

Microsoft Graph テクノロジーを使用して Azure AD からデータを取得する場合、自分または Azure ポータルで構成を行う必要があります。

1. ディレクトリへのアクセスを許可するために使用されるアプリケーションを登録します。

The screenshot shows the Azure AD App Registrations page for the domain 'openlm.com'. The left-hand navigation pane has 'App registrations' highlighted with a red box. The main content area displays a table of registered applications. A red arrow points from the 'App registrations' menu item to the first application in the table.

Display name	Application (client) ID
DSA.openlm.com	66700ba9-9f7f-436d-bf55-a8b2aa3e7c25
openlm-OpenLM-bdc2419f-bc87-4c25-a70c-70afa969c90d	6b97c036-43d8-497a-866d-fd4665430602
openlm-OpenLM-bdc2419f-bc87-4c25-a70c-70afa969c90d	5f5b9697-bc0a-404a-b9cd-2a472a45482e
openlm-OpenLM-bdc2419f-bc87-4c25-a70c-70afa969c90d	3f3ef609-e1d4-4663-98e5-194037df2247

2. 登録時に、パラメータ `client_id`、`tenant_id`、`client_secret` を取得します。最後は 1 回だけ表示されるため、ユーザーは覚えておく必要があります。これらのパラメーターは、Azure AD の DSS UI ドメイン設定で入力する必要があります (`client_secret` は DSS DB で暗号化されます)。これらのパラメーターは、Microsoft Graph サービスに接続して承認するために DSA によって使用され、Azure ディレクトリに関するデータが返されます。

The screenshot shows the details page for the application 'DSA.openlm.com' in the Azure AD App Registrations portal. The 'Essentials' section is expanded, showing the following information:

- Display name : DSA.openlm.com
- Application (client) ID : 66700ba9-9f7f-436d-bf55-a8b2aa3e7c25
- Directory (tenant) ID : 8450043-10000000000000000000000000000000
- Object ID : 2a45d2-10000000000000000000000000000000

The application ID, tenant ID, and object ID values are redacted with black bars. The left-hand navigation pane shows 'Overview' selected.

3. アプリケーションにアクセス許可を付与します (DSA がデータを取得できるようにするため)。

Search (Ctrl+/)

Refresh | Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles | Preview
 - Owners
 - Roles and administrators | Preview
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Some actions may be disabled due to your permissions. To request access, contact the application owner(s) or your administrator. [View application owners](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for openlm.com

API / Permissions name	Type	Description	Admin consent req...	Status	
▼ Microsoft Graph (8)					
AdministrativeUnit.Read.All	Application	Read all administrative units	Yes	✓ Granted for openlm.com	...
Group.Read.All	Application	Read all groups	Yes	✓ Granted for openlm.com	...
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for openlm.com	...
Organization.Read.All	Application	Read organization information	Yes	✓ Granted for openlm.com	...
People.Read.All	Application	Read all users' relevant people lists	Yes	✓ Granted for openlm.com	...
TeamMember.Read.All	Application	Read the members of all teams	Yes	✓ Granted for openlm.com	...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for openlm.com	...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for openlm.com	...

To view and manage permissions and user consent, try [Enterprise applications](#).

ディレクトリ同期 Azure ディレクトリ

ドメインの追加

新しいディレクトリ タイプ Azure Directory をドメイン マネージャー画面に追加します

選択しそれに応じて以下のフィールドを更新します

1. ドメイン名: フリーテキスト
2. ディレクトリ (tenant) ID **-NEW**
3. アプリケーション (client) ID **-NEW**
4. クライアントシークレット **-NEW**

アプリケーション (client) ID とクライアント シークレットは、Azure ディレクトリ (tenant) ID による認証に使用されます。

DSS

ADD DOMAIN ⓘ

Directory type
Active Directory

Domain name
Domain name

Port
389

SSL

Username
Username

Password
Password

CHECK DOMAIN CONNECTIVITY

SAVE SAVE DOMAIN & ADD SYNC

ドメイン接続のチェックと保存ボタンはそのままにしておきます...

同期設定

目的地と時刻

開始ノードのオプション: LDAP ディレクトリとは異なり、Azure の構造は異なります: ユーザーは次のことを行うことができます。

1. 値を空のままにします。その場合、同期はすべてのユーザーとグループがします。(LDAP の root オプションのような)
2. グループ/グループ名 -同期を開始したいグループを入力し、特定のグループから同期します。Azureグループはすべて同じレベルで開かれており、他のどのグループがどのグループに接続されているかを示すポインタを持っています。
その場合、深度を使用すると、設定された検索深度の値に従って、元の開始グループに接続されている他のグループがスキャンされます。開始ノード名を **Start Sync From** で変更します。

目的地と時刻の情報アイコン内の以下のテキストを更新します。

開始ノード: 同期をどこから開始するかを定義します。ディレクトリ内のすべてのユーザーとグループを同期するには空のままにするか、開始したいグループ **"groups/groupname"** を指定します。構成が完了した

ら、「テスト」をクリックしてドメインが有効であることを確認します (テストが完了するまでに最大 2 分かかる場合があります)。

インラインテキスト:すべてのディレクトリを同期するには空のままにするか、*groups/<group name>*を入力します(1グループのみ許可)。

The screenshot shows the 'ADD SYNC' configuration page in the DSS interface. The page is divided into three tabs: 'Destination & Time', 'Object', and 'Group Rules'. The 'Destination & Time' tab is active. It contains a 'Sync name' field with a red error message 'This field is required.' and a 'Status' toggle switch. Below are 'Agent' and 'Domain name' dropdown menus. The 'Start Node' field contains 'LDAP://Domain' and has a 'TEST' button. The 'Sync Schedule' section has radio buttons for 'By Time' (selected) and 'By Interval'. Below are 'Days' and 'Start Time' dropdowns, and a table with 'Day' and 'Start Time' columns.

オブジェクト

オブジェクトの種類

バージョン 1 のオブジェクト タイプ「コンピュータ」はサポートされていません。代わりに、Azure AD には [devices](#) があります。しかし、まだ調査する必要があります。コンピューターのオプションを削除してください。

「オブジェクト」タブの情報テキストを更新します。オブジェクトの同期: どのオブジェクトを同期するかを構成します (現在、ユーザーオブジェクトのみがサポートされています)

同期属性

Azure ディレクトリのデフォルト値は UserPrincipalName です。CN と SAMaccountName を DD リストから削除してください。ユーザーは同期したい属性を入力できます (フリーテキスト)。

メンバーシップフィルター:

Azure ディレクトリが選択されている場合、DD リストが更新されて 2 つのオプションが表示されます

1. すべてのオブジェクト
2. グループメンバーのみ

Azure AD には OU がなく、代わりにAdministrative unitsがありますが、これらのユニットの下に他のユニットを保持することはできません。バージョン 1 についてはサポートされません。

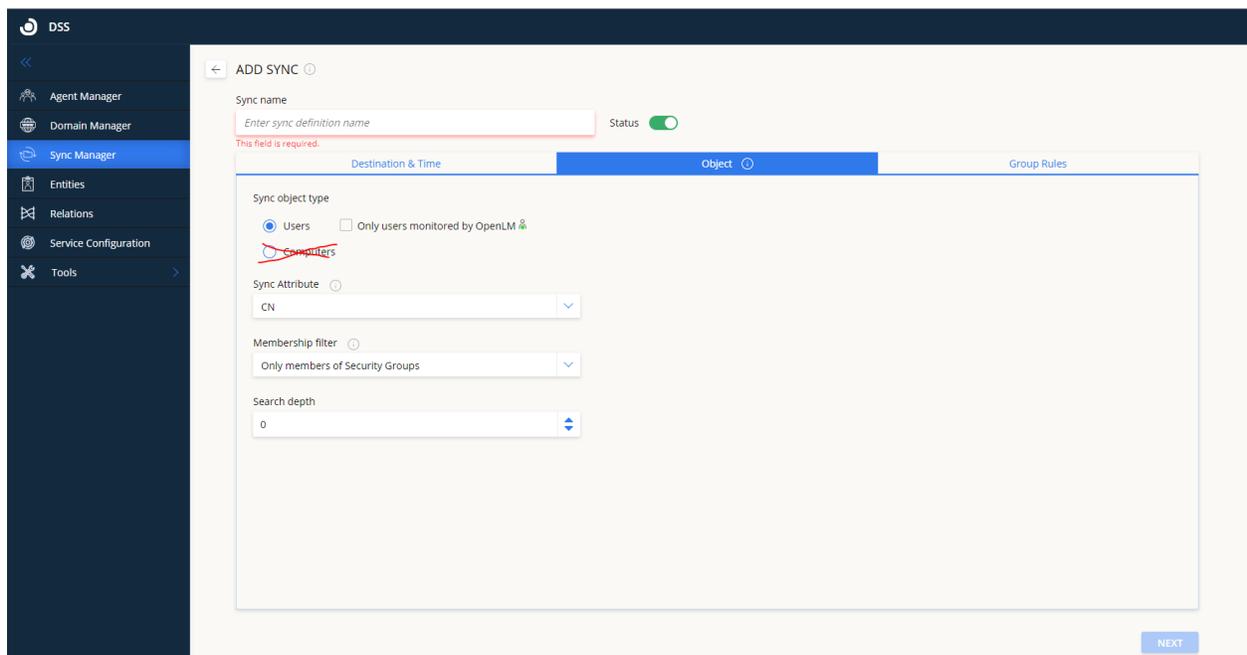
メンバーシップ フィルターの情報アイコンを更新します (Azure Active Directory が選択されている場合のみ)メンバーシップフィルター

すべてのオブジェクトを同期するかどうかを選択します。またはグループに属するもののみ。

検索の深さ

検索の深さは、グループの「開始ノード」を操作する場合にのみ関係します。。

「Start Sync From」がグループを示している場合のみ、ユーザーが検索の深さを入力できるようにする。それが空の場合は、「同期開始元」グループを設定しない限り、検索の深さは 0 にする必要があります。」というエラー メッセージが表示されます。



グループルール

すべてのグループルールがサポートされています (標準 LDAP と同じリスト)。hierarchy synchronizationはグループのみをサポートします。したがって、チェックボックスを選択する必要はありません。

「グループの作成に使用するオブジェクトクラスを選択してください」の代わりに「階層グループは、以下で指定したグループと検索の深さに従って作成されます」と書きます。

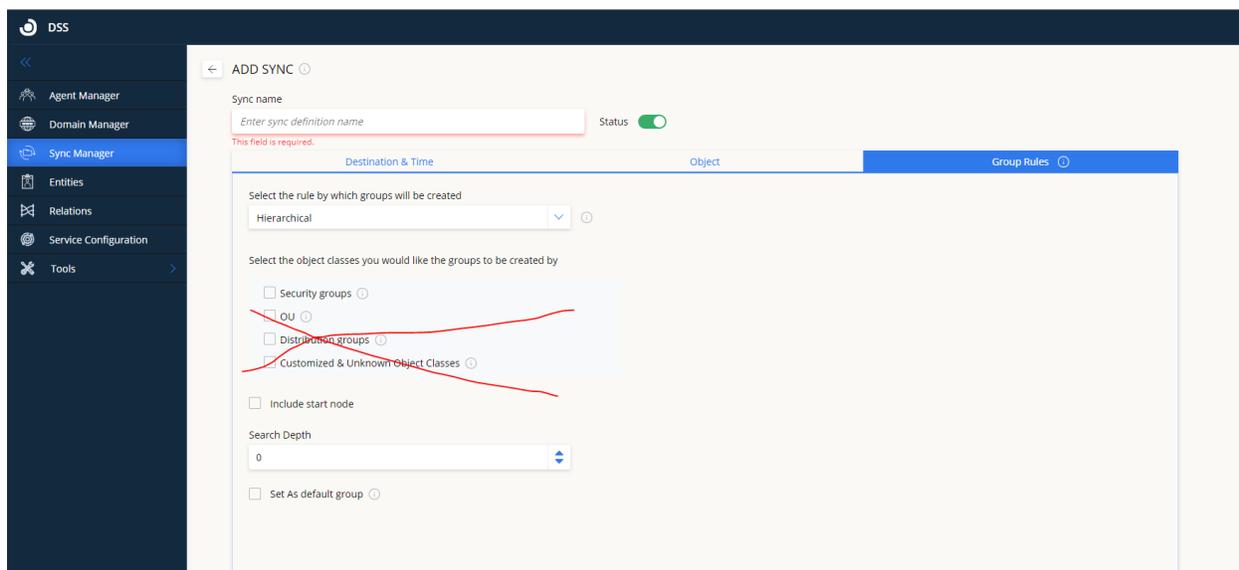
残りのオプション (OU、ディストリビューショングループ、カスタマイズおよび不明なオブジェクトクラス) を削除してください。

開始ノードを含める: 開始グループを含めるに変更します。

検索の深さ - オブジェクト画面で選択した検索深度を超えることはできません。

デフォルトグループの設定 - サポートされています

「開始ノードを含める」を「開始グループを含める」に変更します (開始グループに接続しているユーザーを取得し、開始グループ名の下にグループとして追加します)。



ディレクトリサンプル

ディレクトリにはグループ A ~ E があります

→ あるグループから別のグループへのポインタを示します

A → B

B → C

C→D
C→A
D→E
E

ユーザーリスト:

グループ A - U5、U6

グループ B - U7、U8

グループ C - U1、U2、U3、U4

グループ D - U9、U10

グループ E - U11、U12

グループとルールの検索深さ 3 で Groups\C から同期するように同期が構成されている場合の階層構造

C--

A--

B--

D--

E

U1

U2

U3

U4

U5

U6

U7

U8

U9

U10

U11

U12