

Directory Synchronization – 総合ガイド KB500

by Fumichika Yoshida | Jun 12, 2020

本書は**Directory Synchronization Service (DSS)** と **Directory Synchronization Agent (DSA)** コンポーネントを使用して、組織のディレクトリサービスとOpenLMデータベースを同期する方法を説明する詳細なガイドです。クイックスタートガイド（概略）については [こちら](#) を参照ください。

目次:

1. 概要

2. 要件

3. インストール

3.1. Directory Synchronization Service (DSS)

3.2. Directory Synchronization Agent (DSA)

4. 設定

4.1. Directory Synchronization Service (DSS)

4.2. OpenLM Serverバージョン4.xのLDAP同期定義を移行する

4.3. DSS設定ツール

DB 設定

DB アップグレード

5. 使用

5.1. エージェントマネジャー

5.1.1. 新規エージェントを承認

5.1.2. エージェントプロパティの編集

5.1.3. エージェントプロパティの一括編集

5.1.4. エージェントの削除

5.2. ドメインマネジャー



5.2.1. 新規同期ドメインの追加

5.2.2. ドメインプロパティの編集

5.2.3. ドメインの削除

5.3. 同期マネージャー

5.3.1. 新規同期定義の追加

Destination & Time タブ

Object タブ

Group Rules タブ

Set as default group チェックボックス

5.3.2. 手動で同期を開始する

5.3.3. エンティティ・リレーションシップ・データのリセット

5.3.4. 同期定義の削除

5.4. エンティティ

5.4.1. 全ての同期からエンティティを無視する

5.4.2. 手動でエンティティを同期

5.4.3. エンティティ・リレーションシップを見る

5.5. リレーション

5.5.1. 特定の同期からエンティティを無視する

1. 概要

OpenLMはドメインディレクトリ（例：アクティブディレクトリ）のユーザー情報をOpenLMデータベースを同期する機能を提供します。これは**Directory Synchronization Service (DSS)** と**Directory Synchronization Agent (DSA)** コンポーネントを使用する事で遂行できます。

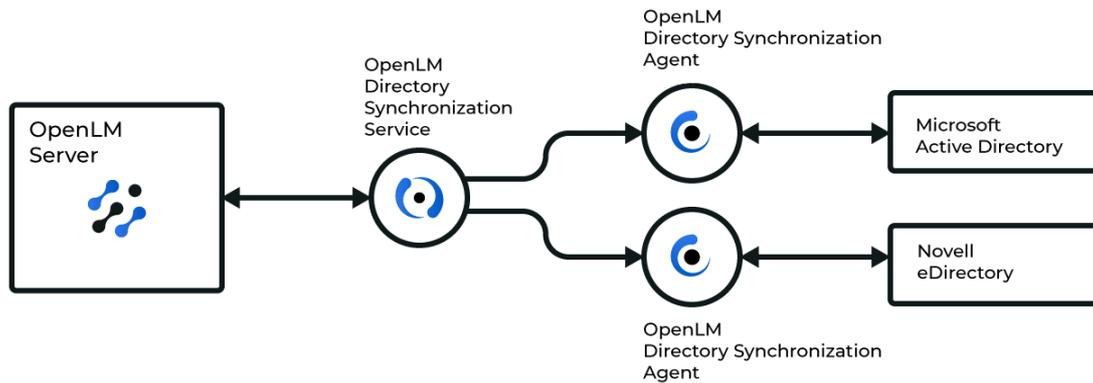
以前、この機能はLDAP同期と呼ばれており、OpenLM Server機能の一部でした。パフォーマンスと安定性を向上させるため、この機能はOpenLM Serverから分離され、DSSとDSAの2つのコンポーネントに分けられました。

LDAP同期を実行するためには両方のコンポーネントのインストールが必要です。



構造概要：

1. DSSはOpenLM Serverに直接接続します。OpenLM Serverと同じマシンか別のマシンにインストールする事ができます。DSSの機能は同期定義を保存する事とDSAを管理する事です。
2. 1つ以上のDSAがDSSに接続します。DSAはDSSと同じマシンか別のマシンにインストールする事ができます。DSAの機能はDSSから同期定義を受け取り、ドメインディレクトリをクエリし、データをDSSに報告します。
3. DSSがDSAからデータを受け取ると、DSSはOpenLM Serverへデータを送信します。



注意: 単一のDSAは複数のディレクトリ（例；ADとeDirectoryの両方）をクエリするように使用する事もできます。このダイアグラムは2つのDSAが使用されていますが、多くの可能な設定の中の一つに過ぎません。

2. 要件

1. OpenLM Serverバージョン5以上
2. Directory Synchronization拡張機能をサポートするOpenLMライセンスファイル (sales@openlm.comにコンタクトしてください)
3. OpenLM Serverと別のマシンにDSSやDSAをインストールする場合、そのマシンがドメインコントローラーと同じネットワークに属する事を必ず確認してください。

ポート設定:

OpenLM Serverと別のマシンにDSSやDSAをインストールする場合、適切なファイアウォール規則がアプリケーションポートに設定されているか必ず確認してください。

1. OpenLM Serverマシン: インバウンド5015、アウトバウンド7026
2. DSS マシン: インバウンド、アウトバウンド共に7026

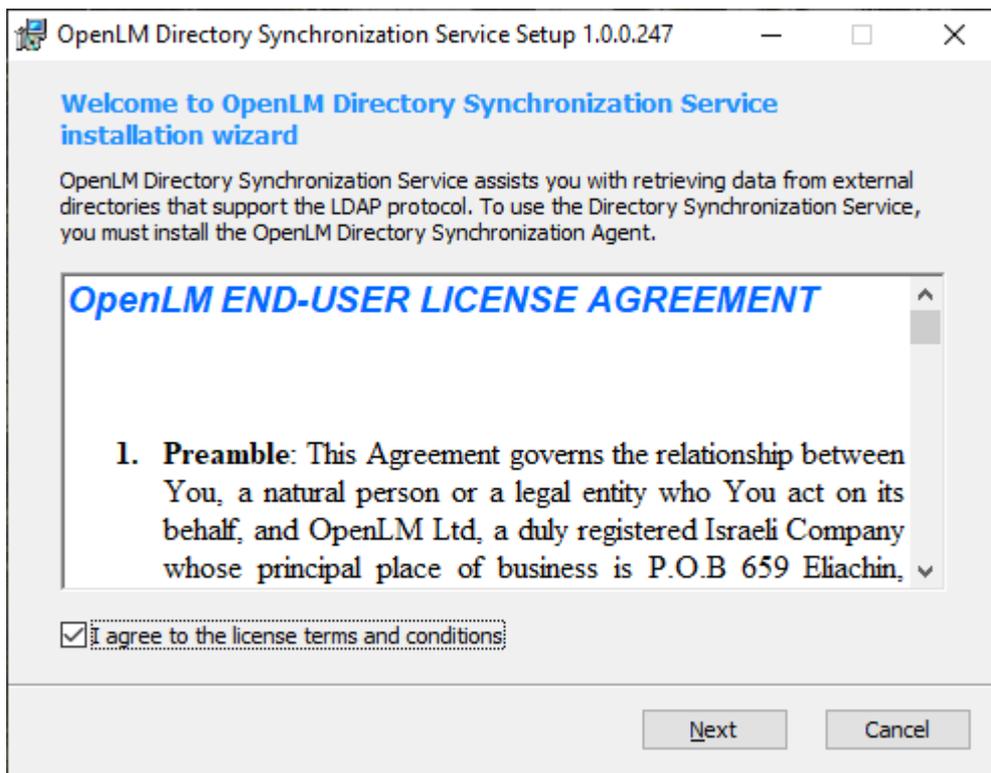


3. DSA マシン: アウトバウンド7026

3. インストール

3.1. Directory Synchronization Service (DSS)

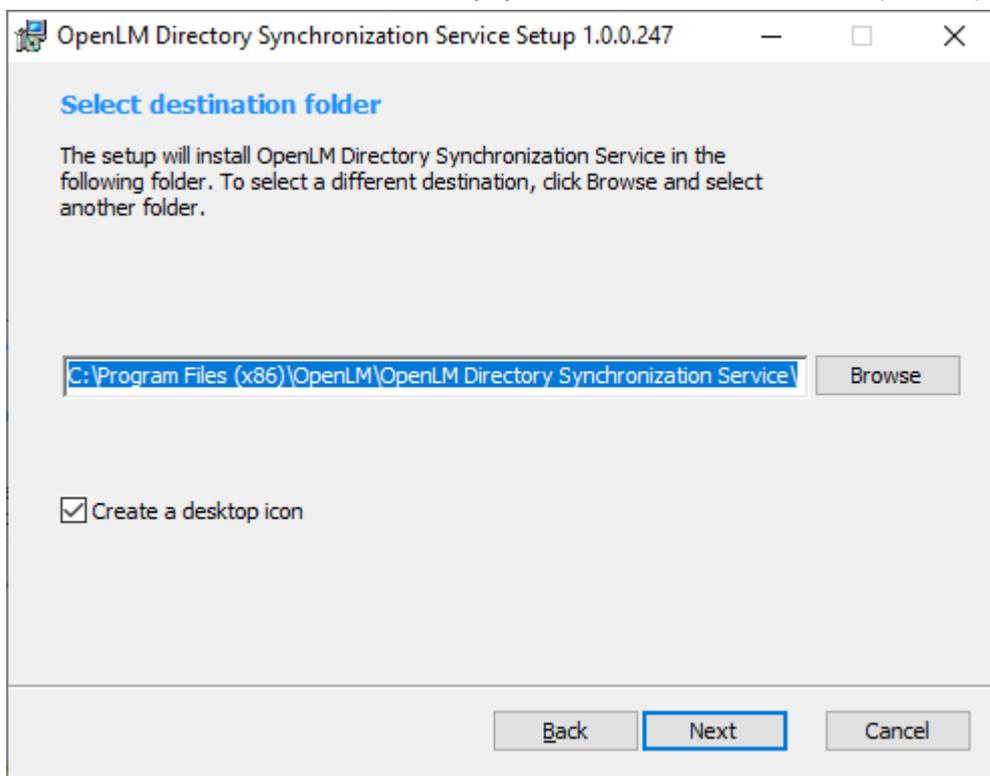
1. ダウンロード ページから最新のDSSをダウンロードしてください。インストーラーをダブルクリックして実行してください。



2. “I agree to the license terms and conditions”（利用規約に同意する）ボックスをチェックして**Next（次へ）** をクリック

3. インストールフォルダーを変更できます。更に、“Create a desktop icon”（デスクトップアイコンを作成）ボックスをチェックすると、DSSのWEBインターフェイスへのショートカットアイコンがデスクトップに作成されます。**Next（次へ）** をクリック。

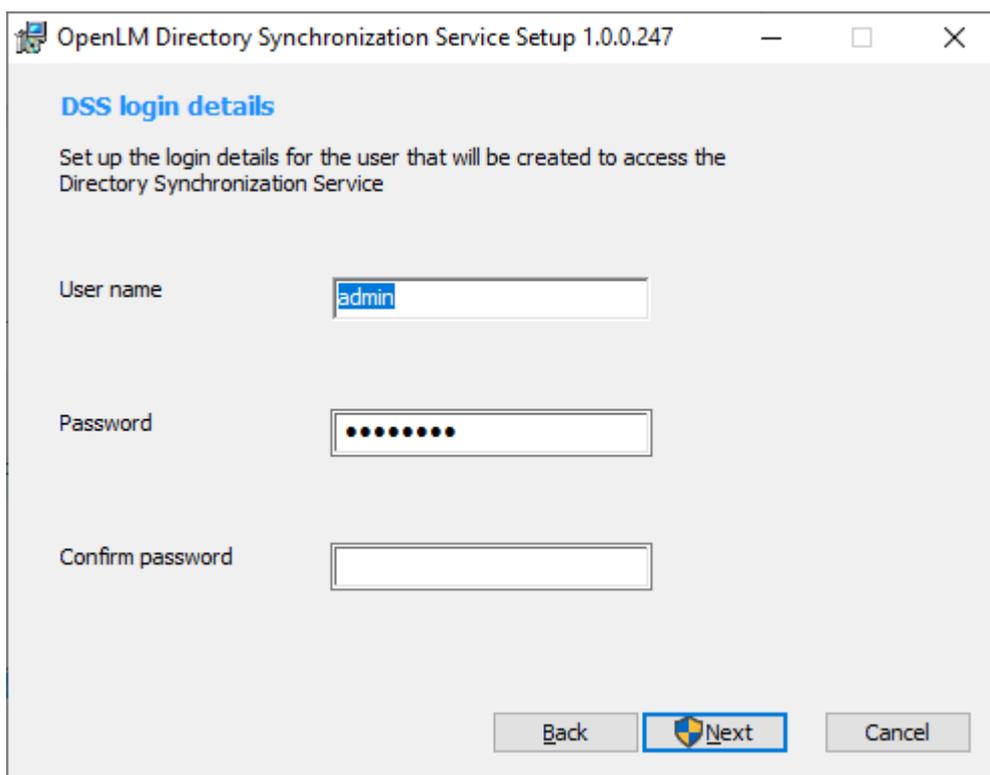




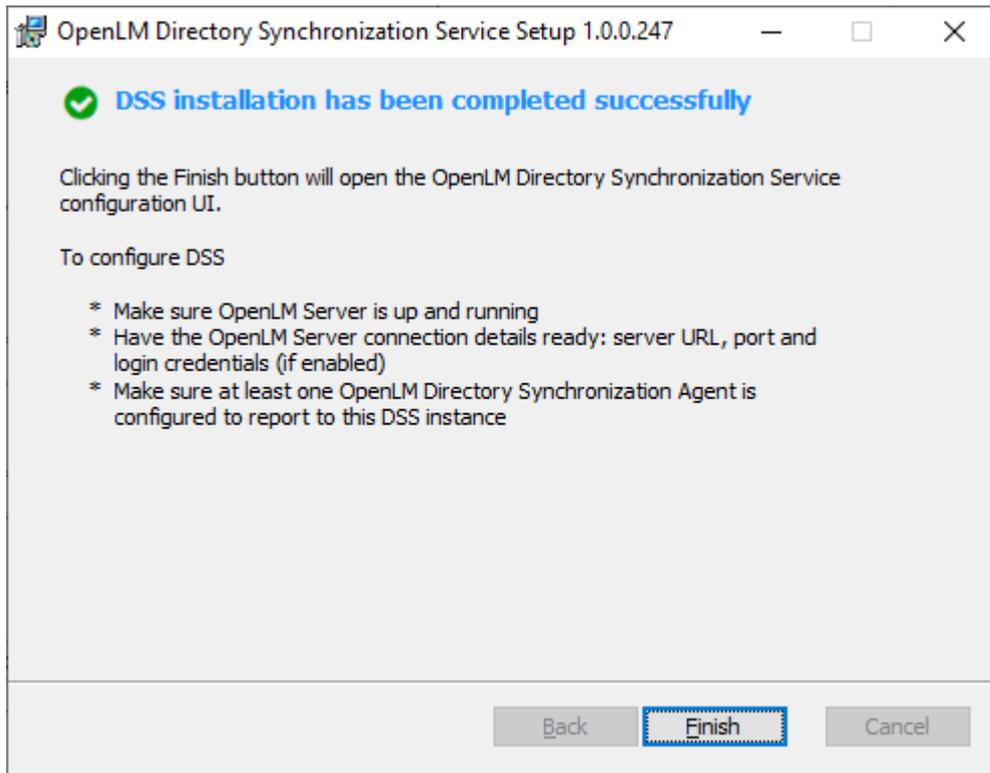
4. DSSにアクセスするために作成するユーザーのログイン詳細を入力してください。 **Next (次へ)** をクリック。

Password requirement (パスワード要件) : 少なくとも8文字。少なくとも小文字を1つ + 大文字を1つ、特殊文字を1つ、数字を1つを含むこと。

注意: このユーザーはDSSを管理するためだけに作成されます。OpenLM Serverのアドミンユーザーとは関係ありません。



5. セットアップが完了したら**Finish (終了)** をクリック。セットアップウィザードを閉じてブラウザでDSSユーザーインターフェイスを開きます。

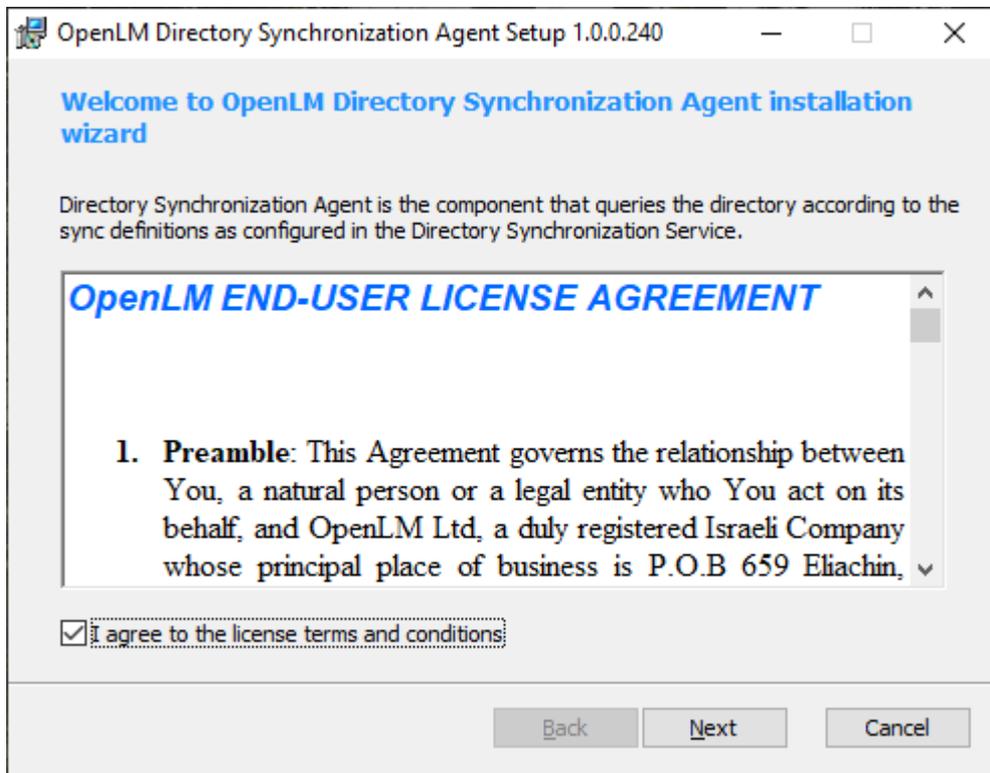


注意: DSSの使用を開始するには、少なくとも1つのDSAインスタンスをインストールする必要があります。(下記説明参照)これが完了すれば、セットアップを完了するために設定セクションに進むことができます。

3.2. Directory Synchronization Agent (DSA)

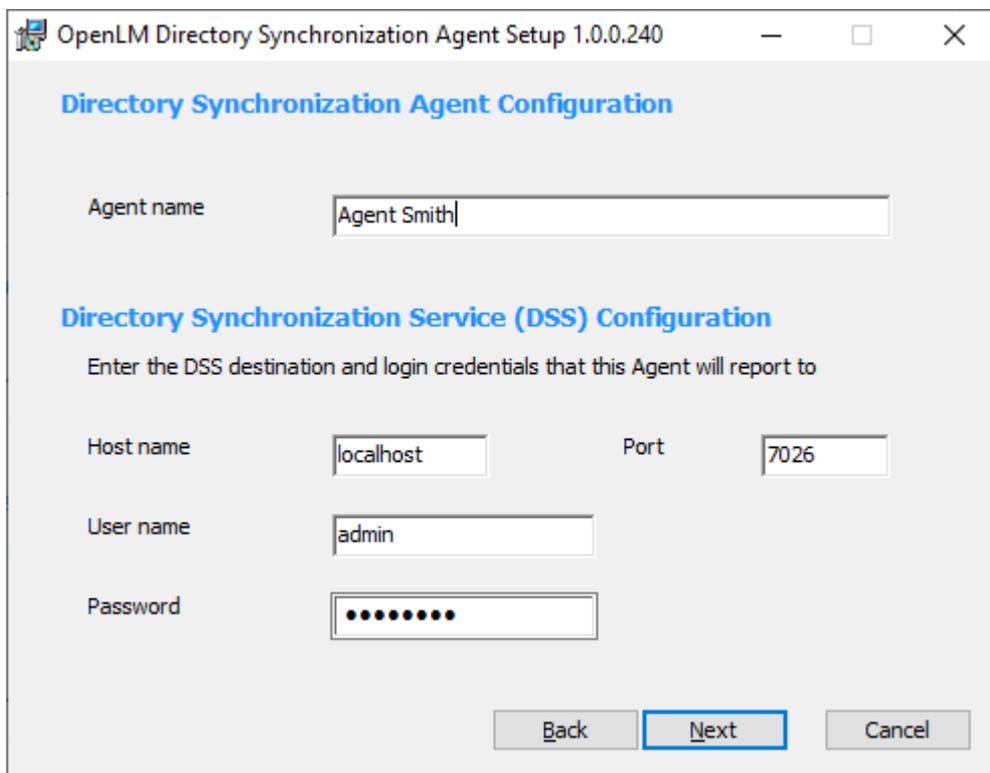
1. [ダウンロードページ](#)から最新のDSAをダウンロードしてください。インストーラーをダブルクリックしてください。





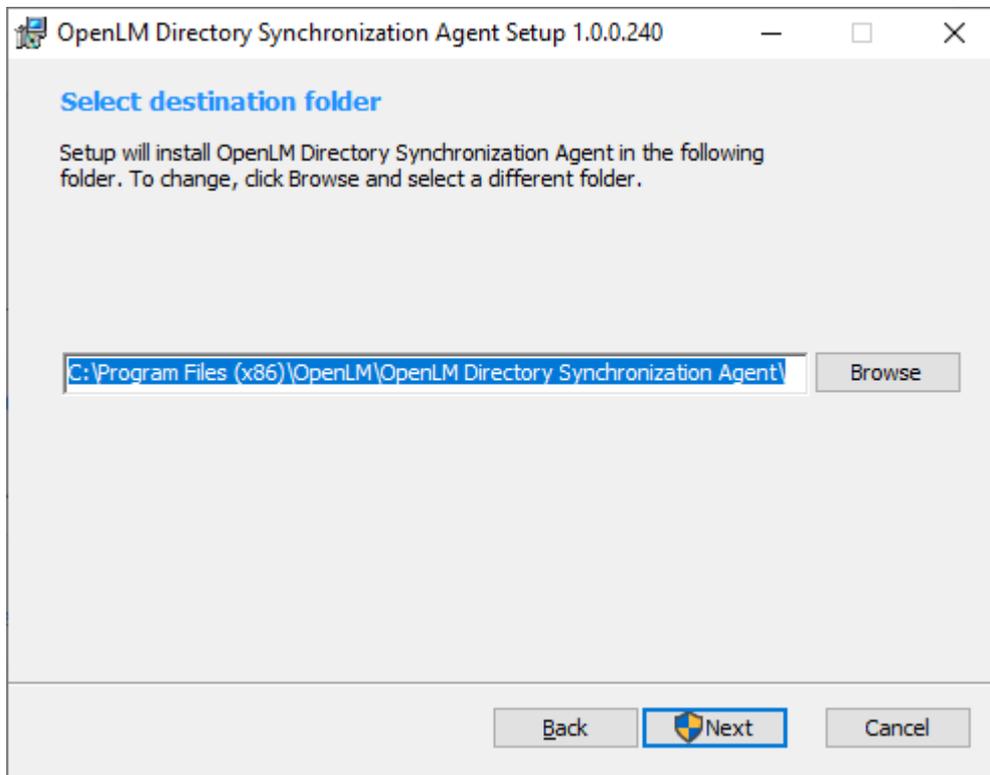
2. “I agree to the license terms and conditions”（利用規約に同意する）ボックスをチェックして **Next（次へ）** をクリック。

3. Agentインスタンスの名前を決めて、DSSインストールの詳細を入力してください。（**DSS UI → DSSサーバー下のService Configurationタブ** 参照） **Next（次へ）** をクリック。

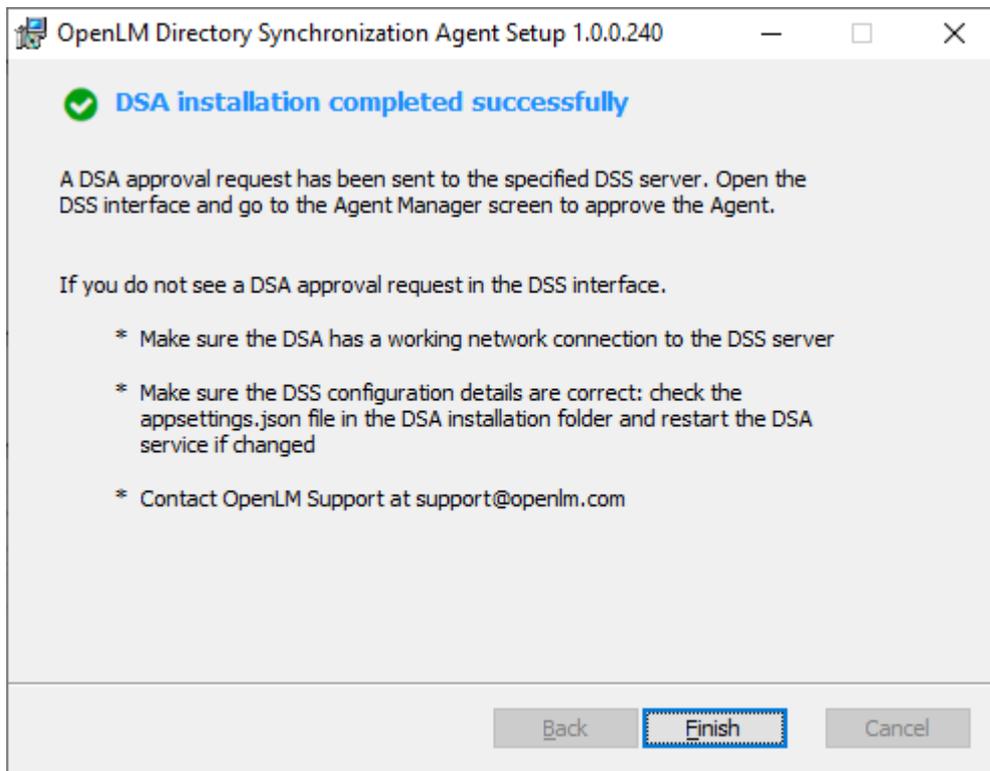


4. インストールフォルダーを変更できます。パスを入力するかBrowseで検索してください。完了したら **Next（次へ）** をクリック。





5. セットアップが完了したら、**Finish (終了)** をクリック。この時点でDSA承認要求がDSSに送られます。セクション5.1.1で説明されている通り、DSSのブラウザを開き、Agent Manager(エージェントマネジャー)タブで承認する必要があります。



4. 設定

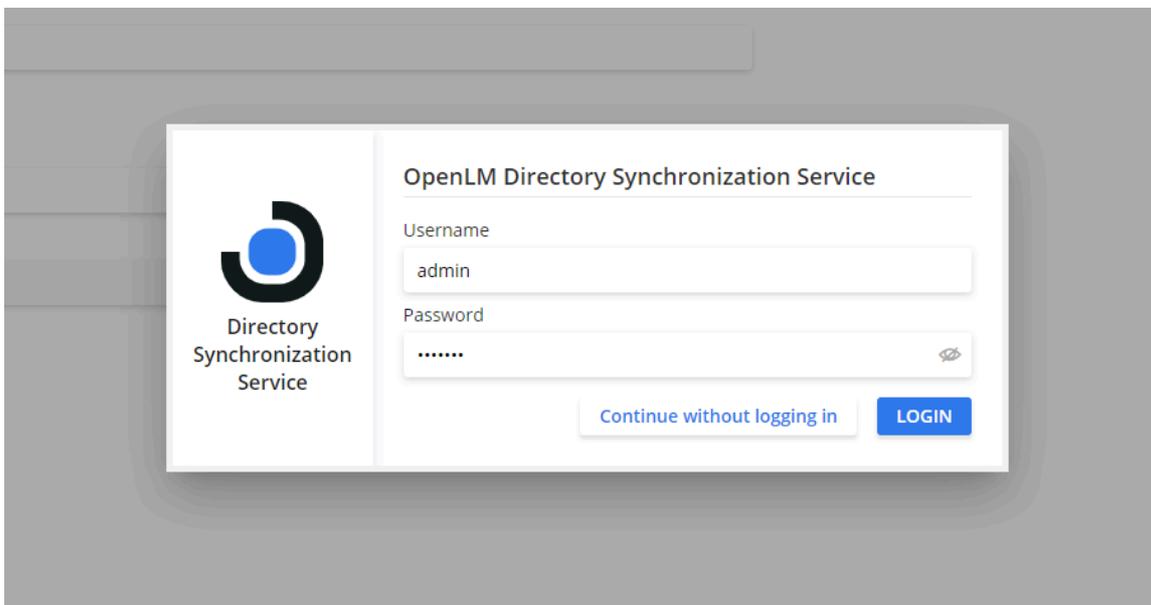
4.1. Directory Synchronization Service (DSS)



DSSを操作する前に、設定を終えなければなりません。設定は次の通りです。

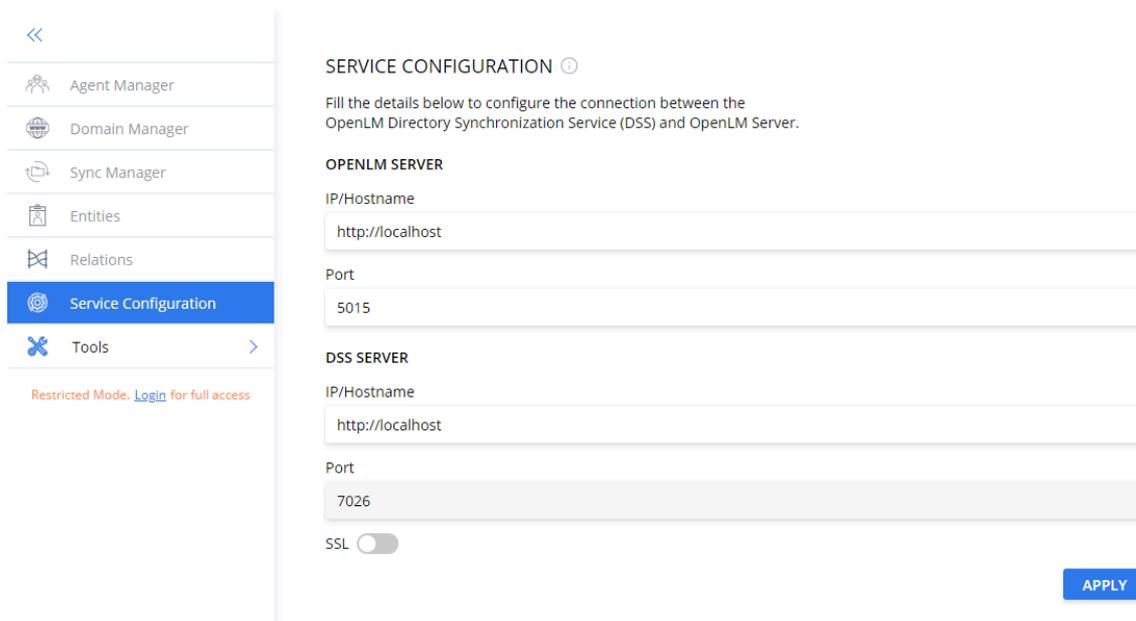
1. DSSのユーザーインターフェイスを開く。DSSインストーラーでFinish（終了）をクリックすると自動的に開く場合と、**Windows Start（開始） → OpenLM → OpenLM Directory Synchronization Service（DSS）**

2. **ログイン認証**を入力し、Loginをクリック。それか、**Continue without logging in（ログインなしに継続）**をクリックし制限モードでブラウザUIを開く。DSS設定に要求されるタブにはアクセスできる。



3. 左のメニューでは、**Service Configurationサービス設定**タブをクリック。

4. 次の通り詳細を入力



イラストレーション: 同じマシンにインストールされたOpenLM ServerとDSSのデフォルト設定

OpenLM Server:

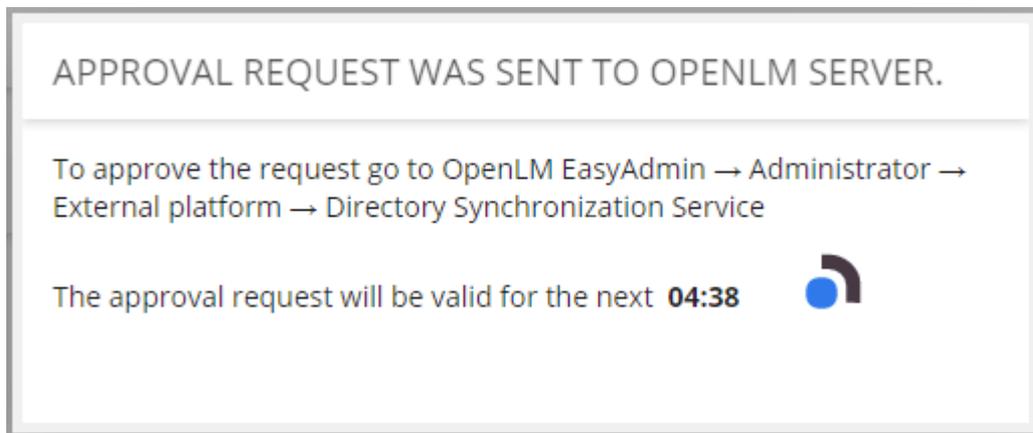


- **IP/Hostname** – DSSが接続しデータを送るOpenLM ServerマシンのURL。OpenLM ServerがHTTPS/SSLを使用する場合、ここでのホスト名がSSL証明書と正確に同じであることを必ず確認する。
- **Port** – OpenLM ServerのAPIポート (デフォルト: 5015)

DSS Server

- **IP/Hostname** – OpenLM ServerマシンにリポートされるDSSサーバーのURL。SSLを使用する場合、ホスト名が正確に証明書ファイルと同じであることを必ず確認する。
- **Port** – DSSのUIで使われるポート(デフォルト: 7026). デフォルトで、このフィールドはRead-only (リードオンリー) です。変更するには、**kestrel.config**ファイルを編集する。
- **SSL** – DSS通信ポートにHTTPSが有効か無効かチェックする。有効の場合、**SSL証明書ファイル(pfx)** とSSL証明書用**パスワード**を指定しなければならない。DSA接続設定はDSAインストールフォルダーの**OpenLM.Ldap.Agent.config** ファイルを編集して調整しなければならない。

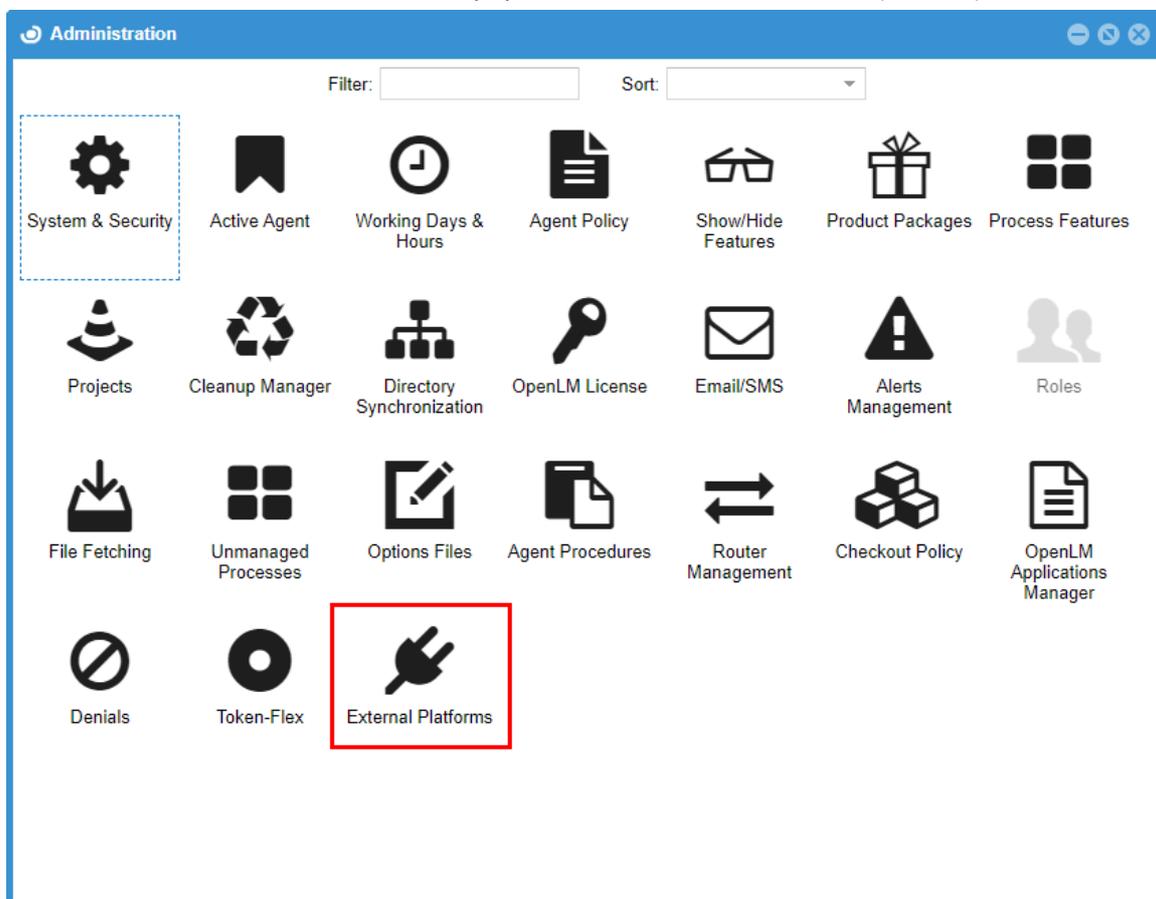
5. 設定を決定するよう**Apply (適用)** をクリック。接続リクエストがOpenLM Serverに送られる。



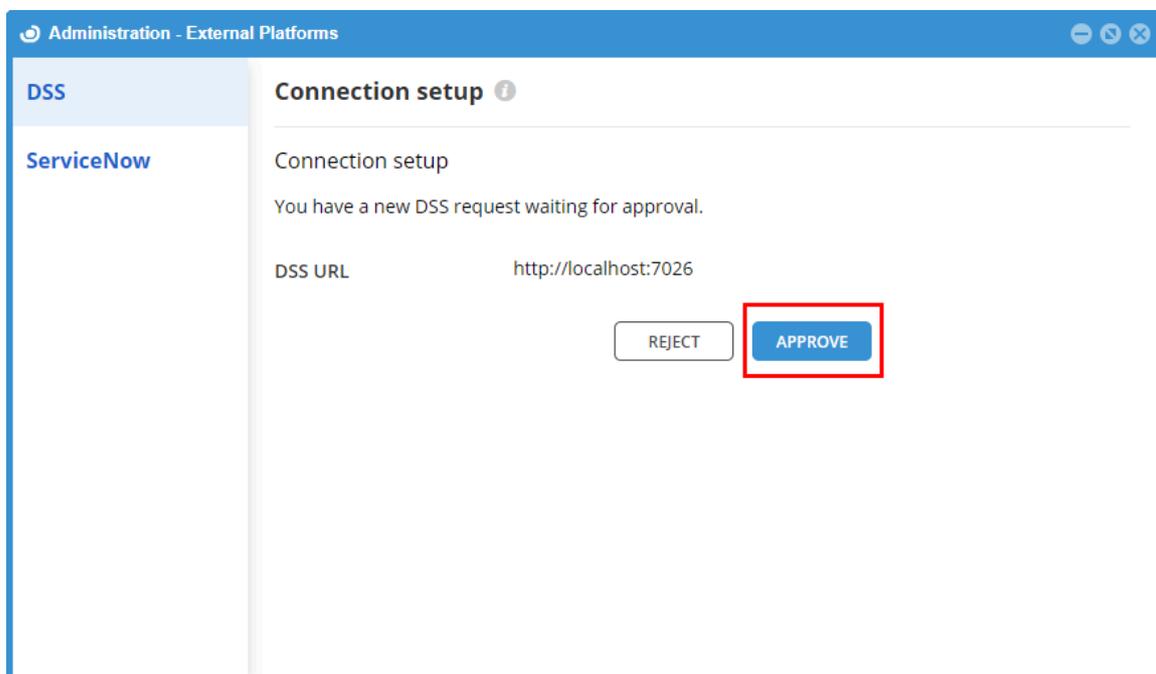
6. EasyAdminを開く (Windows Start (開始) → OpenLM → OpenLM EasyAdminユーザーインターフェイス)

7. **EasyAdmin Start (開始) → Administration (管理) 。 External Platforms (外部プラットフォーム)** をクリック。





8. 左のDSSタブをクリックし**Approve (承認)** をクリック。



9. DSSへの接続が成功したら、成功のメッセージを受け取る。

その時点で、OpenLM ServerとDSSの接続は確立された。

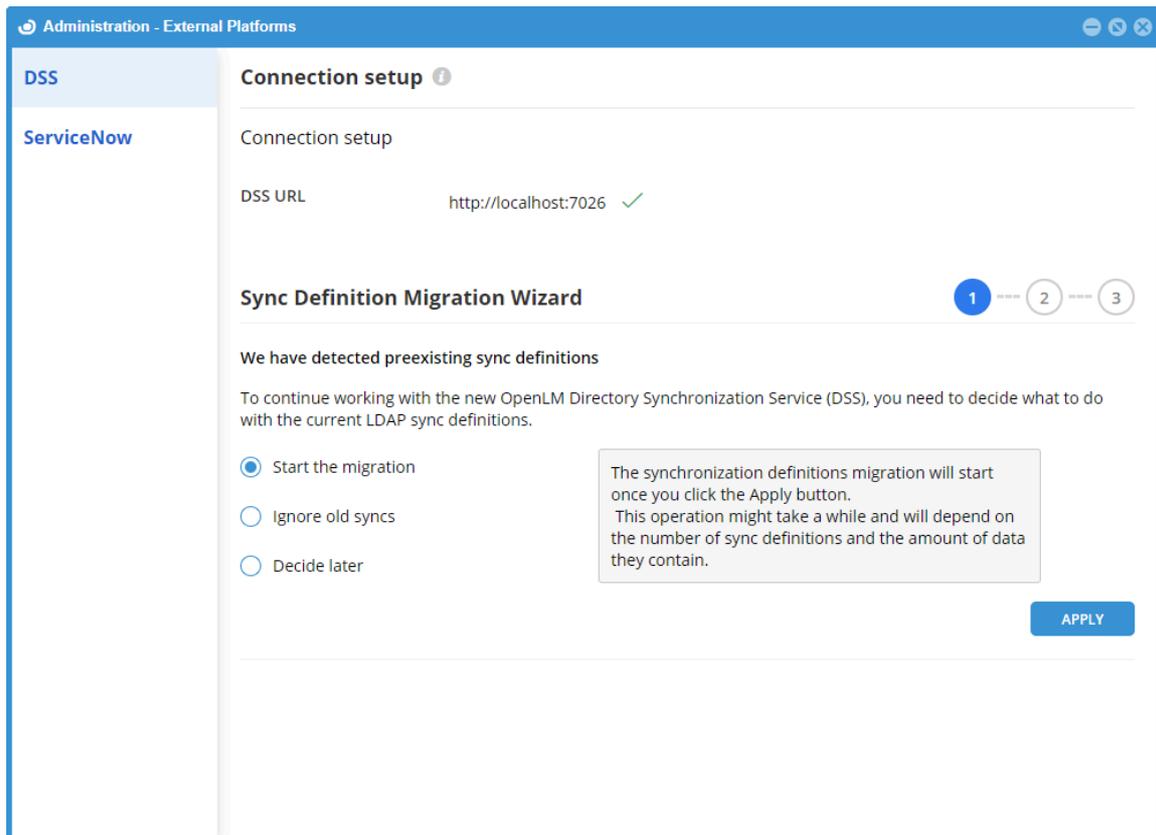
- a) 以前のLDAP同期の定義がある場合、新しいドメインや新しい同期定義を追加設定する前に、どうするか決めなければならない。続けるには下記セクション4.2を参照してください。



b) 以前のLDAP同期定義が無い場合、設定はこれで完了しました。セクション5で説明されるドメインと同期定義の追加を開始する前に、DSAインスタンスを少なくとも1つ追加しなければならない。

4.2. OpenLM Serverバージョン4 LDAP同期定義の移行

バージョン5以前のOpenLM Serverバージョン既存のLDAP同期定義は、DSSとDSAコンポーネントがインストールされた後、移行ができます。マイグレーションウィザードは前のセクションでステップを実行するとDSSの最初の設定で自動的に現れます。

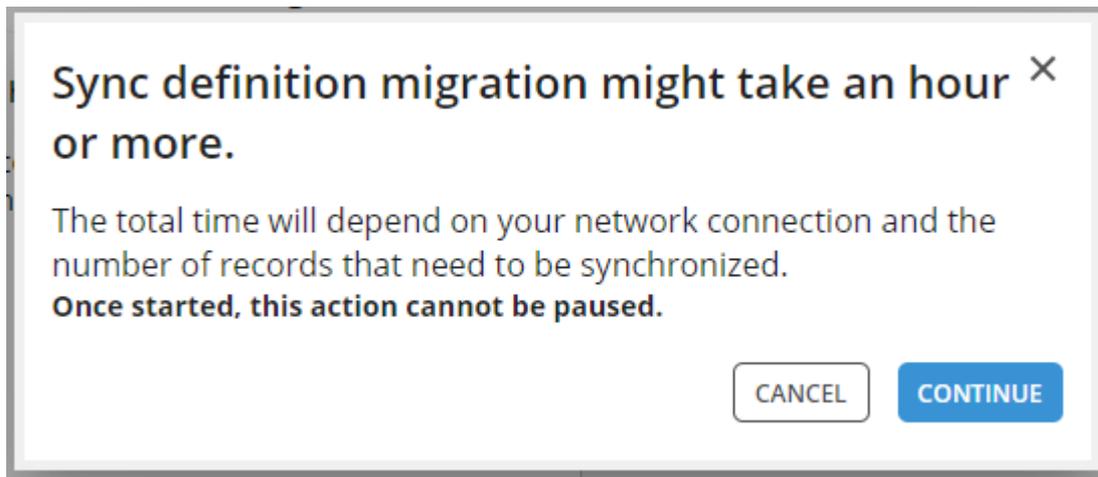


この時点で、3つのオプションから1つのラジオボタンをクリックできます。

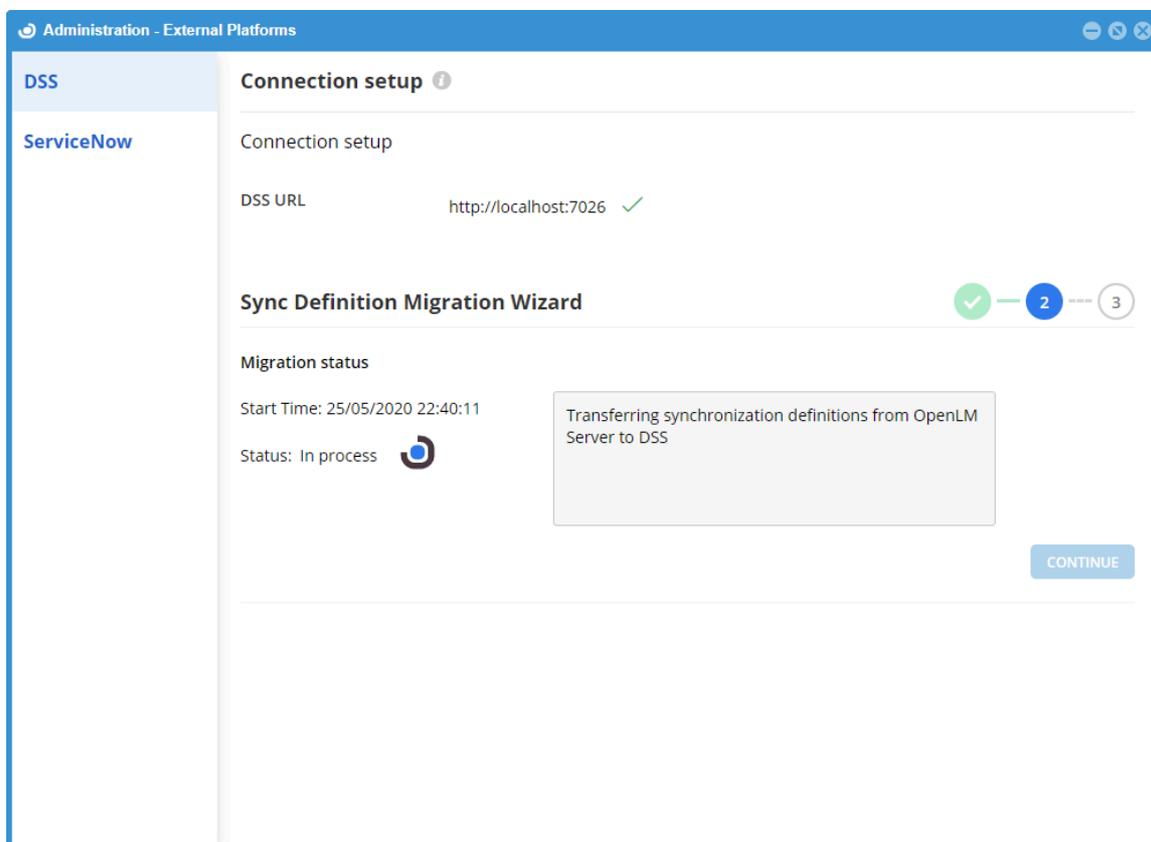
- 1. Start the migration (移行を開始する) – Apply (適用)** すると既存のLDAP同期定義は新しいDSSに移行される。この作業はしばらく時間がかかります。同期定義の数や中のデータ量によって変わってきます。
- 2. Ignore old syncs (古い同期を無視する)** – 既存LDAP同期定義は無視されます。DSSのUIで最初から新しい同期定義を作成できるのみです。このオプションが一旦選択されると、マイグレーションウィザードは閉じて、古いLDAP同期定義のインポートはOpenLMの援助なしには不可能になります。
- 3. Decide later (後で決める)** – このオプションは一時的にSkip (スキップ) ボタンとして動作します。DSS UIは使用できますが、この画面で上記2つの選択のいずれかを選択して作業を終了していないと、新しい同期を作成したり、新しいドメインを追加できません。



1か2を選択すると、作業を知らせる最終のポップアップ画面が現れます。

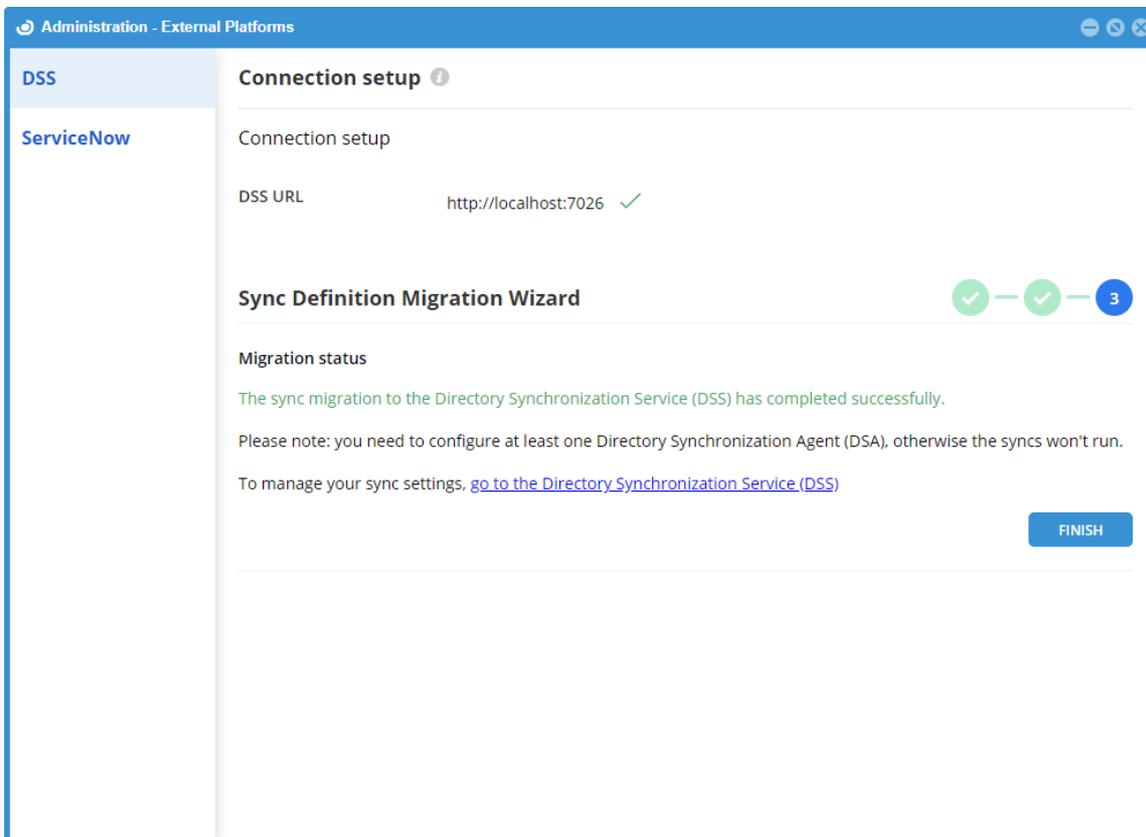


マイグレーションが開始されると、ステータスが見れます。



ウィザードが完了すると、成功メッセージが見れます。





最終ステップはエージェントをインポートした同期定義に割り当てることです。

1. DSSユーザーインターフェイスを開く
2. **Sync Manager (同期マネジャー) を開く**
3. インポートされた同期の行にマウスを運び、右端のペンのアイコンをクリック。
4. ドロップダウンリストからエージェントを選択
5. **Save (保存) をクリック。**

複数の定義を一括で割り当てるには：

1. エージェントに割り当てたい各定義ボックスをチェックする
2. **バルク編集**をクリック
3. ドロップダウンリストからエージェントを選択
4. **Save (保存) をクリックし、確認画面でYes (はい) をクリック。**

この時点でマイグレーション（移行）は完了です。下記セクション5で説明されている通り、DSSユーザーインターフェイスを開き、ドメイン、同期定義を追加し、エージェントを管理する。

4.3. DSS設定ツール

DB設定



DSSがどのデータベースにデータを保存するか設定します。

デフォルトでは、DSSは内蔵されたFirebirdデータベースで動くように設定されています。MySQLやSQL Serverも使用できます。

DB CONFIGURATION ⓘ

DB provider

Firebird

Database file location

Enter database file location

Username

sysdba

Password

.....

Embedded

CANCEL

TEST

APPLY

DB provider (データベースプロバイダ) - データベースのプロバイダを選択してください。標準の認証かWindows認証を持つFirebird、MySQL、Microsoft SQL Server

Server name (サーバー名) - (MySQLかSQL Serverのみ) 外部データベースサーバーのIPかホスト名

Port (ポート) - (MySQLかSQL Serverのみ) データベースのリスニングポート

Database file location (データベースファイルの場所) - (Firebirdのみ) データベースファイルへのパス

DB Name - (MySQLかSQLサーバーのみ) データベース名

Username - データベースユーザーの名前

Password - データベースユーザー用パスワード

Embedded - (Firebirdのみ) デフォルトでチェックされています。分離したFirebirdデータベースを使用する場合はチェックをはずしてください。

Test - データベースへの接続をテストするためにクリックしてください。

Apply (適用) - 設定を保存する

DB Upgrade (DBアップグレード)



このツールはDSSデータベースを最新のデータベーススキーマにアップグレードします。この操作は、DSSスキーマにフォーマットされていない以前の新しく作成されたデータベースを使用する場合に必要です。

データベースをアップグレードするには、データベースタイプを選択し、DB設定タブでログインと接続詳細を入力し、アップグレードをクリックしてウィザードの指示に従ってください。

5. Usage (使用)

5.1. Agent Manager

Agent Managerタブでは、DSSに制御された全てのDSAを見ることができます。

5.1.1. 新規エージェントを承認

DSSにレポートするように設定され新規でインストールされたDSAの全ては、操作をする前に承認されなければなりません。

実行するには:

1. **Agent Manager** タブをクリックしてください
2. Pending approval (承認保留中) ステータスのエージェントの行にマウスを運び、右端

の編集アイコン  をクリックする

Agent name	Description	Status	Alerts	Domains	Syncs	
Agent Smith		Pending Approval	true	0	0	

Start from: type here... < 1-1 of 1 > Show up to: 25 ^

3. エージェント承認画面で、ステータスドロップダウンメニューを開き、**Enabled (有効)** を選択し**Approve (承認)** をクリック。

5.1.2. エージェントプロパティの編集

1. 変更したいエージェント行にマウスを運び、右端の編集アイコン  をクリックする。

2. 要望するフィールドを変更する。各値の意味を下記テキストで理解してください。



← EDIT AGENT ⓘ Agent ID: 3

Agent name

Description 0/200

Status
 ▼

Advanced Settings —

Agent Request Interval
 sec

Sync method
 Parallel Serial

Agent name (エージェント名) - エージェント名。単独名でなければなりません。
(例：他の既存エージェント名と異なる名前)

Description (optional) (説明：オプション) - エージェントを特定したり思い出したりするテキストを入力してください

Status (ステータス) - 次のいずれかに設定する

- Enabled (有効) - エージェント操作可能。同期ジョブのためDSSにクエリ問い合わせし実行。
- Suspended (一時停止) - エージェントで実行される全同期が一時停止となります。ステータスが有効になると、再開します。

Agent request interval (エージェントへのリクエストインターバル) - エージェントが同期ジョブをチェックするためにDSSをクエリする頻度を指定します。5~600秒の間どの値でもかまいません。

Sync method (同期方法) - 次のいずれかに設定できます。

- Parallel (平行) - このモードはエージェントが並行して複数の同期を同時に実行する事を意味します。
- Serial mode (シリアルモード) - FIFO (First最初がINし最初がOUTする) 方法に基づき、一つずつ同期が実行されます。

3. 完了したら**Save (保存)** をクリック

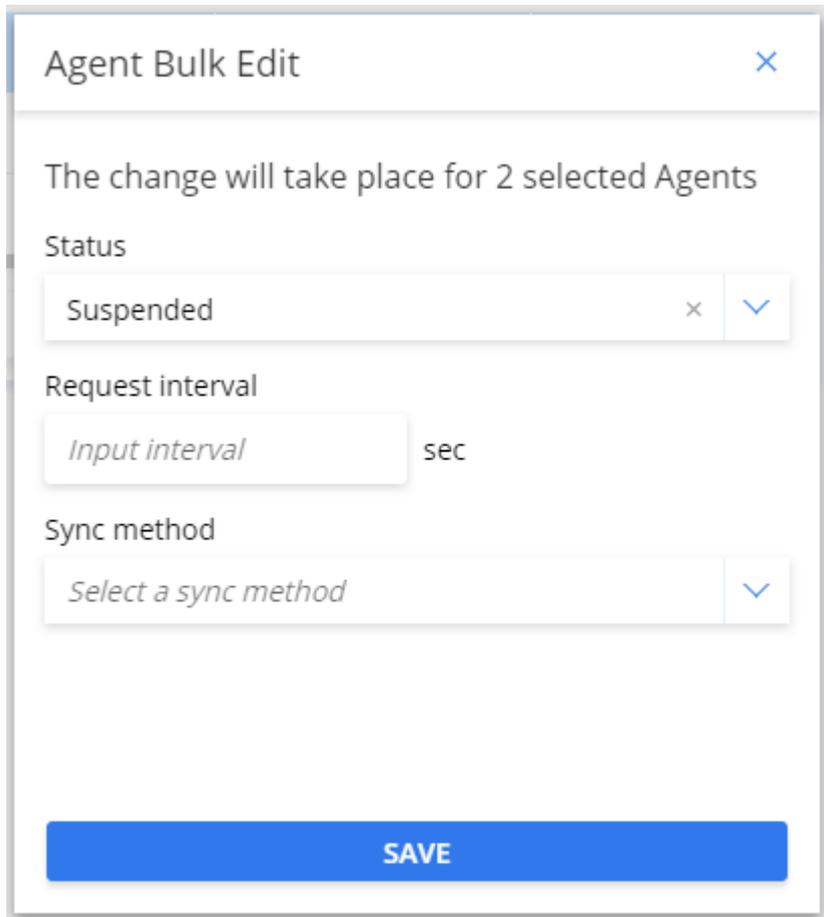


5.1.3. 一括エージェントプロパティ編集

一度に複数のエージェントのプロパティを変更:

1. 編集したい各エージェントのチェックボックスをチェックする
2. **Bulk Edit (一括編集)** をクリック

一括エディターを開きます。



Agent Bulk Edit

The change will take place for 2 selected Agents

Status

Suspended

Request interval

Input interval sec

Sync method

Select a sync method

SAVE

利用可能なプロパティは上記セクション5.1.2で説明されているのと同じです。

3. 完了したら、変更を適用するため、**Save (保存)** をクリック

5.1.4. エージェントの削除

1つ以上のエージェントを削除するには、削除したいエージェントのチェックボックスをチェックし、**Delete (削除)** をクリックする。

注意: 1つ以上の同期がエージェントに割り当てられた場合、削除する前に代理エージェントを選択するように促されます。



DELETE AGENT ×

Are you sure you want to delete the following Agent ?

One or more Agents have syncs associated with them.

Agent Name	Syncs
Agent Smith	3

To delete the Agent, assign the syncs to another Directory Synchronization Agent

Select the Agent you want to assign the syncs to. ▼

CANCEL DELETE

5.2. Domain Manager

Domain ManagerタブではOpenLMが同期するドメインディレクトリを設定できます。

5.2.1. 新規の同期ドメイン追加

1. **Add Domain (ドメイン追加)** を選択。ドメイン追加画面が開きます。下記指示に従い、フィールドを設定してください。



← ADD DOMAIN ⓘ

Directory type
Active Directory

Domain Name
server2008r2ldap.openlm.biz

Port
389

SSL

Username
Administrator

Password
.....

CHECK DOMAIN CONNECTIVITY

CANCEL SAVE SAVE DOMAIN & ADD SYNC

Domain type (ドメインタイプ) - 同期したいLDAPドメインディレクトリのタイプ。現在次のいずれかを選択できます。

- Active Directory
- eDirectory
- ApacheDS

Domain name (ドメイン名) - ドメインコントローラのホスト名/IP

Port (ポート) - ドメインコントローラのポート

SSL - ドメインコントローラへの接続がSSLで暗号化されている場合チェック

Username (ユーザー名) - ドメインコントローラユーザーのユーザー名

Password (パスワード) - ドメインコントローラユーザーのパスワード

2. **Check domain connectivity (ドメインへの接続をチェック)** をクリックしてTESTを実行します。接続テストを実行するエージェントを選択するように促されます。作業自体は最大2分かかります。完了したら、ボタンの下に成功か失敗かのメッセージが出ます。

3. ドメイン設定を保存する**Save (保存)** をクリックするか、設定を保存しこのドメインが選択されたままで**Add Sync (同期追加)** 画面を開くには、**Save Domain & Add Sync (ドメイン保存&同期追加)** をクリックします。



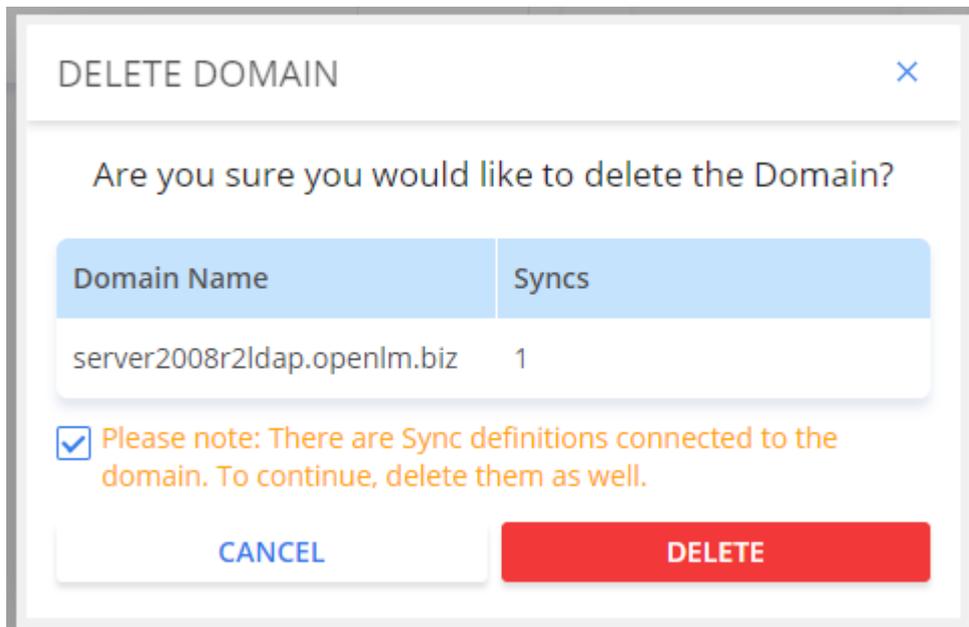
5.2.2. ドメインのプロパティ編集

1. 変更したいドメインの行にマウスを運び、右端の**編集アイコン**  をクリック。
2. 変えたいフィールドを変更する。各フィールドの意味は上記セクション5.1.1で説明されています。
3. 完了したら**Save (保存)** をクリック。

5.2.3. ドメインを削除

1つ以上のドメインを削除するには、削除したいドメインの箱をチェックし**Delete (削除)** をクリック。

最終確認画面がポップアップします。



注意: ドメインと結びついた同期定義がある場合、同期定義も削除されます。このチェックボックスをチェックしないと先には進みません。

5.3. Sync Manager (同期マネジャー)

Sync ManagerタブでOpenLMが同期するドメインの同期定義を設定できます。

5.3.1. 新規同期定義を追加



新しい同期定義を追加するには：

1. **Add Sync（同期追加）** をクリック。
2. 次の通りにフィールドを入力：

← ADD SYNC ○

Sync name
New Demo Sync1 Status

Destination & Time ○ Object Group & Rules

Agent
Agent Smith Domain name
server2008r2ldap.openlm.biz

Start Node
LDAP://server2008r2ldap.openlm.biz TEST ○

Sync Schedule
 By Time By Interval ○
To configure a sync, select the day and time then click Add.

Days Start Time
Select sync day hh:mm ADD

Day	Start Time
-----	------------

Sync time has not been configured

CANCEL NEXT

Sync name（同期名） – 同期定義を特定するテキストを入力。単独名でなければなりません。(例：他の同期定義名と異なる事)

Status（ステータス） – 同期が有効か無効かチェック

Destination & Timeタブ

Agent（エージェント） – この同期を実行するエージェントを選択

Domain name（ドメイン名） – 同期されるドメインを選択。ドロップダウンリストはDomain Managerタブのドメインがリストされます。

Start node（開始ノード） – この同期が開始するノードへのLDAPパスを入力。大きいサービスディレクトリにおいては、ツリーのノードを指定する事で、検索を狭めパフォーマンスを向上します。デフォルトでこの値は、選択されたドメインディレクトリのルートに対応するように自動的に入力されます。ディレクトリのスタートノード



を検証するには**Test (テスト)** をクリックします。2分ほどかかります。LDAP接続文字列が正しいフォーマットである事を必ず確認してください。

例 #1: ドメインコントローラー10.0.0.153でドメイン“testdev1domain.openlm.biz”の組織単位“OU_AB”を選択

```
LDAP://10.0.0.153/OU=OU_AB,DC=testdev1domain,DC=openlm,DC=biz
```

例 #2 ドメインコントローラーserver2008r2ldap.openlm.bizでドメイン“openlm.com”の“SecGroup”セキュリティグループを選択

```
LDAP://server2008r2ldap.openlm.biz/CN=SecGroup,DC=openlm,DC=com
```

例 #3: “testdev1domain.openlm.biz” ドメインで順に組織単位“OU_AB”、“OU_A”の下“Group_AB1”グループを選択

```
LDAP://10.0.0.153/CN=Group_A2,OU=OU_A,OU=OU_AB,DC=testdev1domain
```

正しいノードパスを見つけるには、[LDAP Adminツール](#)の使用をお勧めします。ノードツリーを右クリックし、“Copy dn to clipboard”（クリップボードにdnディレクトリノード?をコピー）を選択。

Sync schedule (同期スケジュール) - 同期がいつ実行されるかスケジュールを定義する

- **By time (時間単位)** - 同期の日と開始時間を選択しAdd (追加) をクリックしてスケジュールに追加する。複数の時間が追加可能。
- **By interval (インターバル単位)** - 開始時間(hh:mmフォーマット)を入力し、同期が繰り返されるインターバル(無稼働期間)を入力する。(1~720時間までのいずれかの値) DSSが再開されると、同期を引き起こす開始時間まで待ちます。

Object (対象物) タブ

Sync object type (同期オブジェクトタイプ) - 同期するオブジェクトタイプを選択。

- **Users (ユーザー)** - ユーザーオブジェクトのみ同期されます。 **Only users monitored by OpenLM (OpenLMに監視されてるユーザーのみ)** ボックスを選択できます。(下記説明参照)



- **Computers (コンピューター)** - コンピューターオブジェクトのみ同期されます。

Only users monitored by OpenLM (OpenLMに監視されてるユーザーのみ)

同期を実行する時このボックスがチェックされていると、OpenLMのユーザー名と合致するディレクトリユーザーのデータのみインポートされ同期されます。このオプションはOpenLMシステムで関連するライセンス活動の履歴データのないディレクトリユーザーを追加したくない時に便利です。

Sync attribute (同期属性) - 同期するディレクトリ属性を選択するか入力する。特定のディレクトリタイプでその属性が存在するか必ず確認してください。“Sync attribute” (同期属性) はユーザーオブジェクトタイプでのみサポートされています。次から選択してください:

- **cn** はLDAPディレクトリで使用される標準の“Common Name” (共通名) 属性です。
- **sAMAccountName** (例: “jdoe”) はWindows Server 2000より前のアクティブディレクトリのバージョンで使用されます。
- **userPrincipalName** (例: “john.doe@company.com”) はWindows Server 2000以降のアクティブディレクトリのバージョンで使用されます。

Membership filter (メンバーシップフィルター) - 全てのオブジェクト (フィルター無) を同期するか、組織ユニット (OU) かセキュリティグループに属するオブジェクトのみ同期するかを選択。

Search depth (検索深度) - 同期深度を定義します。このオプションは特定の階層レベルに同期プロセスを限定する事ができます。

- **0** (デフォルト) - 完全にツリーグループ階層が同期されます。
- **1** - 開始ノードグループのみ同期されます。
- **2** - 開始ノードグループとその第1子達のみ同期されます。
- **3** - 開始ノードとその第2子孫達までのみ同期されます。
- これ以降同じパターンです。

グループのルールタブ

どのグループが作成されるか規則を選択します。



No groups (グループなし) - グループの同期でデフォルトの選択です。このオプションはオブジェクトが属するどのグループも無視します。全てのオブジェクトはシステムデフォルトの**OpenLM_Everyone**グループに割り当てられます。

Flat (平坦) - 全てのオブジェクトはアドミニストレーターに定義されるグループのメンバーとなります。同期ツリーで見つかる全てのオブジェクトはこの単一グループのメンバーに割り当てられます。どの階層構造も無視されます。

Hierarchical (階層) - 階層LDAPノードツリーに従ってグループが作成されます。このルールで含むオブジェクトクラスの種類を選択できます。

- **Organizational Units 組織単位(OUs)** - ディレクトリの既存組織単位が持つグループからは同じ名前で作成され、その中に属するオブジェクトはそれらのグループのメンバーとして割り当てられます。
- **Security Groups (セキュリティグループ)** - ディレクトリの既存セキュリティグループが持つグループは同じ名前で作成され、その中に属するオブジェクトはそれらのグループのメンバーとして割り当てられます。
- **Distribution groups (配布グループ)** - ディレクトリの既存配布グループが持つグループは同じ名前で作成され、その中に属するオブジェクトはそれらのグループのメンバーとして割り当てられます。
- **Customized & Unknown Object Classes (カスタマイズか未知オブジェクトクラス)** - 未知かカスタムされたオブジェクト(OU、Security GroupやDGの標準ディレクトリクラスタイプ外の物) が持つグループは同じ名前で作成され、その中に属するオブジェクトはそれらのグループのメンバーとして割り当てられます。

Include start node(開始ノードを含む) - 同期に開始ノードを含めるか否か。

Search depth (検索深度) - 同期深度を定義します。このオプションは特定の階層レベルに同期プロセスを限定する事ができます。

- **0 (デフォルト)** - 完全にツリーグループ階層が同期されます。
- **1** - 開始ノードグループのみ同期されます。
- **2** - 開始ノードグループとその第1子達のみ同期されます。
- **3** - 開始ノードとその第2子孫達までのみ同期されます。
- これ以降同じパターンです。



Select a rule to create a group

Hierarchical



Select the object classes you would like the groups to be created by

Security groups

OU

Distribution groups

Customized & Unknown Object Classes

Include start node

Search Depth

0



Entity attribute (エンティティ属性) - メンバーがもつ特定の属性に従ってグループが作成されます。入力するか、同期したい属性をドロップダウンメニューから選択してください。(例：“Division”, “Employee ID”, “Initials”, “Department”等)。各単独属性で、新しいOpenLMグループが作成されます。ユーザーやコンピューターが同じ属性を持つ場合、各グループに追加されます。

Regular expression to specify the sub-level of the selected attribute 選択された属性の準レベルを指定する通常表現 (オプション) - 通常表現に合致する属性で同期を可能にします。例：“Country”属性が選択され、“USA”を入力すると、“Country”属性が“USA”に設定された物のみ同期される。

Set as default group デフォルトグループとして設定 チェックボックス

リポート目的で、デフォルトグループはユーザーのライセンス使用時間が数えられる目的のグループとして考えられます。デフォルトで、手動や同期に関わらず全ての作成されたユーザーはシステムデフォルトのOpenLM_Everyoneグループに割り当てられます。このボックスをチェックすると、このデフォルト設定を上書きします。

- **FlatとEntity Attribute** (平坦とエンティティ属性) 同期ルールの場合、デフォルトグループは入力したかメニューで選択したものとなります。
- **Hierarchical (階層)** 同期ルールの場合、デフォルトグループは検索中に見つかった最初のものになります。(例；JohnDoeが順にグループ A、B、Cに属する場合、デフォルトグループはA)



“Set as default group”がチェックされている場合、オブジェクトのデフォルトグループは同期が実行されるたびに設定され書き換えられます。

5.3.2. 手動で同期を起動させる

1つ以上の同期定義が選択された状態で、 アイコンをクリックすると、各同期の実行がこのように手動で動作します。

作動した後、進捗を示すアニメアイコンが表示されます。アイコンにマウスを運ぶと同期動作の進捗ステータスが表示されます。

Status	Domain
Enabled	server2008r2ldap
Enabled	Processing Data
Enabled	10.0.0.179

5.3.3. エンティティ・リレーションシップ・データのリセット

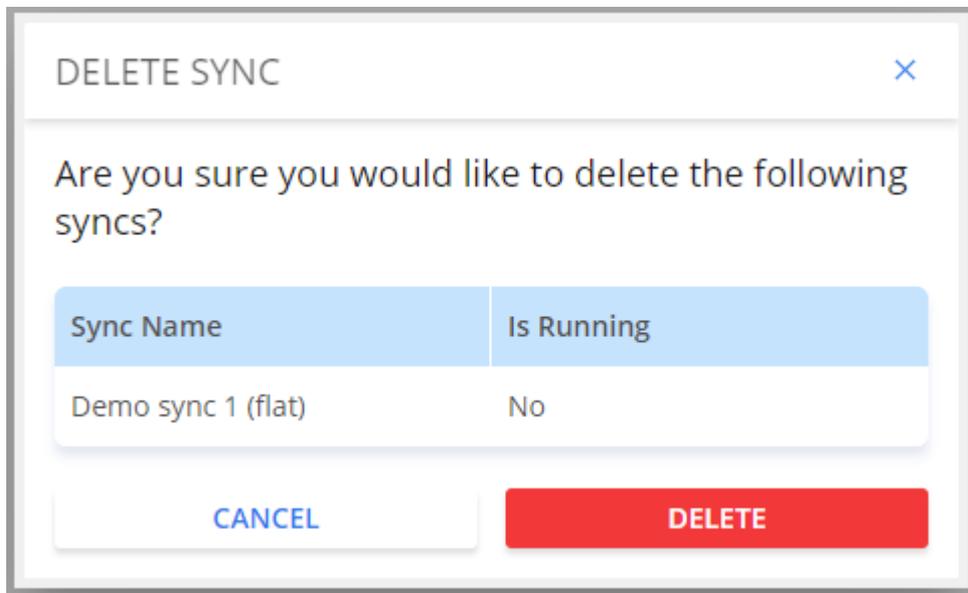
1つ以上の同期定義が選択された状態で  アイコンをクリックすると、同期定義で生成された全てのリレーションシップデータはクリアされます。以前設定されたかもしれない“ignore”(無視する)フラグ (5.4.1参照) も含まれます。実際のユーザーデータには影響はありません。

5.3.4. 同期定義の削除

1つ以上の同期定義を削除するには、削除したい定義ボックスをチェックし **Delete (削除)** をクリックします。

実際に削除する前に最終確認画面がポップアップします。





注意: 同期が実行されている場合、削除はできません。

5.4. エンティティ

Entitiesタブで、DSS同期で作成されたエンティティを見ることができ、各々にignore（無視）フラグを設定します。列はDSSデータベースにエンティティが持つIDを表示し、定義が最後に同期したエンティティタイプ、最後同期の日時などを表示します。どの同期でどのエンティティが修正されたか見るにはフィルターを使用するか、特定のエンティティを検索してください。

5.4.1. 全ての同期でエンティティを無視する

特定のエンティティの**Ignore（無視）** ボックスをチェックし、**Save（保存）** をクリックすると、全ての同期定義でそのエンティティを無視します。ディレクトリデータで起きるかもしれない更新は、そのエンティティに関してはOpenLMデータベースに反映されません。

5.4.2. 手動でエンティティを同期する



アイコンをクリックすると特定のエンティティに手動で同期を動作させます。このオプションは以前設定されたかもしれない"ignore（無視）"フラグに関係なく作動します。

5.4.3. エンティティ・リレーションシップを見る

特定のエンティティで  アイコンをクリックすると、Relationsタブを開き、特定の工



ンティティが持つリレーションを表示します。

5.5. リレーション

Relationsタブで、DSSデータベースにエンティティが持つ全てのリレーションを見ることができます。このエンティティのディレクトリをクエリしたエージェント、エンティティが属するドメイン、関係する同期定義、エンティティ名、存在すればその親の名前、同期された最終日時など確認できます。フィルターを使用してどのリレーションがいつ更新されたかをご確認ください。

適切なタブにスイッチするリンクをクリックする事で、リンクされたアイテム（エージェント、ドメイン、同期、エンティティ）の詳細を表示できます。

5.5.1. 特定の同期でエンティティを無視する

特定のエンティティで**Ignore（無視）** ボックスをチェックし**Save（保存）** をクリックすると、“Sync Name”(同期名)で関連する同期でそのエンティティを無視します。この特定の同期定義において、ディレクトリデータで起きるかもしれない更新は、そのエンティティに関してはOpenLMデータベースには反映されません。

+81 (0)50 5893 6263

sales@openlm.com

