんでした。
```

12006 不正な URL です

`smail_refresh_token.ini` 等が参照できず `TokenURI` が参照できない場合発生します。

もしくは `smail_refresh_token.ini` 中の `TokenURI` の URL の記述が間違っています。