Claris FileMaker Server と Azure Active Directory の連携

エミックオンラインセミナー

2022年1月25日

株式会社エミック

- Claris FileMaker対応ホスティングサービスを1998年から提供
- FMP48開発サービス（定額制オンライン対面開発サービス）
- FileMaker ライセンス販売
- kintone導入支援・カスタマイズ開発

Claris Partner

自己紹介

- 松尾篤（まつおあつし）／株式会社エミック代表取締役社長
  - Claris FileMaker 認定デベロッパ
  - kintone認定 アプリデザインスペシャリスト（2020年2月）
  - kintone認定 カスタマイズスペシャリスト（2020年3月）

Claris FileMaker CERTIFIED DEVELOPER

kintone CERTIFIED Customization SP 2020

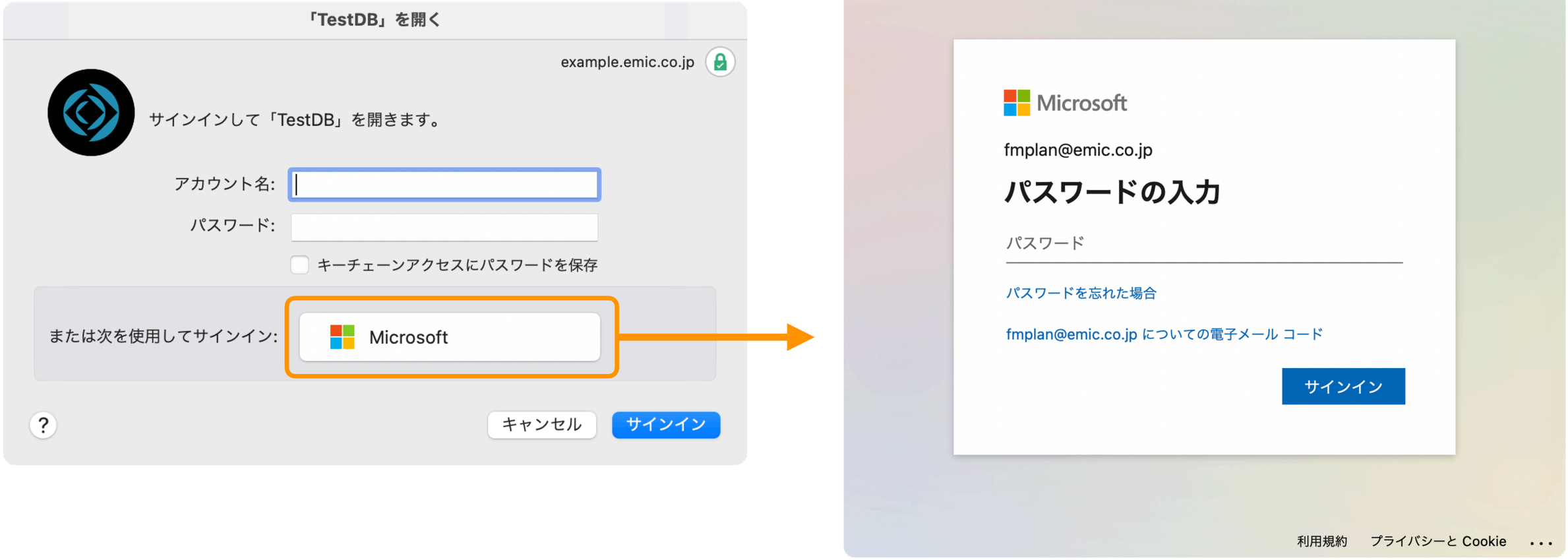
kintone CERTIFIED App Design SP 2020

今回の話題

- Claris FileMaker ServerでOAuthを利用するメリット
- Azure Active Directoryの資格情報を使用する方法について
- Azure Active Directoryにおける設定時の注意点

Claris FileMaker ServerでOAuthを利用するメリット

OAuth


「TestDB」を開く
example.emic.co.jp
サインインして「TestDB」を開きます。
アカウント名:
パスワード:
キーチェーンアクセスにパスワードを保存
または次を使用してサインイン:
Microsoft
キャンセル
サインイン
login.live.com/oauth20_auth
Microsoft
fmplan@emic.co.jp
パスワードの入力
パスワード
パスワードを忘れた場合
fmplan@emic.co.jp についての電子メール コード
サインイン
利用規約
プライバシーと Cookie

FileMaker Server & OAuth

- FileMaker Server 16でOAuthに対応
  - OAuth アイデンティティプロバイダの資格情報を使用してFileMaker データベースにログインできるように設定可能
  - FileMaker Serverで共有されているファイルであることが前提

FileMaker Server & OAuth

- サポートされているOAuth アイデンティティプロバイダ
  - Amazon
  - Google
  - Microsoft Azure Active Directory

FileMaker Server & OAuth

- サポートされているクライアント
  - Claris FileMaker Pro
  - Claris FileMaker Go
  - Claris FileMaker WebDirect

FileMaker Server & OAuth

- ［参考］FileMaker Server 19.4.1の新機能
  - カスタム OAuth アイデンティティプロバイダに対応

OAuthを利用するメリット

- OAuth アイデンティティプロバイダの資格情報を使用
  - アカウントの一元管理が可能
  - Claris FileMaker側でパスワードの管理が不要になる
  - 2要素認証を用いてセキュリティを向上させることができる

アカウント管理の悩み

- ファイル数が多い場合
  - ユーザーが増えるたびに各ファイルにアカウントを登録する必要がある
- ユーザー数が多い場合
  - ファイルを追加するたびに多数のアカウントを登録する必要がある

Azure Active Directory

- FileMaker Server 16からサポートされているOAuth アイデンティティプロバイダのうちMicrosoft Azure Active Directoryであればグループでの認証がサポートされている
  - アカウントではなくグループを登録できるのでアカウント管理の手間を大幅に軽減

Azure Active Directoryの資格情報を使用する方法について

Demo

必要な設定

- Azure Active Directory（Azure AD）での設定
- FileMaker Serverでの設定
- FileMaker Proでの設定

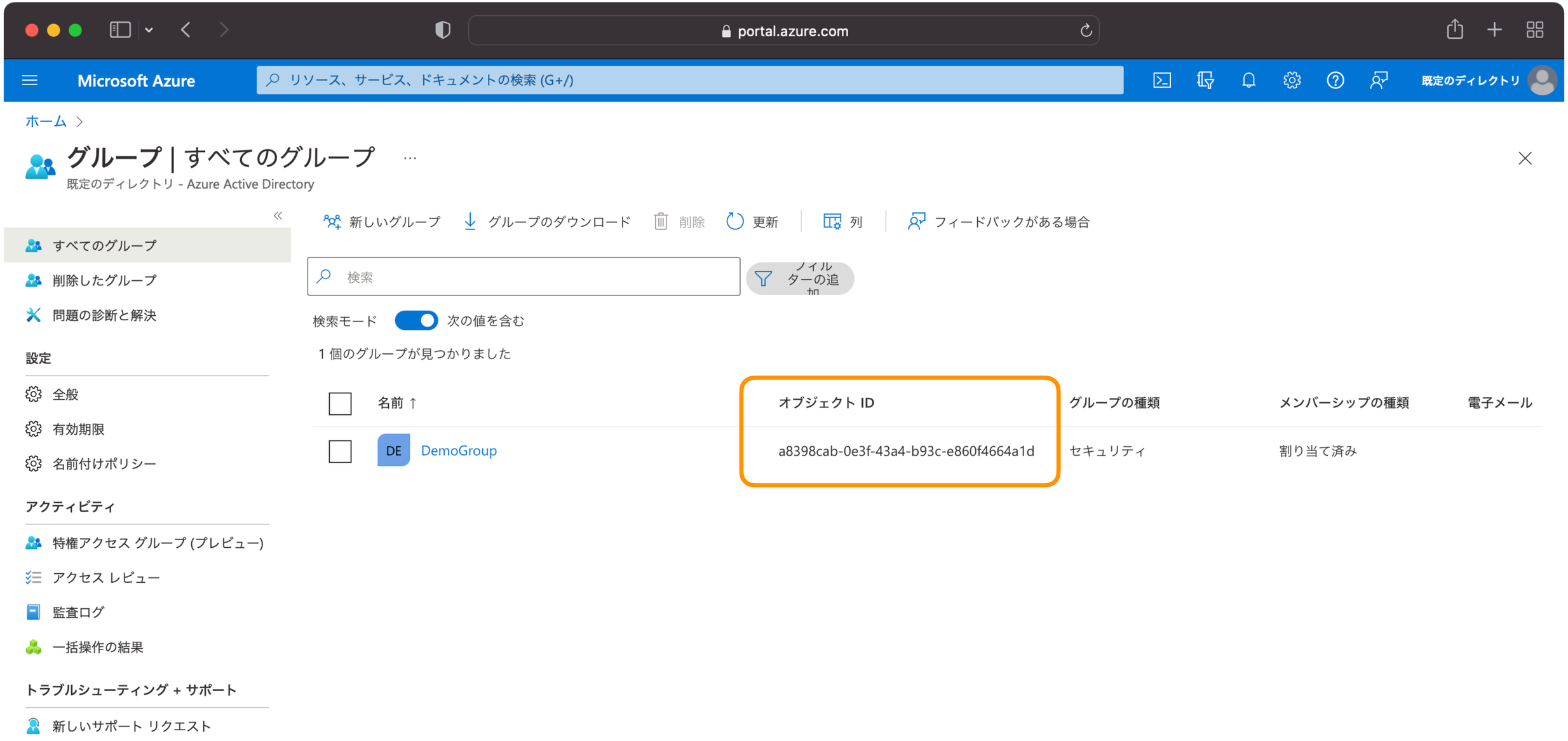
Azure ADでの設定

- Azure ADの設定にはMicrosoft Azureのサブスクリプションが必要
  - サブスクリプションがない場合にはサインアップして無料アカウントを作成（ https://azure.microsoft.com/ja-jp/free/ ）
  - https://portal.azure.com/ にサインイン

注）本資料は2022年1月時点の情報に基づいた解説となっています

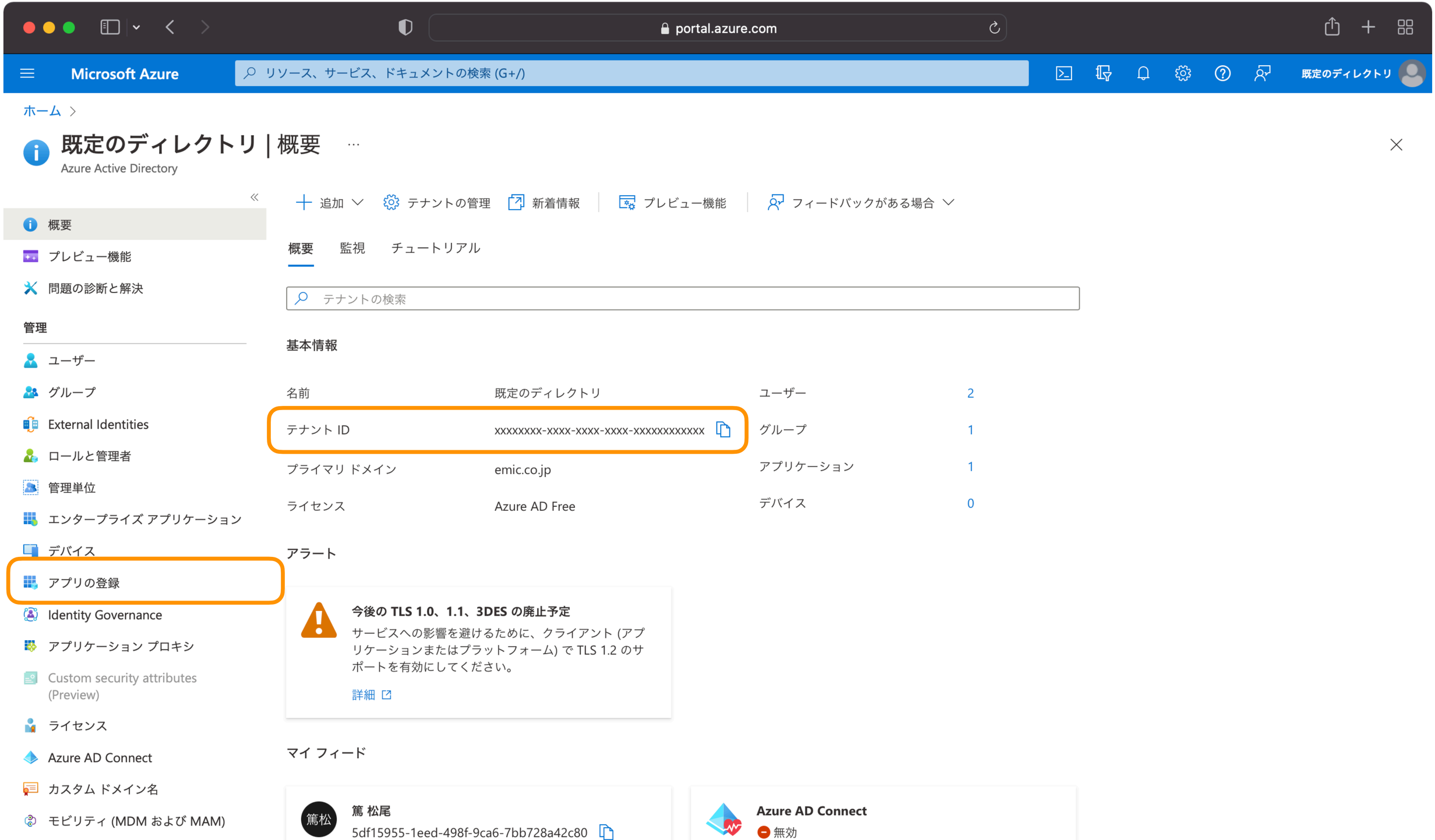
Azure ADでの設定

- Azure ADでユーザーとグループを登録
  - グループにメンバーを追加
  - グループの**オブジェクト ID**を確認


portal.azure.com
Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
既定のディレクトリ
ホーム
グループ | すべてのグループ
既定のディレクトリ - Azure Active Directory
新しいグループ
グループのダウンロード
削除
更新
列
フィードバックがある場合
すべてのグループ
削除したグループ
問題の診断と解決
設定
全般
有効期限
名前付けポリシー
アクティビティ
特権アクセス グループ (プレビュー)
アクセス レビュー
監査ログ
一括操作の結果
トラブルシューティング + サポート
新しいサポート リクエスト
検索
フィルターの追加
検索モード
次の値を含む
1 個のグループが見つかりました
名前 ↑
オブジェクト ID
グループの種類
メンバーシップの種類
電子メール
DE
DemoGroup
a8398cab-0e3f-43a4-b93c-e860f4664a1d
セキュリティ
割り当て済み

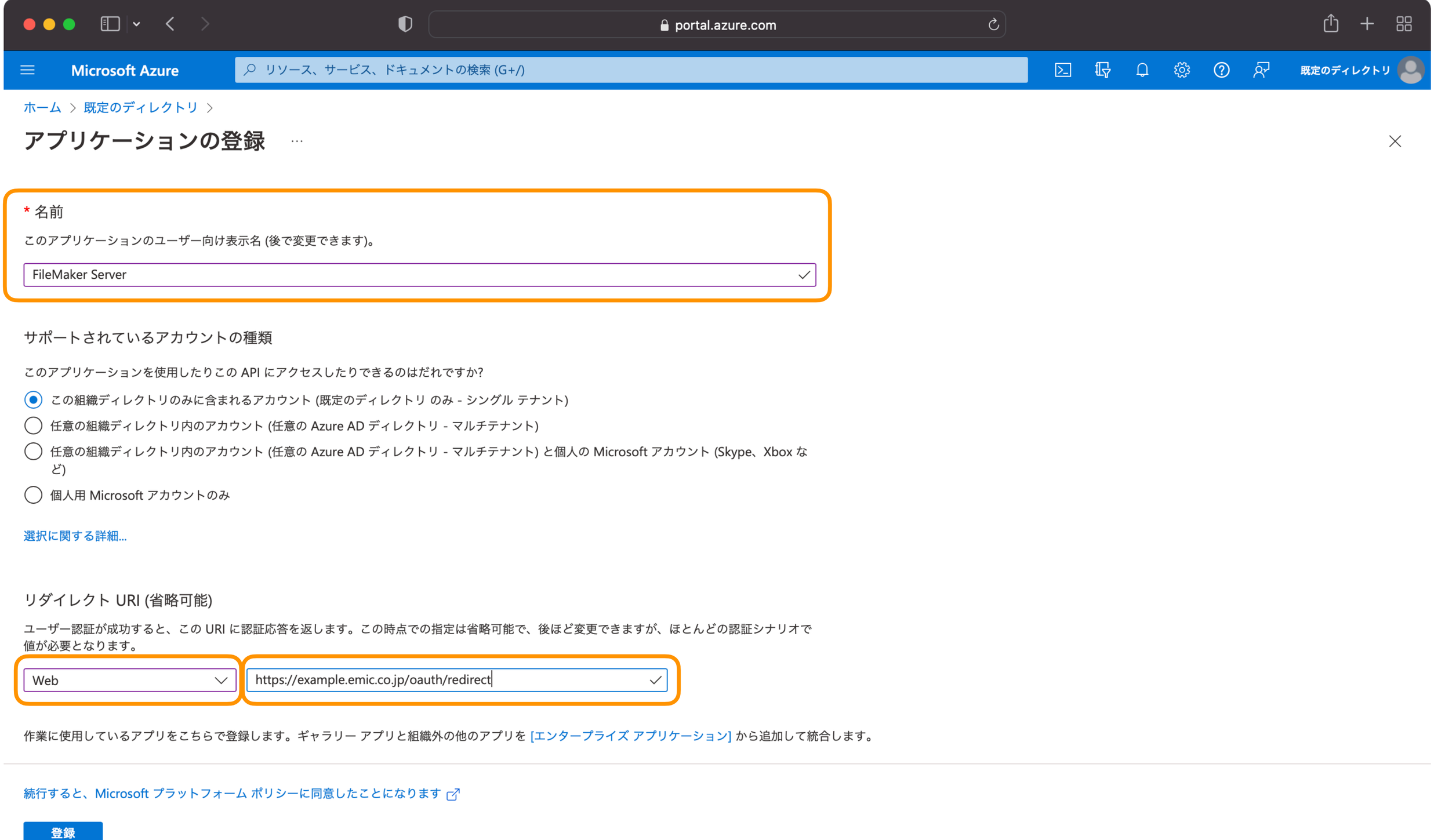
Azure ADでの設定

- Azure ADの［概要］で**テナント ID**を確認
- Azure ADの［**アプリの登録**］で新しいアプリケーションを追加


portal.azure.com
Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
既定のディレクトリ
ホーム
既定のディレクトリ | 概要
Azure Active Directory
追加
テナントの管理
新着情報
プレビュー機能
フィードバックがある場合
概要
監視
チュートリアル
テナントの検索
概要
プレビュー機能
問題の診断と解決
管理
ユーザー
グループ
External Identities
ロールと管理者
管理単位
エンタープライズ アプリケーション
デバイス
アプリの登録
Identity Governance
アプリケーション プロキシ
Custom security attributes (Preview)
ライセンス
Azure AD Connect
カスタム ドメイン名
モビリティ (MDM および MAM)
基本情報
名前
既定のディレクトリ
テナント ID
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
プライマリ ドメイン
emic.co.jp
ライセンス
Azure AD Free
ユーザー
2
グループ
1
アプリケーション
1
デバイス
0
アラート
今後の TLS 1.0、1.1、3DES の廃止予定
サービスへの影響を避けるために、クライアント (アプリケーションまたはプラットフォーム) で TLS 1.2 のサポートを有効にしてください。
詳細
マイ フィード
篤 松尾
5df15955-1eed-498f-9ca6-7bb728a42c80
Azure AD Connect
無効

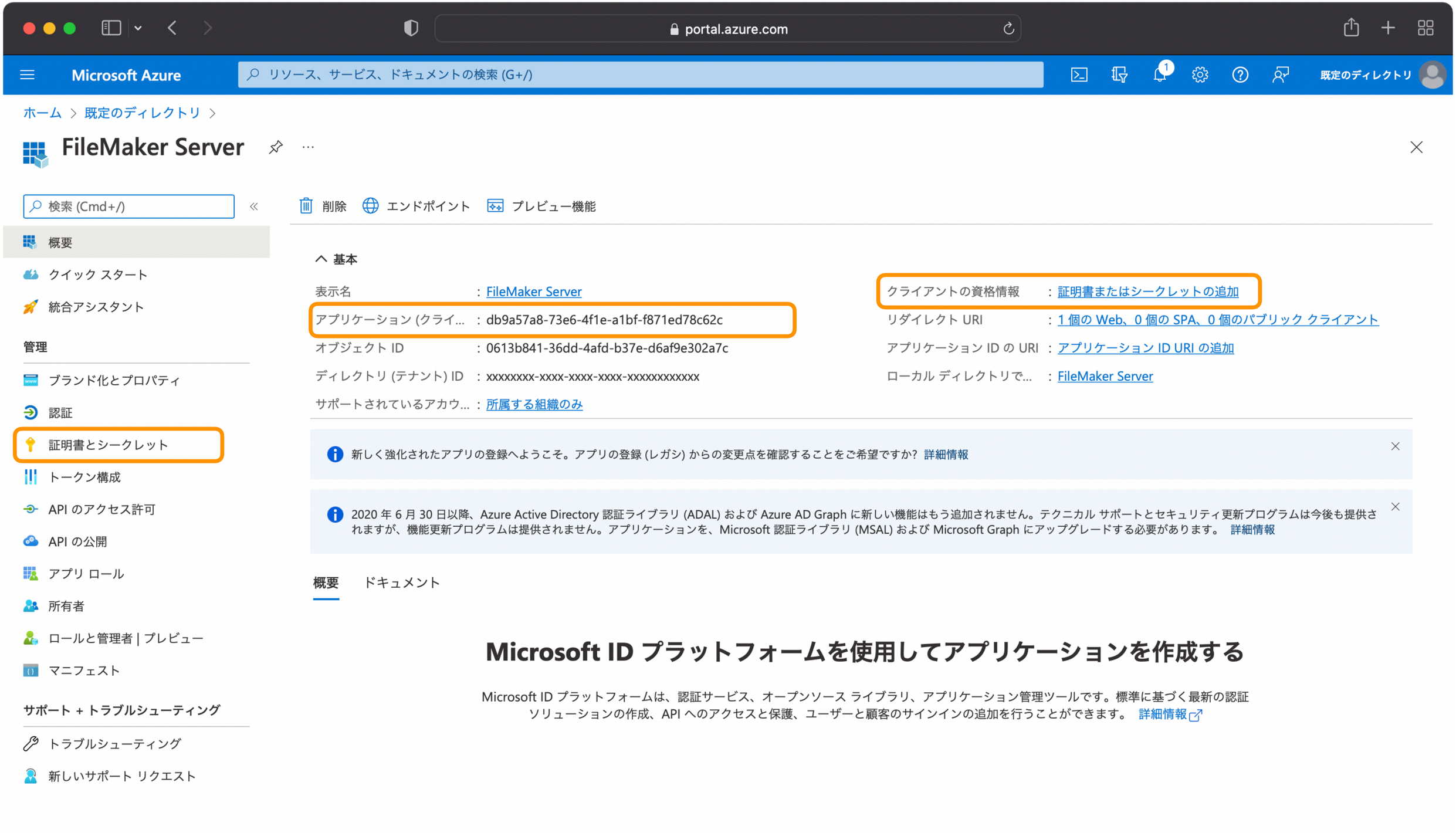
Azure ADでのアプリの登録

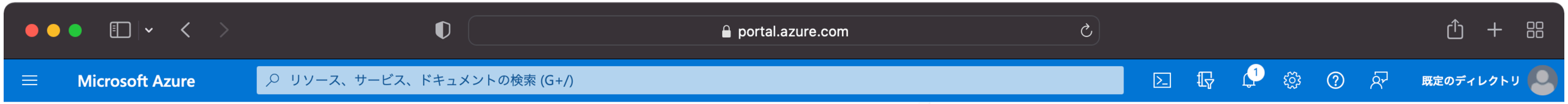
- Azure ADにおけるアプリの新規登録時
  - 名前（ユーザー向け表示名）には**任意の名称を入力**
  - リダイレクト URIを設定して登録
    - ［プラットフォームの選択］では「**Web**」を選択
    - URLには「**https://<完全修飾ドメイン名>/oauth/redirect**」を入力
      - FileMaker Serverで使用している完全修飾ドメイン名を入力


portal.azure.com
Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
既定のディレクトリ
ホーム > 既定のディレクトリ >
アプリケーションの登録 ...
* 名前
このアプリケーションのユーザー向け表示名 (後で変更できます)。
FileMaker Server
サポートされているアカウントの種類
このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?
この組織ディレクトリのみに含まれるアカウント (既定のディレクトリ のみ - シングル テナント)
任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)
任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype、Xbox など)
個人用 Microsoft アカウントのみ
選択に関する詳細...
リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。
Web
https://example.emic.co.jp/oauth/redirect
作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [エンタープライズ アプリケーション] から追加して統合します。
続行すると、Microsoft プラットフォーム ポリシーに同意したことになります
登録

Azure ADでのアプリの管理

- アプリを追加した後に概要で**アプリケーション (クライアント) ID**を確認
- アプリの管理時においてはキーではなく**新しいクライアント シークレット**を追加（［**証明書またはシークレットの追加**］をクリック）
  - クライアント シークレットの説明を入力して［追加］をクリック
  - 追加直後に**クライアント シークレットの値をコピー**（この情報は再び表示されることはないため）


portal.azure.com
Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
既定のディレクトリ
ホーム > 既定のディレクトリ >
FileMaker Server
検索 (Cmd+/)
削除
エンドポイント
プレビュー機能
概要
クイック スタート
統合アシスタント
管理
ブランド化とプロパティ
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
基本
表示名 : FileMaker Server
アプリケーション (クライ... : db9a57a8-73e6-4f1e-a1bf-f871ed78c62c
オブジェクト ID : 0613b841-36dd-4afd-b37e-d6af9e302a7c
ディレクトリ (テナント) ID : xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
サポートされているアカウ... : 所属する組織のみ
クライアントの資格情報 : 証明書またはシークレットの追加
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
アプリケーション ID の URI : アプリケーション ID URI の追加
ローカル ディレクトリで... : FileMaker Server
新しく強化されたアプリの登録へようこそ。アプリの登録 (レガシ) からの変更点を確認することをご希望ですか? 詳細情報
2020 年 6 月 30 日以降、Azure Active Directory 認証ライブラリ (ADAL) および Azure AD Graph に新しい機能はもう追加されません。テクニカル サポートとセキュリティ更新プログラムは今後も提供されますが、機能更新プログラムは提供されません。アプリケーションを、Microsoft 認証ライブラリ (MSAL) および Microsoft Graph にアップグレードする必要があります。 詳細情報
概要
ドキュメント
Microsoft ID プラットフォームを使用してアプリケーションを作成する
Microsoft ID プラットフォームは、認証サービス、オープンソース ライブラリ、アプリケーション管理ツールです。標準に基づく最新の認証ソリューションの作成、API へのアクセスと保護、ユーザーと顧客のサインインの追加を行うことができます。 詳細情報



ホーム > 既定のディレクトリ > FileMaker Server

FileMaker Server | 証明書とシークレット

検索 (Cmd+/)

- 概要
- クイック スタート
- 統合アシスタント

管理

- ブランド化とプロパティ
- 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

フィードバックがある場合

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、
にするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットでは

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアント シークレット (0)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリ

+ 新しいクライアント シークレット

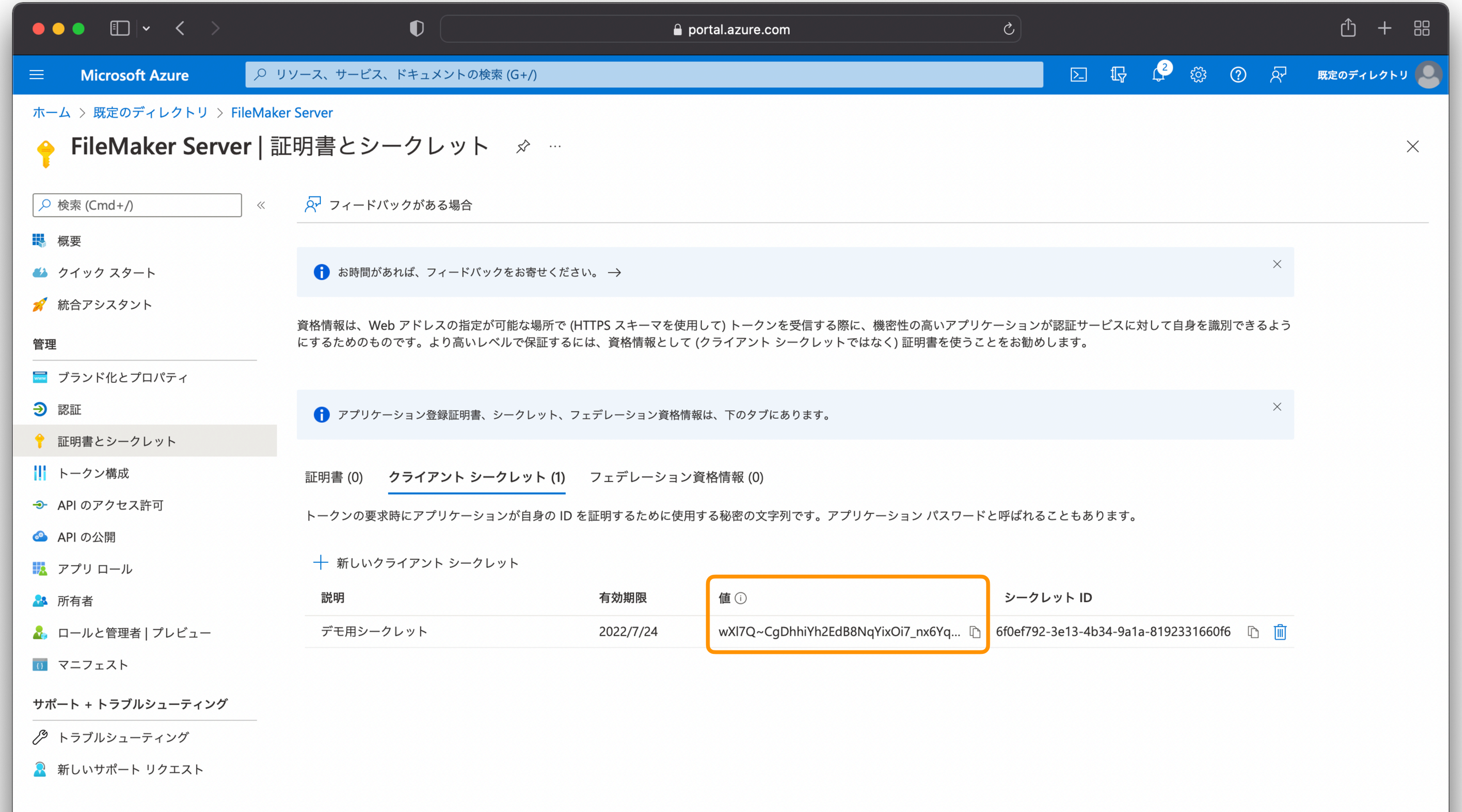
説明	有効期限	値

このアプリケーションのクライアント シークレットは作成されていません。

クライアント シークレットの追加

説明 このクライアント シークレットの説明を入力してく

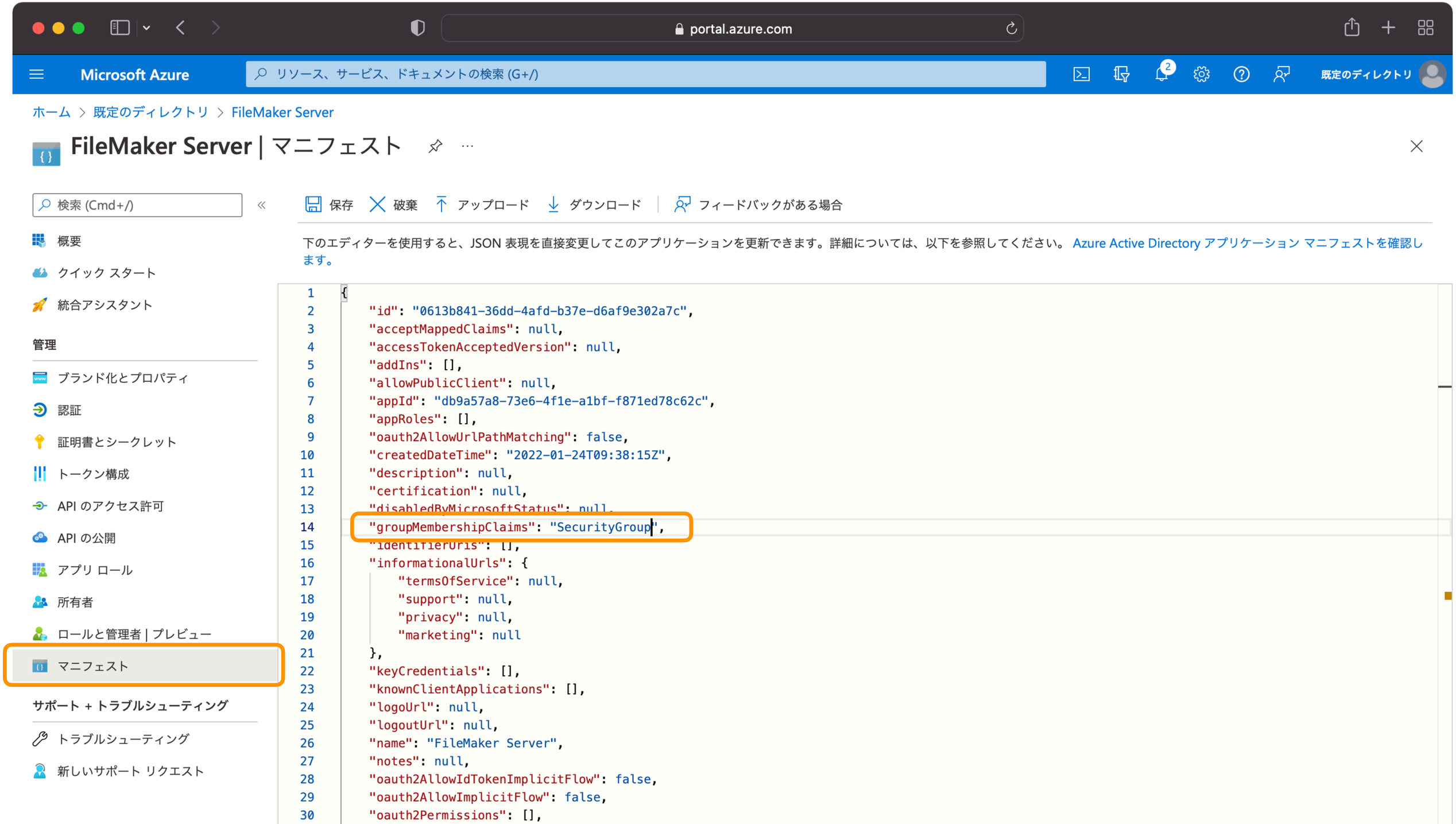
有効期限 推奨: 6 か月


portal.azure.com
Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
既定のディレクトリ
ホーム > 既定のディレクトリ > FileMaker Server
FileMaker Server | 証明書とシークレット
検索 (Cmd+/)
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
ブランド化とプロパティ
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
お時間があれば、フィードバックをお寄せください。 →
資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。
アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。
証明書 (0)
クライアント シークレット (1)
フェデレーション資格情報 (0)
トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。
新しいクライアント シークレット
説明
有効期限
値
シークレット ID
デモ用シークレット
2022/7/24
wXl7Q~CgDhhiYh2EdB8NqYixOi7_nx6Yq...
6f0ef792-3e13-4b34-9a1a-8192331660f6

Azure ADでのアプリの管理

- アプリの［**マニフェスト**］の内容を要更新

  - 「"groupMembershipClaims": null,」を
    「"groupMembershipClaims": **"SecurityGroup",**」に変更・保存


portal.azure.com
Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
既定のディレクトリ
ホーム > 既定のディレクトリ > FileMaker Server
FileMaker Server | マニフェスト
検索 (Cmd+/)
概要
クイック スタート
統合アシスタント
管理
ブランド化とプロパティ
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
保存
破棄
アップロード
ダウンロード
フィードバックがある場合
下のエディターを使用すると、JSON 表現を直接変更してこのアプリケーションを更新できます。詳細については、以下を参照してください。 Azure Active Directory アプリケーション マニフェストを確認します。
{
"id": "0613b841-36dd-4afd-b37e-d6af9e302a7c",
"acceptMappedClaims": null,
"accessTokenAcceptedVersion": null,
"addIns": [],
"allowPublicClient": null,
"appId": "db9a57a8-73e6-4f1e-a1bf-f871ed78c62c",
"appRoles": [],
"oauth2AllowUrlPathMatching": false,
"createdDateTime": "2022-01-24T09:38:15Z",
"description": null,
"certification": null,
"disabledByMicrosoftStatus": null,
"groupMembershipClaims": "SecurityGroup",
"identifierUris": [],
"informationalUrls": {
"termsOfService": null,
"support": null,
"privacy": null,
"marketing": null
},
"keyCredentials": [],
"knownClientApplications": [],
"logoUrl": null,
"logoutUrl": null,
"name": "FileMaker Server",
"notes": null,
"oauth2AllowIdTokenImplicitFlow": false,
"oauth2AllowImplicitFlow": false,
"oauth2Permissions": [],

FileMaker Serverでの設定

- FileMaker Server Admin Consoleで外部認証の設定を行う
  - Admin Consoleの［管理］>［**外部認証**］において［**定義済みアイデンティティプロバイダ (IdP) 認証設定**］＞［**Microsoft**］にある［変更］をクリック

Claris FileMaker Server

2022年1月24日 月曜日 18:47 サーバー | サインアウト

ダッシュボード | データベース | バックアップ | 構成 | コネクタ | 管理 | ログ

管理

ライセンスの管理、Admin Console アカウントの管理、外部認証の管理などのサーバーの管理タスクを実行できます。下のタブをクリックしてこれらの設定を指定してください。

- FileMaker ライセンス
- 管理者
- 外部認証

外部認証

定義済みアイデンティティプロバイダ (IdP) 認証設定

アイデンティティ認証プロバイダを構成する設定を指定します。その後、下のサインイン設定を有効にします。

Admin Console にサインインするための外部アカウント	未構成	変更
Amazon	未構成	変更
Google	未構成	変更
Microsoft	未構成	変更

https://YourDomain/oauth/redirect

Azure アプリケーション ID

Azure キー

Azure ディレクトリ ID

Microsoft Azure

認証設定を保存

カスタム IdP 認証設定

独自のカスタムアイデンティティ認証プロバイダを構成します。その後、下のサインイン設定を有効にします。

FileMaker Serverでの設定

- ［Azure アプリケーション ID］にアプリを追加した後に概要で確認した**アプリケーション (クライアント) ID**を入力
- ［Azure キー］にクライアント シークレットを追加した直後にコピーした**クライアント シークレットの値**を入力
- ［Azure ディレクトリ ID］にAzure ADの［概要］で確認した**テナント ID**を確認
- ［認証設定を保存］をクリック

管理

ライセンスの管理、Admin Console アカウントの管理、外部認証の管理などのサーバーの管理タスクを実行できます。下のタブをクリックしてこれらの設定を指定してください。

- FileMaker ライセンス
- 管理者
- 外部認証

外部認証

定義済みアイデンティティプロバイダ (IdP) 認証設定

アイデンティティ認証プロバイダを構成する設定を指定します。その後、下のサインイン設定を有効にします。

Admin Console にサインインするための外部アカウント	未構成	変更
Amazon	未構成	変更
Google	未構成	変更
Microsoft	未構成	変更

https://YourDomain/oauth/redirect

Azure アプリケーション ID

Azure キー

Azure ディレクトリ ID

Microsoft Azure

認証設定を保存

カスタム IdP 認証設定

独自のカスタムアイデンティティ認証プロバイダを構成します。その後、下のサインイン設定を有効にします。

FileMaker Serverでの設定

- Admin Consoleの［管理］>［外部認証］において［**データベースにサインイン**］＞［**外部サーバーアカウント**］を「有効」に変更
    - さらに［**Microsoft**］を有効に変更

ライセンスの管理、Admin Console アカウントの管理、外部認証の管理などのサーバーの管理タスクを実行できます。下のタブをクリックしてこれらの設定を指定してください。

- FileMaker ライセンス
- 管理者
- 外部認証

定義済みアイデンティティプロバイダ (IdP) 認証設定

アイデンティティ認証プロバイダを構成する設定を指定します。その後、下のサインイン設定を有効にします。

Admin Console にサインインするための外部アカウント	未構成	変更
Amazon	未構成	変更
Google	未構成	変更
Microsoft	構成済み	変更

カスタム IdP 認証設定

独自のカスタムアイデンティティ認証プロバイダを構成します。その後、下のサインイン設定を有効にします。

カスタム OAuth	未構成	変更

アイデンティティプロバイダを検証

Admin Console にサインイン

外部アカウント	未構成	

データベースにサインイン

外部サーバーアカウント	有効	
Amazon	未構成	
Google	未構成	
Microsoft	有効	
カスタム OAuth	未構成	

FileMaker Proでの設定

- ［ファイル］メニュー＞［管理］>［セキュリティ...］において［認証方法］を「**Microsoft Azure AD**」に変更
  - グループを新規追加（グループまたはユーザで「**グループ**」を選択）
    - グループ名にAzure ADで確認したグループの**オブジェクト ID**を入力
    - アクセス権セットは専用のものを作成して割り当てることを推奨

「TestDB」のセキュリティの管理

認証方法: Microsoft Azure AD 現在のホストでサポートされています

優先度	アクティブ	名前	アクセス権セット
1	✓	a8398cab-0e3f-43a4-b9...	OAuth

+新規

認証方法:

Microsoft Azure AD

グループまたはユーザ:

グループ ユーザ

グループ名 (オブジェクト ID):

a8398cab-0e3f-43a4-b93c-e8

アクティブ

アクセス権セット:

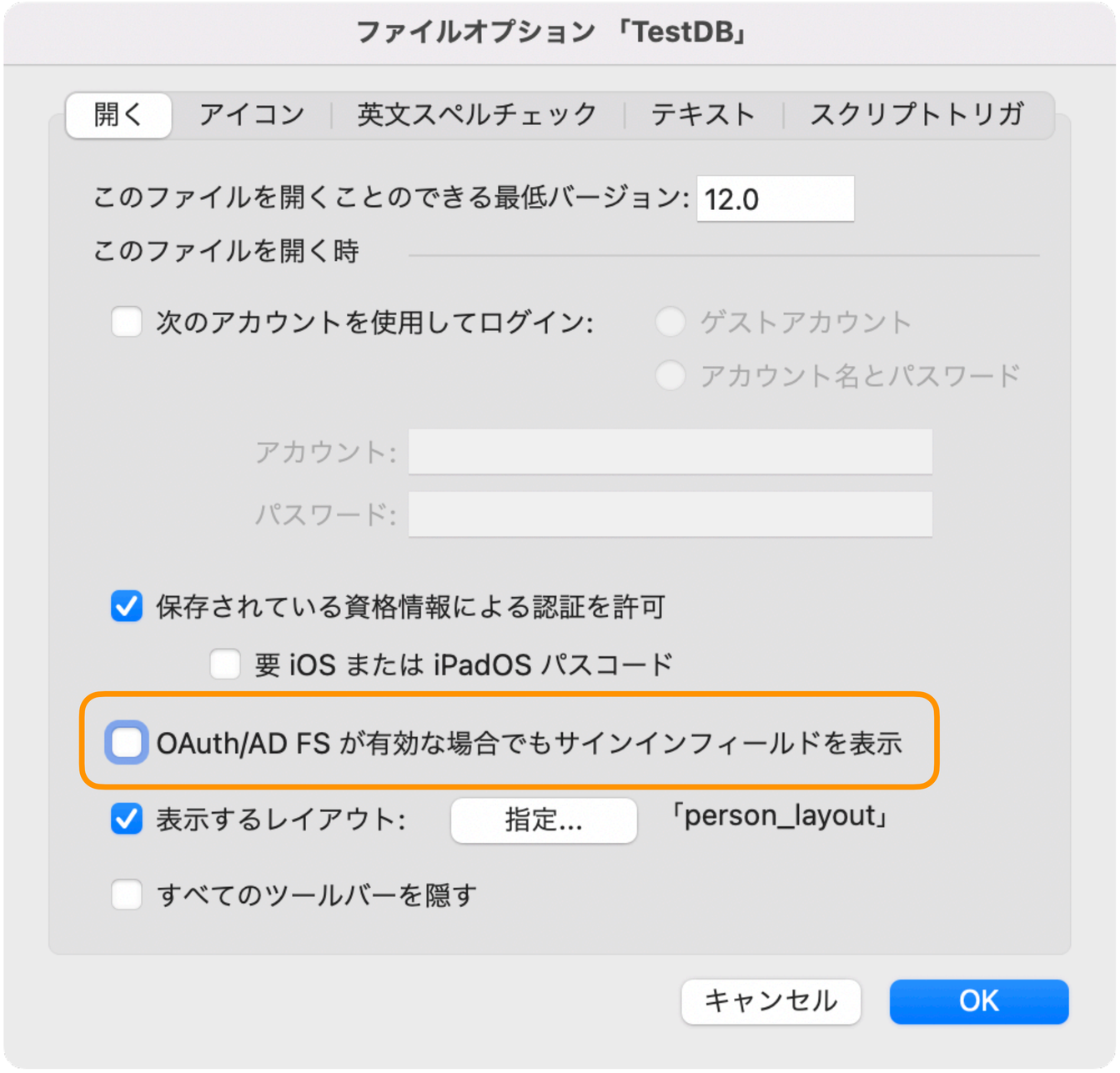
OAuth

説明:

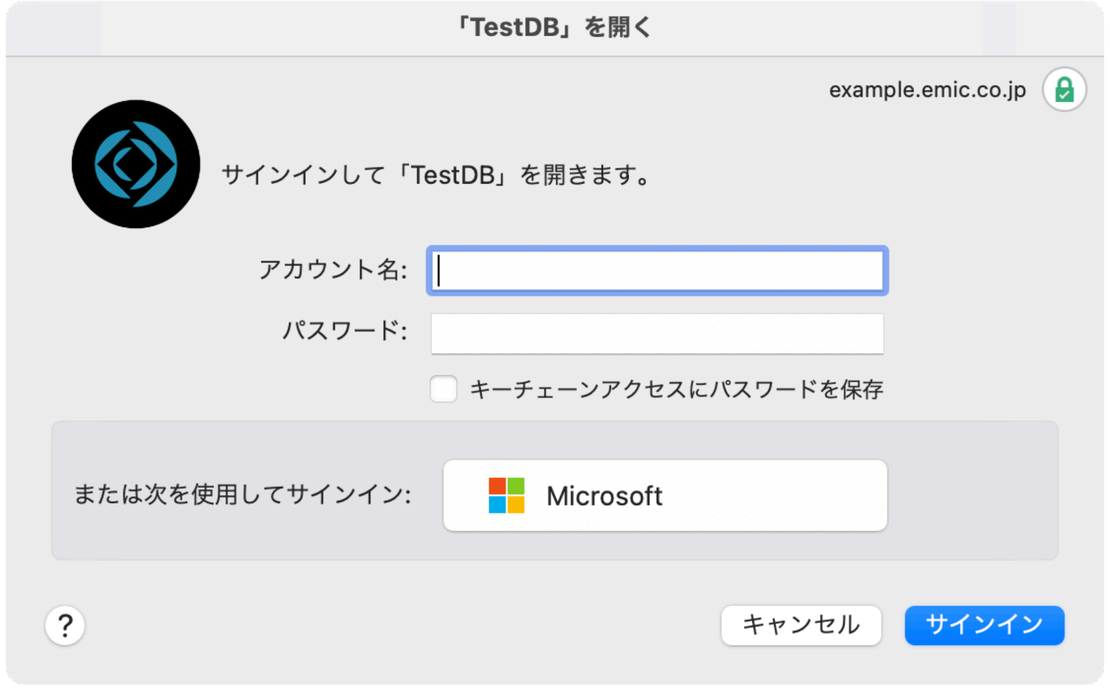
ユーザデータ...

FileMaker Proでの設定

- FileMaker Pro 19.2.2でOAuthでサインインする際にアカウント名およびパスワードフィールドが表示されないように
  - ［ファイル］メニュー＞［ファイルオプション...］の［**OAuth/AD FS が有効な場合でもサインインフィールドを表示**］オプションで調整可
  - Shiftキー（Windows）またはoptionキー（macOS）を押しながらファイルを開く方法でもサインインフィールドを一時的に表示可



サインインフィールドの表示を有効にすると



Azure Active Directory における設定時の注意点

Azure ADにおける設定時の注意点

- ［Azure Active Directory］の［プロパティ］ではディレクトリ IDではなく**テナント ID**を確認

- ［Azure Active Directory］の［アプリの登録］では（アプリケーションの種類ではなく）プラットフォームの選択において「**Web アプリ/API**」ではなく「**Web**」を選択

注）本資料は2022年1月時点の情報に基づいた解説となっています

Azure ADにおける設定時の注意点

- アプリの管理時においてはキーではなくシークレットを追加（［**証明書またはシークレットの追加**］をクリック）

- 新しいクライアント シークレットの追加直後に**クライアント シークレットの値をコピー**（この情報は再び表示されることはないため）

Azure ADにおける設定時の注意点

- アプリの［**マニフェスト**］の内容を要更新

  - 「"groupMembershipClaims": null,」を
    「"groupMembershipClaims": **"SecurityGroup",**」に変更・保存

（参考）Claris ナレッジベース

- オープン認証 (OAuth) 資格情報を使用したソリューションへのアクセス

  https://support.claris.com/s/answerview/?launguage=ja&anum=000025886

- Claris FileMaker Pro 19.2.2 リリースノート

  https://support.claris.com/s/answerview/?launguage=ja&anum=000035513

（参考）Claris ナレッジベース

- Accessing solutions using Open Authentication (OAuth) credentials

  https://support.claris.com/s/answerview?language=en_US&anum=000025886

- Authenticating OAuth groups via Microsoft Azure

  https://support.claris.com/s/answerview?language=en_US&anum=000025890

お知らせ

FMプラン

- 長年の運用実績と安心のサポート
- 大容量ストレージとファイルサーバー
- 月額料金に含まれる各種付帯サービス
- Webサーバー機能を備えて独自ドメイン名にも対応した上位プランも用意

➡詳しくは www.emic.co.jp/fmplan をご覧ください

Claris Partner

FMPress Forms

- Contact Form 7の機能を拡張するWordPressプラグインを公開
  - フォームデータをFileMakerデータベースにデータを登録
  - FileMaker ServerのFileMaker Data APIを利用
  - WordPress公式プラグインディレクトリから無料でダウンロード可能

➡ ［詳細］https://www.emic.co.jp/fmpress/forms/

エミックラーニング

- 弊社が提供するeラーニングサービス
  - Claris FileMakerやWordPressに関する知識について学習できるコンテンツを無料でご利用いただくことができます（要登録）
  - FMPress Formsを使用するにあたり必要となるClaris FileMakerやWordPressにおける具体的な設定方法を解説している動画もあります
  - FMPress Formsやfmcsadminに関するご質問およびご意見につきましてはエミックラーニングに用意しているフォーラムにお寄せください

➡［詳細］https://www.emic.co.jp/learning/

FMP48開発サービス

- 定額48万円（税別）で、お客さまのFileMakerデータベースに、WordPressを利用したWebアプリを追加する定額制対面開発サービス
  - データベース検索、Webフォームもしくはマイページ機能を備えたWebサイトを開発可能
  - 有料版のFMPress Proプラグインが含まれます

➡［詳細］https://www.emic.co.jp/fmpress/fmp48/

Claris Partner