mstep

Microsoft Dynamics 365 Finance / SCM 概説 Azure Active Directory 編

Microsoft Dynamics 365

2020年8月版

免責事項

MICROSOFT CONFIDENTIAL

本資料は情報提供のみを目的としており、本資料に記載されている情報は、本資料作成時点でのマイクロソフトの見解を示したものです。状況等の変化により、内容は変更される場合があります。本資料に表記されている内容（提示されている条件等を含みます）は、貴社との有効な契約を通じて決定されます。それまでは、正式に確定するものではありません。従って、本資料の記載内容とは異なる場合があります。マイクロソフトは、本資料の情報に対して明示的、黙示的または法的な、いかなる保証も行いません。

目次

- Azure Active Directory 概要
- Dynamics 365 Finance and Operations のサービスに外部からアクセスする
- Dynamics 365 Finance and Operations から Azure AD テナントのリソースにアクセスする

本資料では、Azure Active Directory のライセンスに関する説明はいたしません。
詳細については、下記の資料よりご確認ください。
https://azure.microsoft.com/ja-jp/pricing/details/active-directory/
https://docs.microsoft.com/ja-jp/azure/active-directory/fundamentals/active-directory-whatis

Azure Active Directory 概要

Azure Active Directory (Azure AD, AAD)

- Azure Active Directory は、Microsoft が提供するクラウドベースの ID およびアクセス管理サービス
- Azure AD ディレクトリには、必ず xxx.onmicrosoft.com という初期ドメイン名がつけられる
  初期ドメイン名に加えて組織のドメインを追加することもできる
  (カスタム ドメイン名を追加すると user@contoso.com のようなユーザー名を作成できる)

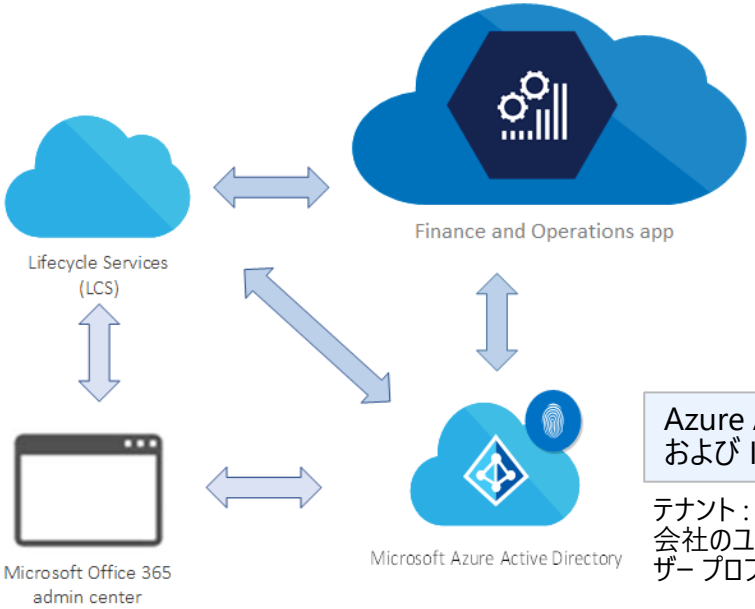
https://docs.microsoft.com/ja-jp/azure/active-directory/fundamentals/active-directory-whatis

Azure AD と Dynamics 365 Finance and Operations

Dynamics 365 Finance and Operations は ID のストアとして Azure Active Directory を使用

Lifecycle Services (LCS) はコラボレーション ポータルで、Dynamics 365 Finance and Operations アプリの実装のアプリケーション ライフサイクルを管理するための環境と定期的に更新されるサービスを提供する

LCS には Azure AD の資格情報を使用してログインする



Dynamics 365 Finance and Operations アプリは、LCS を介して展開される

Microsoft 365 管理センターは、ユーザー (Azure AD) およびサブスクリプションの管理機能を提供

Azure AD はクラウド ベースのディレクトリおよび ID 管理サービス

テナント : Azure AD で、テナントは組織を表す会社のユーザー情報が格納される (パスワード、ユーザー プロファイル データ、アクセス許可、その他)

https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/fin-ops/imp-lifecycle/architecture-overview

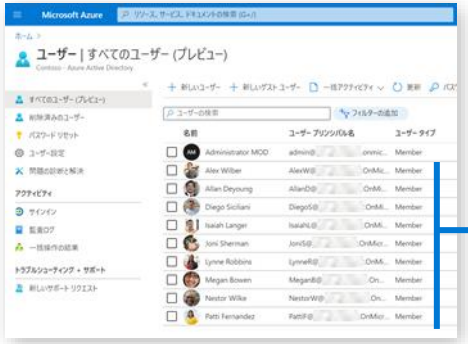
Azure AD と Dynamics 365 Finance and Operations

Dynamics 365 Finance and Operations にアクセスする際、Azure Active Directory の資格情報を使用

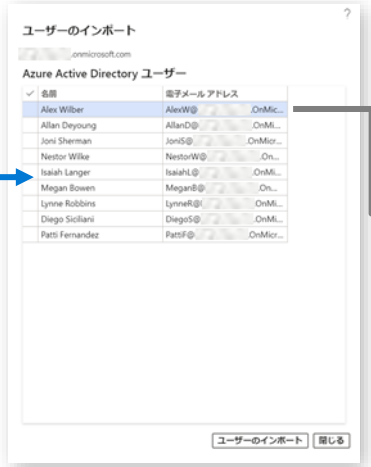
Azure AD と Dynamics 365 Finance and Operations

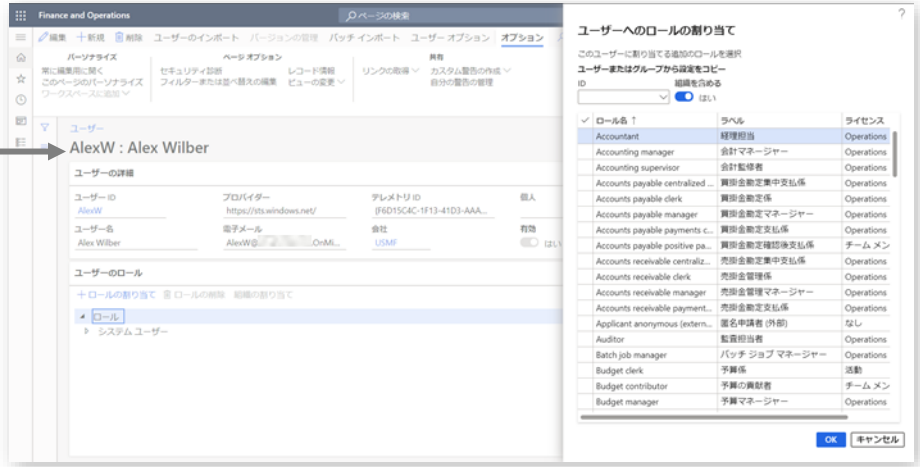
Azure Active Directory のユーザーを Dynamics 365 Finance and Operations にインポートして追加することも可能

Azure Active Directory



Dynamics 365 Finance and Operations



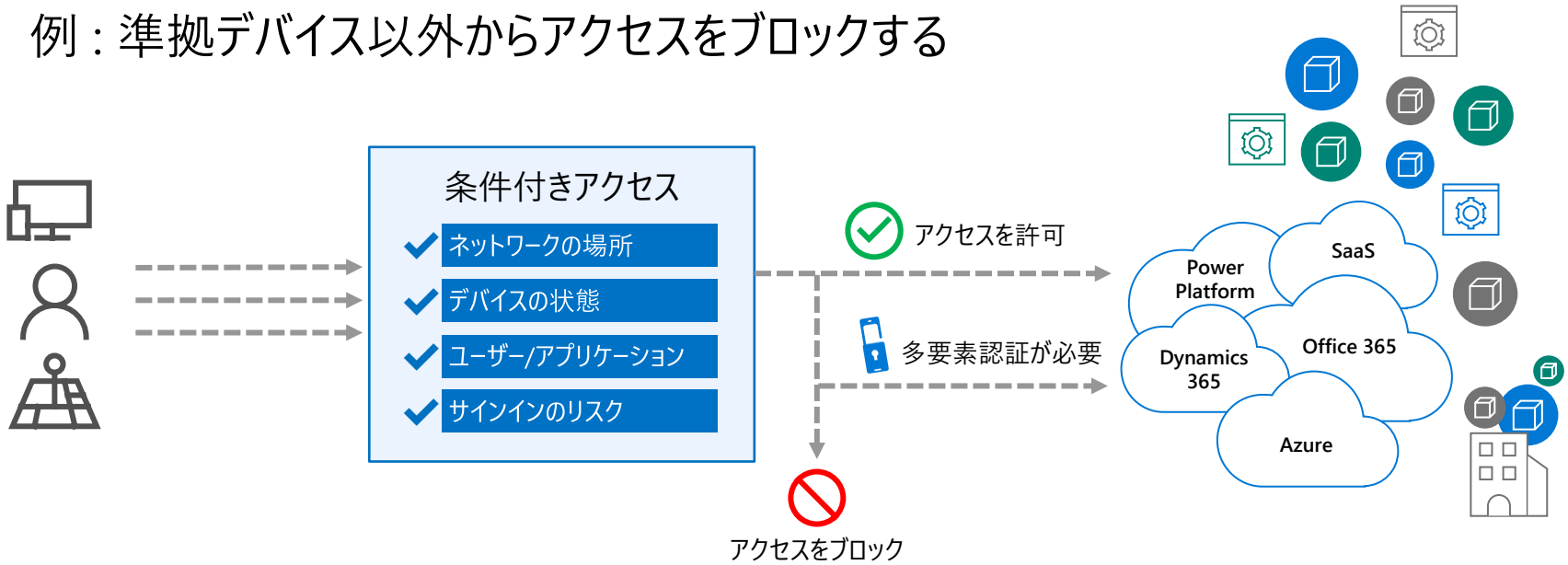


Azure AD の機能 : 条件付きアクセス

条件に基づいて適切なアクセス制御を適用し、組織のセキュリティを維持する

例 : 社外からサービスにアクセスする場合、多要素認証を必須にする

例 : 準拠デバイス以外からアクセスをブロックする



*条件付きアクセスは Azure AD Premium P1 ライセンスが必要

*内容によって、Intune、Azure AD Premium P2 ライセンスが必要

https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/overview

Azure AD の機能 : 多要素認証 (MFA)

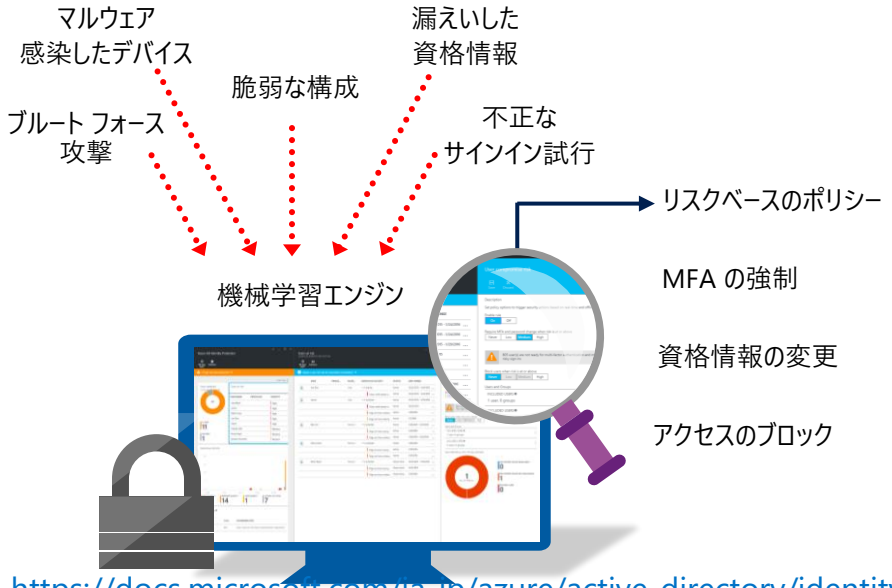
- 多要素認証は、サインイン プロセス中に追加で本人確認できるものをユーザーに求める仕組み
- 2 つ目の認証形式を義務付けることでセキュリティを向上
- 次の認証方法のうち 2 つ以上が必要とされる
  - ユーザーが知っているもの (通常はパスワード)
  - ユーザーが持っているもの (信頼できるデバイス)
  - ユーザー自身 (生体認証)

*内容によって、Azure AD Premium P1 または P2 ライセンスが必要

https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/concept-mfa-howitworks

Azure AD の機能 : Azure AD Identity Protection

- 機械学習とヒューリスティック システムによって、脆弱なアカウント、怪しいサインイン イベント、ユーザー イベントを検出する
- リスク イベントの内容に基づいて、リスク レベルを計算し、レポートとアラートを生成する
- リスク レベルに基づいてポリシーを実行し、組織の ID を自動的に保護する

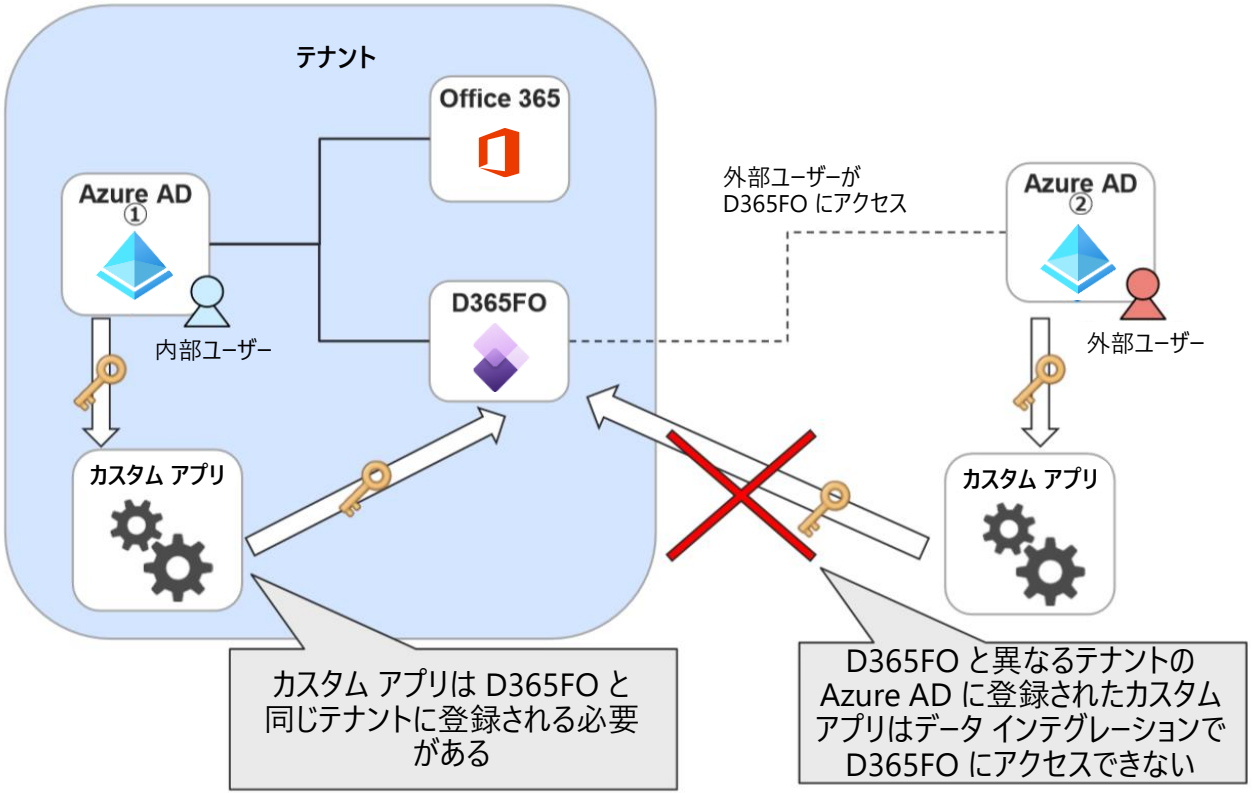


*Azure AD Premium P2 ライセンスが必要

https://docs.microsoft.com/ja-jp/azure/active-directory/identity-protection/overview-identity-protection

Dynamics 365 Finance and Operations のサービスに外部からアクセスする

Dynamics 365 Finance and Operations のサービスに外部連携する

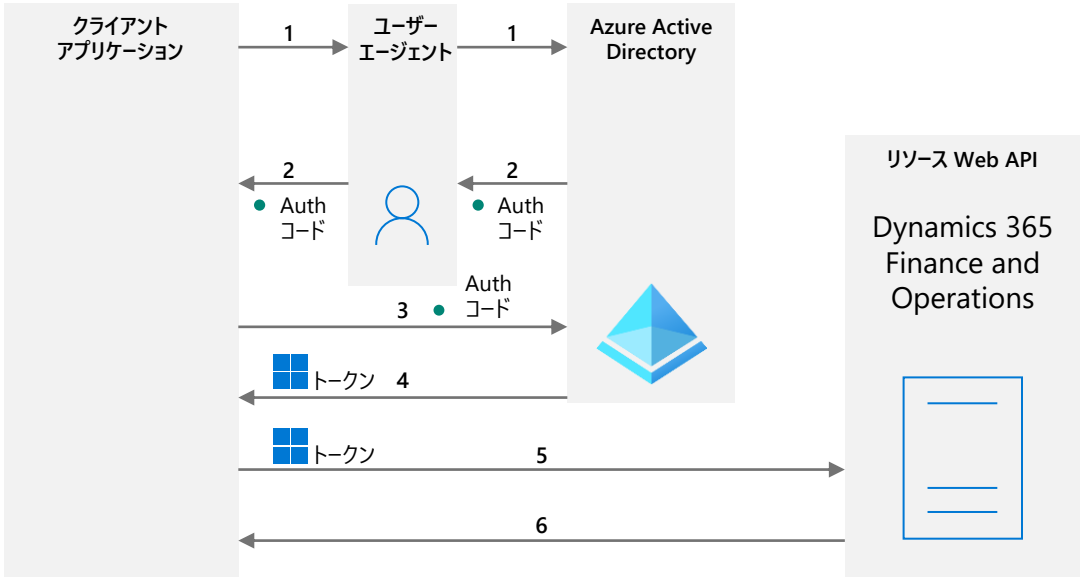


認証 (OAuth 2.0)

- OData サービス、JSON ベースのカスタム サービス、REST メタデータ サービスは標準の OAuth 2.0 認証をサポート
- “認証コードの付与フロー” や “クライアントの資格情報を使用したサービス間の呼び出し” をサポート
- Azure Active Directory では、以下の 2 種類のアプリケーションがサポートされる
  - ネイティブ クライアント アプリケーション
    ユーザー名とパスワードで認証
  - Web アプリケーション
    シークレットまたは証明書で認証

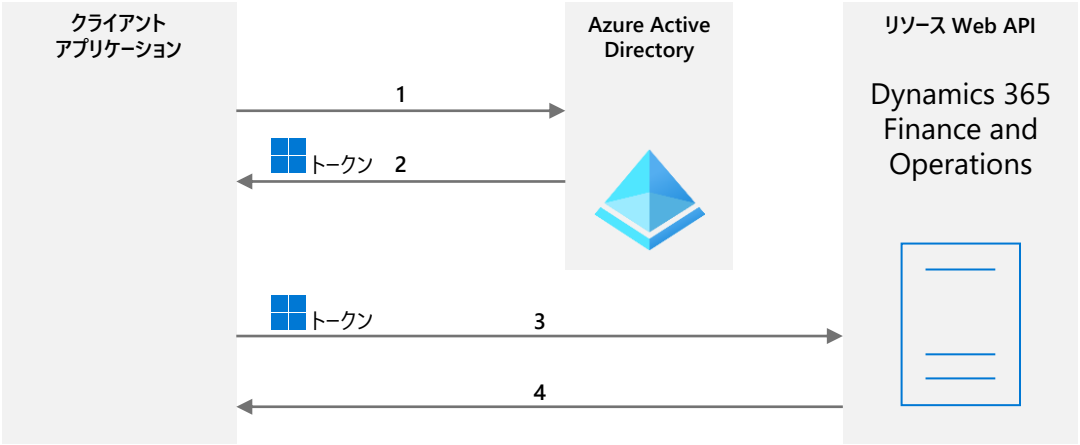
https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/dev-itpro/data-entities/services-home-page

認証コード付与フロー



https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/dev-itpro/data-entities/services-home-page

クライアント資格情報付与フロー



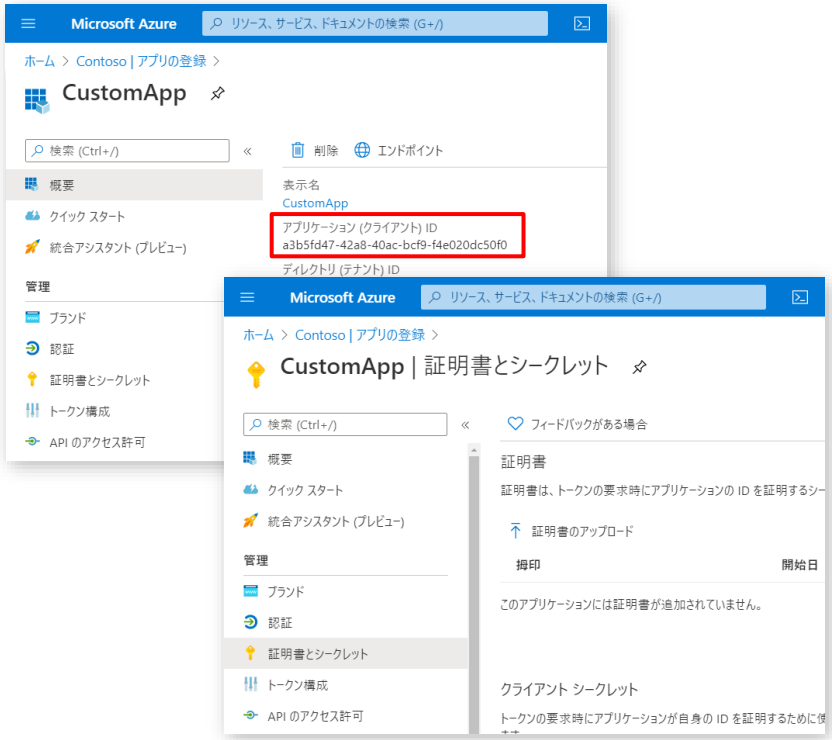
https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/dev-itpro/data-entities/services-home-page

アプリで認証を行うための準備

Azure Active Directory にアプリを登録

クライアントがサービスと通信する際、Azure Active Directory にアプリ登録が必要

- Azure Portal の [Azure Active Directory] – [アプリの登録] にアクセス
- [新規] をクリックし、アプリケーションの名前を設定してアプリを登録し、必要に応じてシークレットの作成、API のアクセス許可の設定などを行う

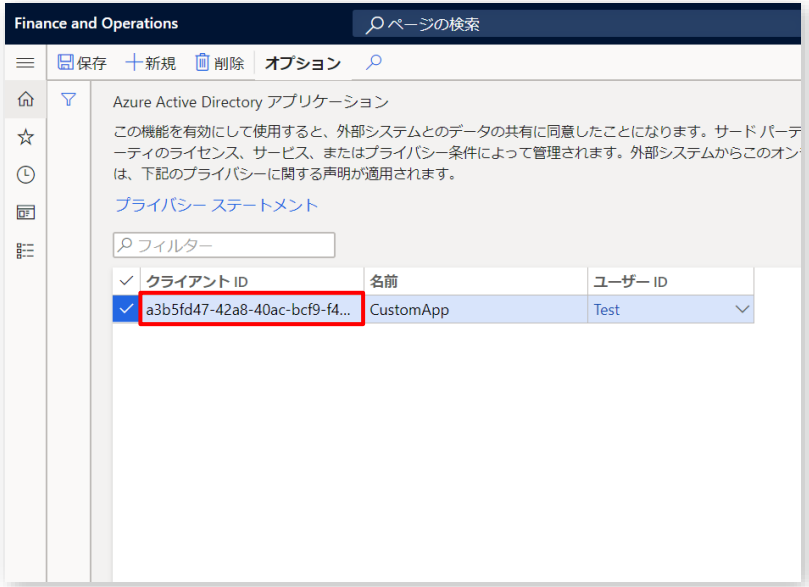


https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/dev-itpro/data-entities/services-home-page

アプリで認証を行うための準備

Dynamics 365 Finance and Operations で Azure Active Directory アプリを登録

- システム管理> 設定 > Azure Active Directory アプリケーション にアクセス
- [新規] をクリックし、"クライアント ID" には Azure Active Directory に登録したアプリケーション ID、"名前" にはアプリケーションの名前、"ユーザー ID" にはサービス アカウントのユーザー ID を設定



https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/dev-itpro/data-entities/services-home-page

認証の実装

Authentication flows

https://docs.microsoft.com/en-us/azure/active-directory/develop/msal-authentication-flows

Microsoft identity platform code samples (v2.0 endpoint)

https://docs.microsoft.com/en-us/azure/active-directory/develop/sample-v2-code

Azure Active Directory code samples (v1.0 endpoint)

https://docs.microsoft.com/en-us/azure/active-directory/azuread-dev/sample-v1-code

Dynamics 365 Finance and Operations から Azure AD テナントのリソースにアクセスする

Dynamics 365 Finance and Operations の外のリソースにアクセスする

Dynamics 365 Finance and Operations から、Azure AD テナントによってセキュリティ保護されたリソースにアクセスするために、Azure AD にアプリケーションを登録し、サービス プリンシパルを作成する

例 : Entity Store のデータを Azure Data Lake Storage Gen2 へエクスポートする

https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/dev-itpro/data-entities/entity-store-data-lake

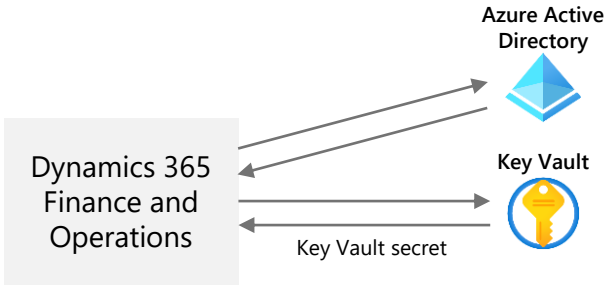
例 : ビジネス イベントをエンドポイント (Azure Service Bus など) に送信する

https://docs.microsoft.com/ja-jp/dynamics365/fin-ops-core/dev-itpro/business-events/how-to/how-to-servicebus

Dynamics 365 Finance and Operations の外のリソースにアクセスする

前述の ADLS やビジネス イベント利用時の Azure AD の設定について要約

- Azure AD にアプリを登録 (アプリケーション ID を作成) し、シークレットを作成
- Key Vault を作成し、該当の接続文字列を入力したシークレットを作成
- サービス プリンシパルを Key Vault に追加して、Key Vault のシークレットを取得するためのアクセス許可を設定
- Dynamics 365 Finance and Operations の該当機能に、アプリケーション ID/アプリケーション シークレット および Key Vault の DNS 名/シークレット名を設定



Dynamics 365 Finance and Operations が Key Vault のシークレット (つまり、接続文字列) を取得し、目的の処理 (ADLS への接続等) を行う

MICROSOFT CONFIDENTIAL

本資料は情報提供のみを目的としており、本資料に記載されている情報は、本資料作成時点でのマイクロソフトの見解を示したものです。状況等の変化により、内容は変更される場合があります。本資料に表記されている内容（提示されている条件等を含みます）は、貴社との有効な契約を通じて決定されます。それまでは、正式に確定するものではありません。従って、本資料の記載内容とは異なる場合があります。マイクロソフトは、本資料の情報に対して明示的、黙示的または法的な、いかなる保証も行いません。