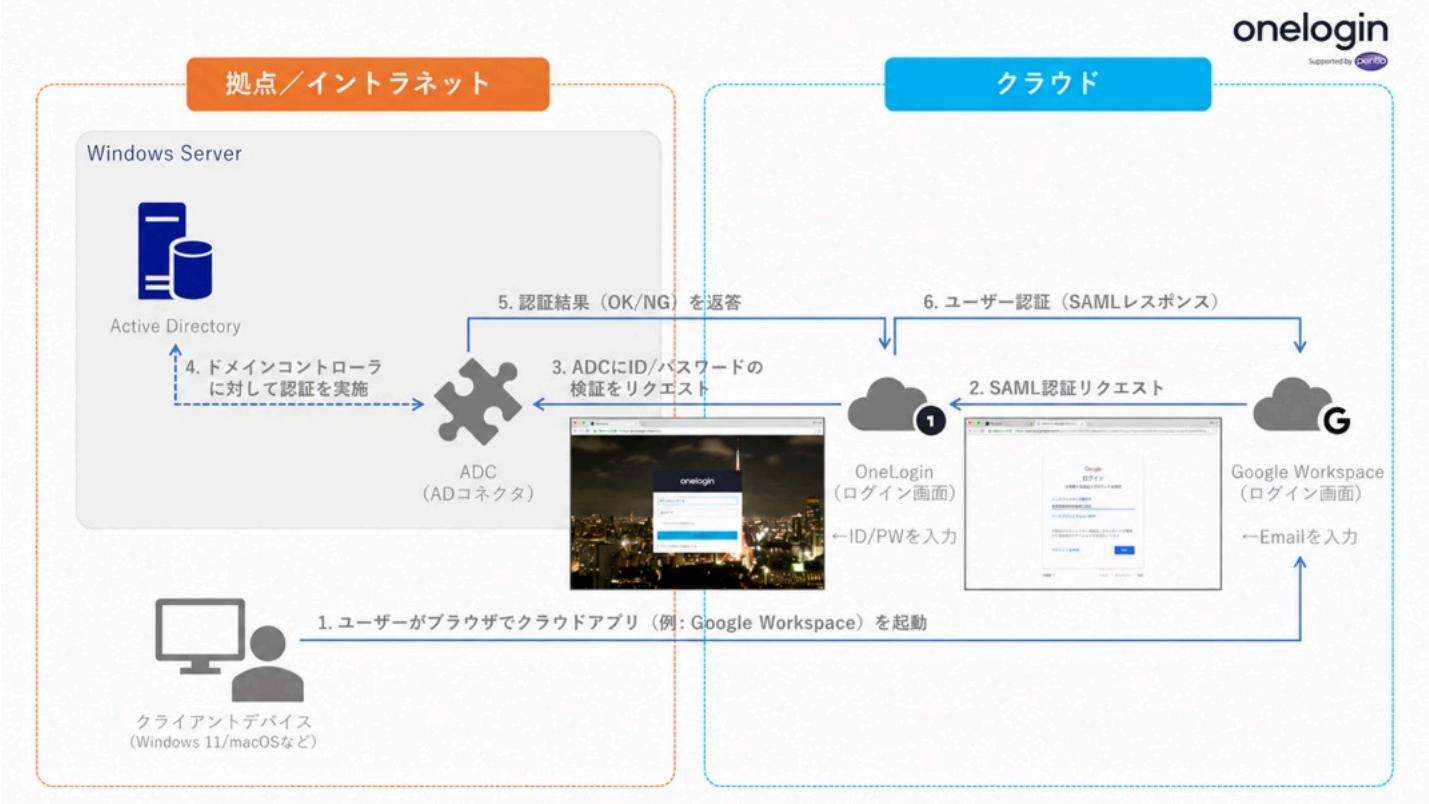
Active Directoryとディレクトリを統合する

長田 紘典
作成日 · 2018年4月23日 · 更新日 · 2026年11月17日



本記事では、OneLoginとActive DirectoryをOneLogin Active Directory Connectorを利用してディレクトリ連携し、ユーザー情報の同期とOneLoginのログイン認証をActive Directoryで実施するための設定について解説いたします。

本記事をオフライン閲覧する場合など、PDFファイルをご利用になる場合は以下のリンクをご活用ください。

- Active Directoryとディレクトリを統合する
- Active Directoryとディレクトリを統合する-システム要件抜粋版-

目次

- Windows Server 2025への対応状況
- 前提条件
- ご利用・ご設定の前に
  1. OneLogin Active Directory Connectorとは

    2. OneLogin Active Directory Connectorと連携できるWindows Serverについて
- ご利用上の注意
    1. マネージドADサービスご利用上の注意点
    2. その他の注意点
- OneLogin Active Directory Connectorシステム要件
- Active Directoryユーザー項目について
    1. 必須項目
    2. 標準同期項目
    3. 標準同期項目以外を同期する
- OneLoginにActive Directory連携を設定する
    1. OneLoginにディレクトリ連携設定を追加する
    2. OneLogin Active Directory ConnectorをWindows Serverにインストールする
    3. 同期対象OUを設定する
        a. OU内の全ユーザーを同期する
        b. OU内の特定のグループに所属するユーザーを同期する
- Connector Instancesタブの各項目について
- ディレクトリ連携のアドバンスド設定を行う
- 高度な設定について
- ユーザー同期間隔の変更
- OneLogin ADCアカウントの設定
    1. ユーザーの作成
    2. 作成したユーザーに権限を付与
- OneLogin Active Directory Connectorをメンバーサーバーにインストールする場合
- ドメイン名とドメイン識別名の確認
- トラブルシュート
    1. インストールにおけるトラブル
    2. ユーザー同期に関するトラブル

Windows Server 2025への対応状況

Windows Server 2025にはOneLogin Active Directory Connectorのバージョン7.0.2以上で対応しております。Windows Server 2025をご利用、もしくはリプレースを行うお客様は必ずバージョン7.0.2以上のOneLogin Active Directory Connectorをご利用ください。

前提条件

- OneLoginのライセンスプラン が **SSO**（1ディレクトリまで）, **Advanced**, **Professional** または旧ライセンスプラン **Starter**, **Enterprise**, **Unlimited** のいずれかであること
- OneLoginの **Super User** または **Account Owner** 権限を持つアカウントを所有していること

- OneLogin Active Directory Connectorをホストするサーバーの **Domain Admins** 権限を持つアカウントを所有していること
- **Active Directoryのドメインコントローラーの設定が完了し、正常に稼働していること**

ご利用・ご設定の前に

1. OneLogin Active Directory Connectorとは

OneLogin Active Directory Connector（以下、OneLogin ADC）とは、OneLoginとActive Directoryを接続して下記の機能を提供・実現するWindowsアプリケーションです。

1. **ユーザー情報のリアルタイム同期**
2. **Active Directoryの認証情報を用いたOneLoginへのログイン**
3. 統合Windows認証を用いたOneLoginへのSSO

本記事では **1. ユーザー情報のリアルタイム同期** および **2. Active Directoryの認証情報を用いたOneLoginへのログイン** の設定手順を解説いたします。統合Windows認証を用いたOneLoginへのSSOについては統合Windows認証を追加する：Windows Domain Authenticationインストールガイドをご覧ください。

2. OneLogin Active Directory Connectorと連携できるWindows Serverについて

OneLogin ADCのインストール先として、下記のWindows Serverを利用できます。必ずしもドメインコントローラーにインストールする必要はありません。

- Active Directory ドメインコントローラー
- Active Directory ドメインに参加したメンバーサーバー

ご利用上の注意

1. マネージドADサービスご利用上の注意点

- AWS Directoryが提供するManaged ADなど、マネージドADサービスとOneLoginを **直接的に** 連携することはできません。これはOneLogin ADCがWindows Serverにインストールして動作するプログラムであるため、プログラムをインストールするWindows Server環境が必須となるためです
- マネージドADサービスとOneLoginのディレクトリ連携をご希望される場合は、中継用のWindows Serverをご用意頂き、中継用サーバーがOneLogin ADCのシステム要件を満たすようにご設定ください
- マネージドADサービスにより、一部機能に制約が発生することがございます。これは本来OneLogin ADCはActive Directory ドメイン管理者権限を利用する必要があるサービスですが、マネージドADサ

ービスではお客様に完全なドメイン管理権限が付与されないケースがあるためです。事前にマネージドADサービス提供会社に対して、ドメイン管理権限が取得できるかをご確認ください。OneLoginが必要とする詳細な権限については、下記米国One Identityのサポート記事に記載しております
Create a Domain Service Account to run Active Directory Connector

2. その他の注意点

- Active Directoryのユーザー設定により、ユーザーがログインできるワークステーション制限を設定すると当該ユーザーはOneLoginにログインできません。OneLoginとの連携をご希望の場合には、必ずワークステーション制限は解除する必要があります

OneLogin Active Directory Connectorシステム要件

オペレーションシステム	Windows Server 2012 R2以降 *** Windows Server 2025でのご利用はOneLogin ADC 7.0.2以上が必要です** * FIPS準拠モードでは起動が失敗するためご注意ください
.NET Framework	.NET Framework 4.5.1以降
CPU	Pentium 4 以上
メモリ	512MB 以上
ストレージ	120MB 以上
ネットワーク	アウトバウンド 443ポート ** 通信先IPアドレスは次のネットワークレンジを参照*
ネットワークレンジ	• 23.183.113.12 • 23.183.112.12 • 52.34.225.194/31 • 52.34.255.196/30 • 52.34.255.200/29 • 52.34.255.208/28 • 52.34.255.224/27 • 18.216.23.64/26 (18.216.23.64 - 18.216.23.127) • 52.24.165.42 • 52.15.145.203 • 13.52.4.72/29 (13.52.4.72 - 13.52.4.79) • 23.183.112.0/24 • 23.183.113.0/24

プロキシ	インターネットオプションで設定したプロキシを利用可能 ** OneLogin ADCインストール時に指定したADCサービス実行アカウントでWindows Serverにログインし、インターネットオプションからプロキシ設定が必要です*
機能レベル	フォレスト / ドメイン 2003以上
リモートサーバー管理ツール	Active Directory Domain ServicesとActive Directory Lightweight Directory Services管理ツール ** Active Directory Connectorが動作するサーバーがドメインコントローラーでない場合は個別にインストールが必要です（ドメインコントローラーの場合はすでにインストール済みです）*

Active Directoryユーザー項目について

必須項目

OneLoginに同期するActive Directoryユーザーのアカウントは以下の4項目の登録が必須となっております。

Active Directory側の項目名（表示タブ）	OneLogin側の項目名
姓（全般）	Last name
名（全般）	First name
電子メール（全般）	Email
表示名（全般）	Active Directory側の必須項目であり、通常OneLogin側へは同期されません

標準同期項目

必須項目に加え以下の項目がOneLoginへ同期可能です。

Active Directory側の項目名（表示タブ）	OneLogin側の項目名
所属するグループ（所属するグループ）	MemberOf
ステータス（全般）	Status
会社名（組織）	Company

部署（組織）	Department
役職（組織）	Title
上司（組織）	Manager
Object GUID（属性エディター）	Object GUID ** 本項目の編集はできません*
ユーザーログオン名（アカウント）	UserPrincipalName ** 本項目の編集はできません*
Distinguished name（属性エディター）	Distinguished name ** 本項目の編集はできません*
sAMAccountName（属性エディター）	ユーザーログオン名（Windows 2000より前） ** 本項目の編集はできません*

標準同期項目以外を同期する

上記の標準同期項目以外はCustom User Fieldsを用いることで同期が可能です。例えば、Active Directoryの表示名（全般）をOneLoginのdisplayNameに表示するなどが可能です。設定手順はActive Directoryから標準同期項目以外の属性を追加同期するをご覧ください

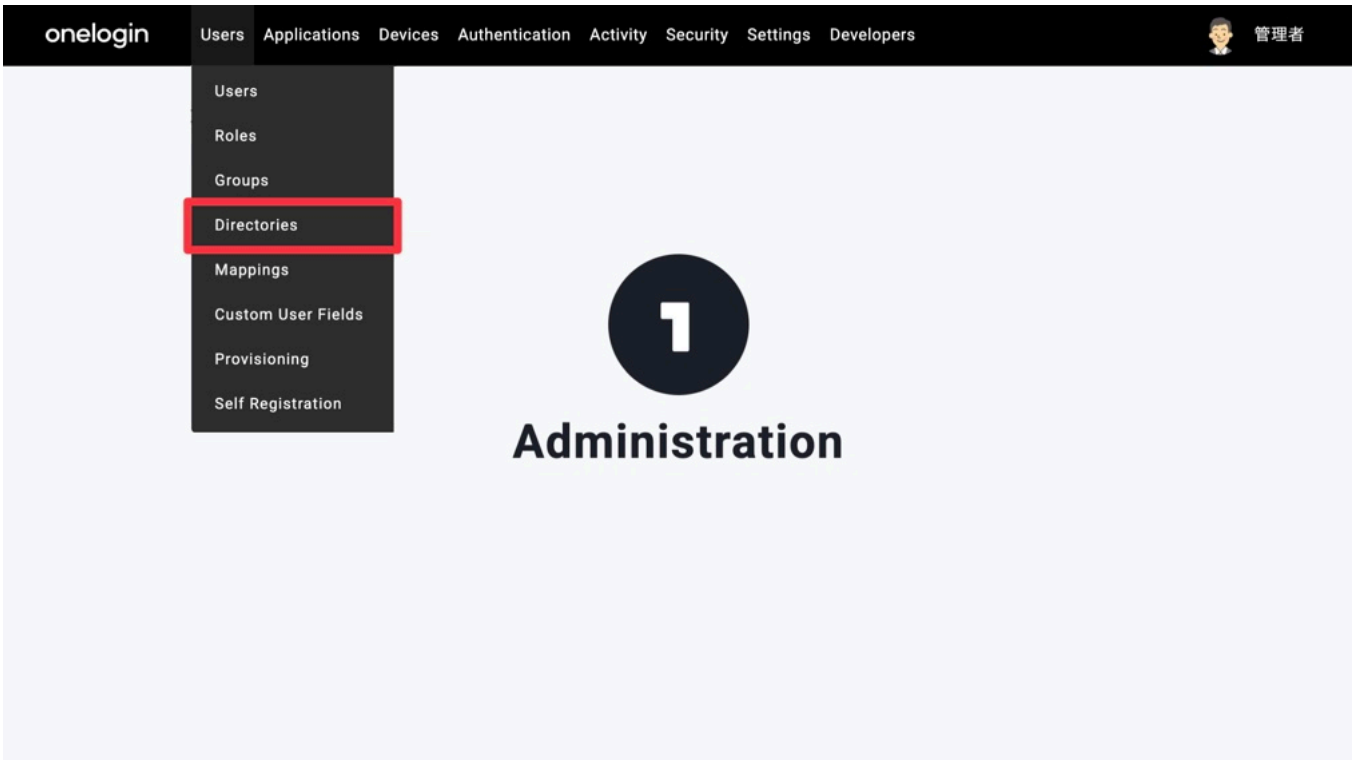
OneLoginにActive Directory連携を設定する

1. OneLoginにディレクトリ連携設定を追加する

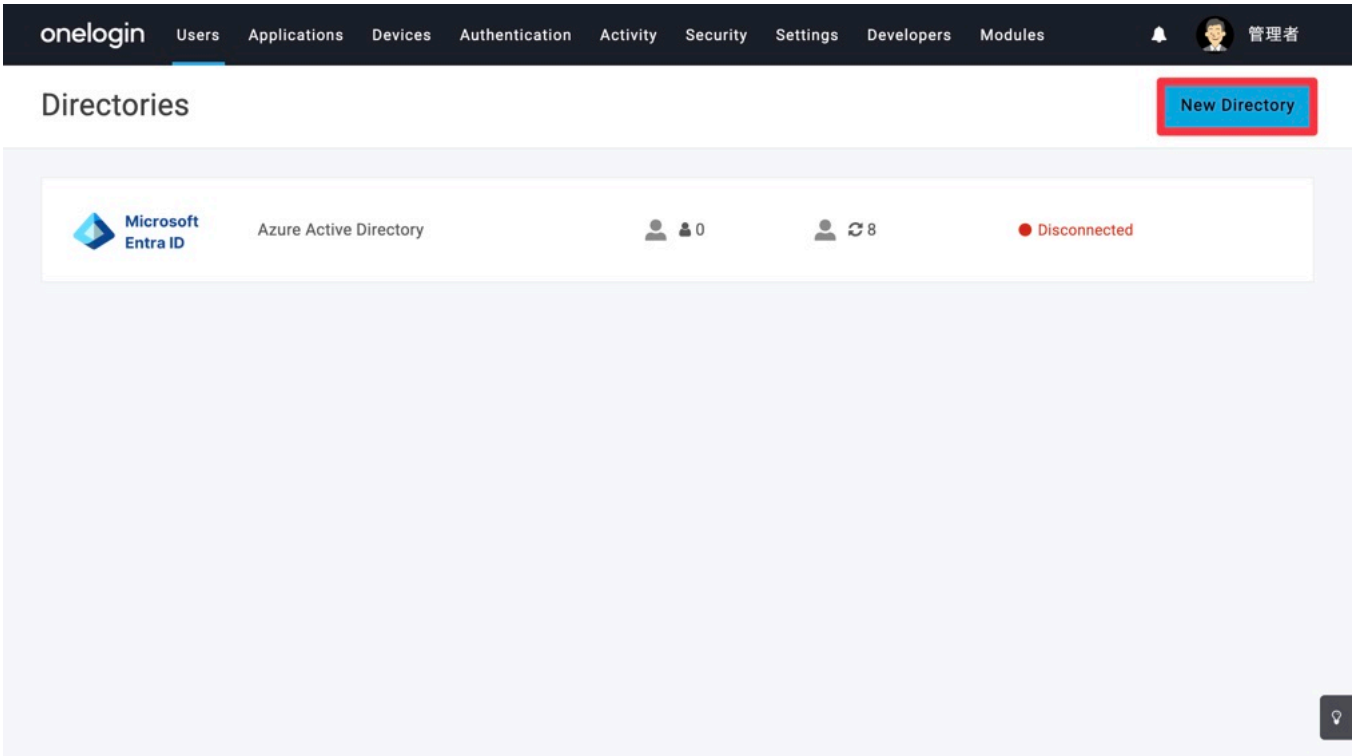
1. OneLoginに管理者でログインし、**管理** を開きます



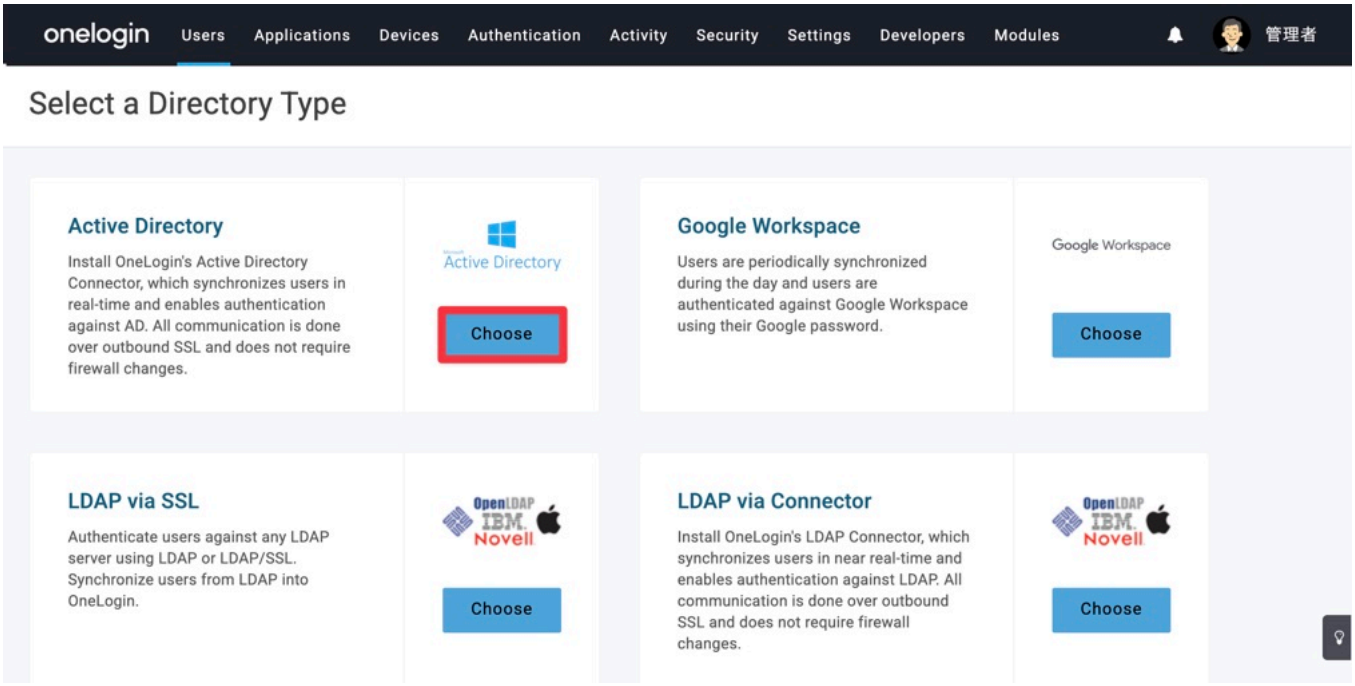
2. Users > **Directories** を開きます



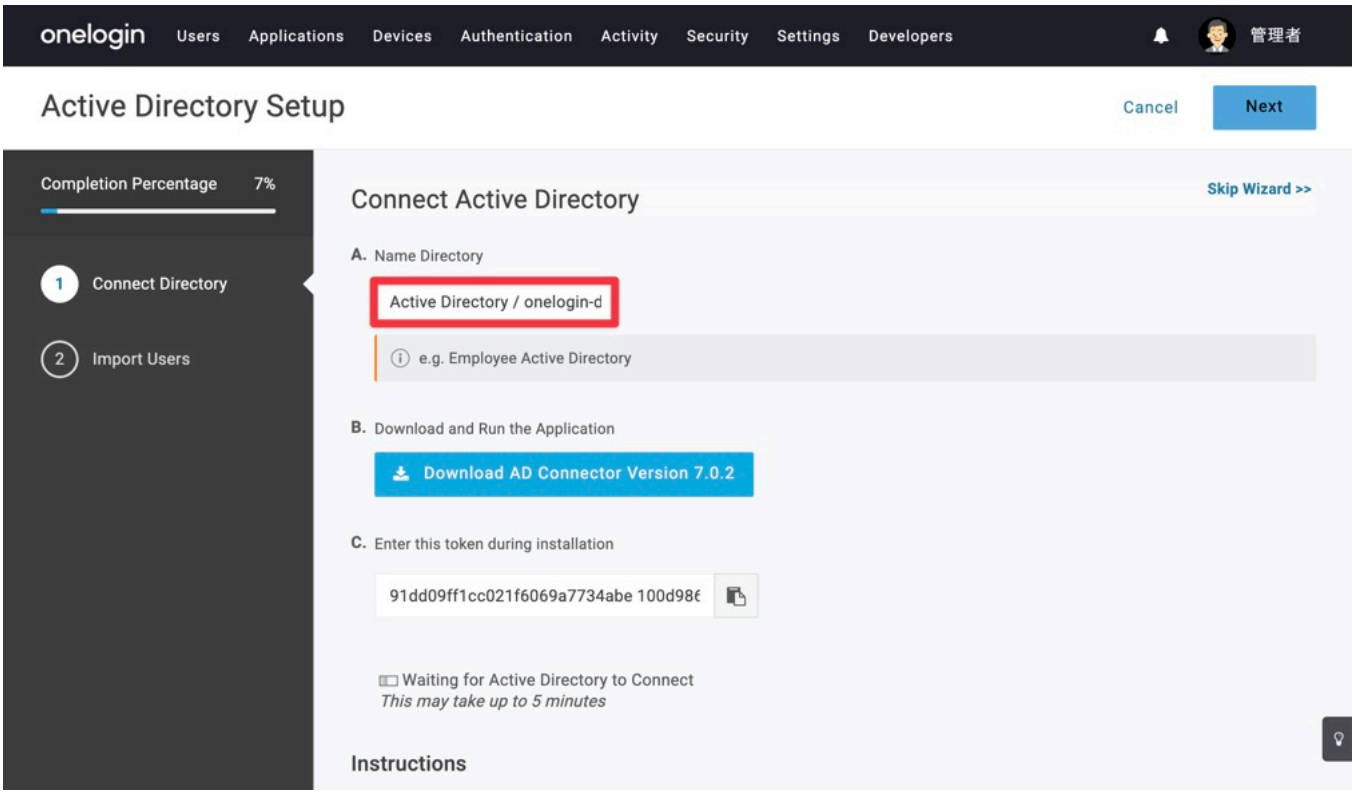
3. ［**New Directory**］をクリックします



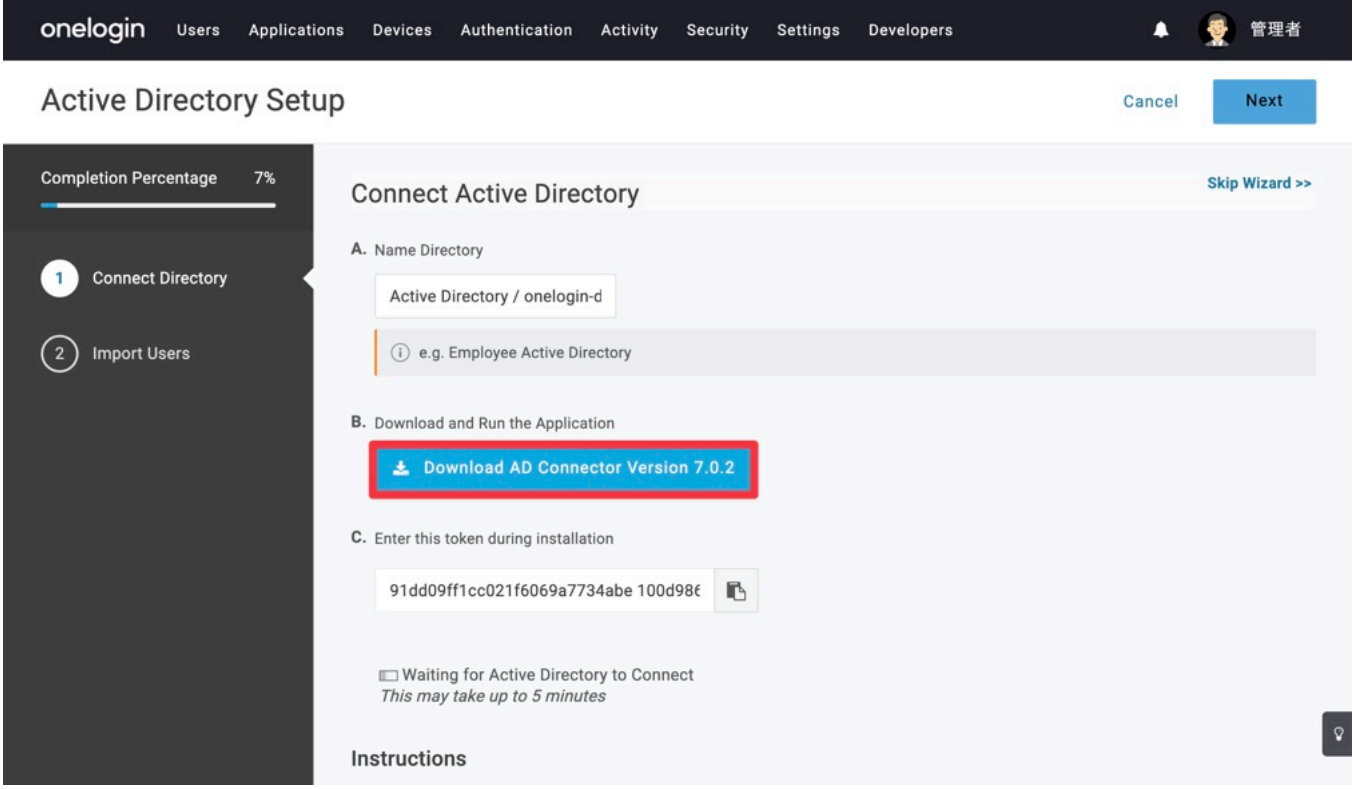
4. Active Directory >［**Choose**］をクリックします



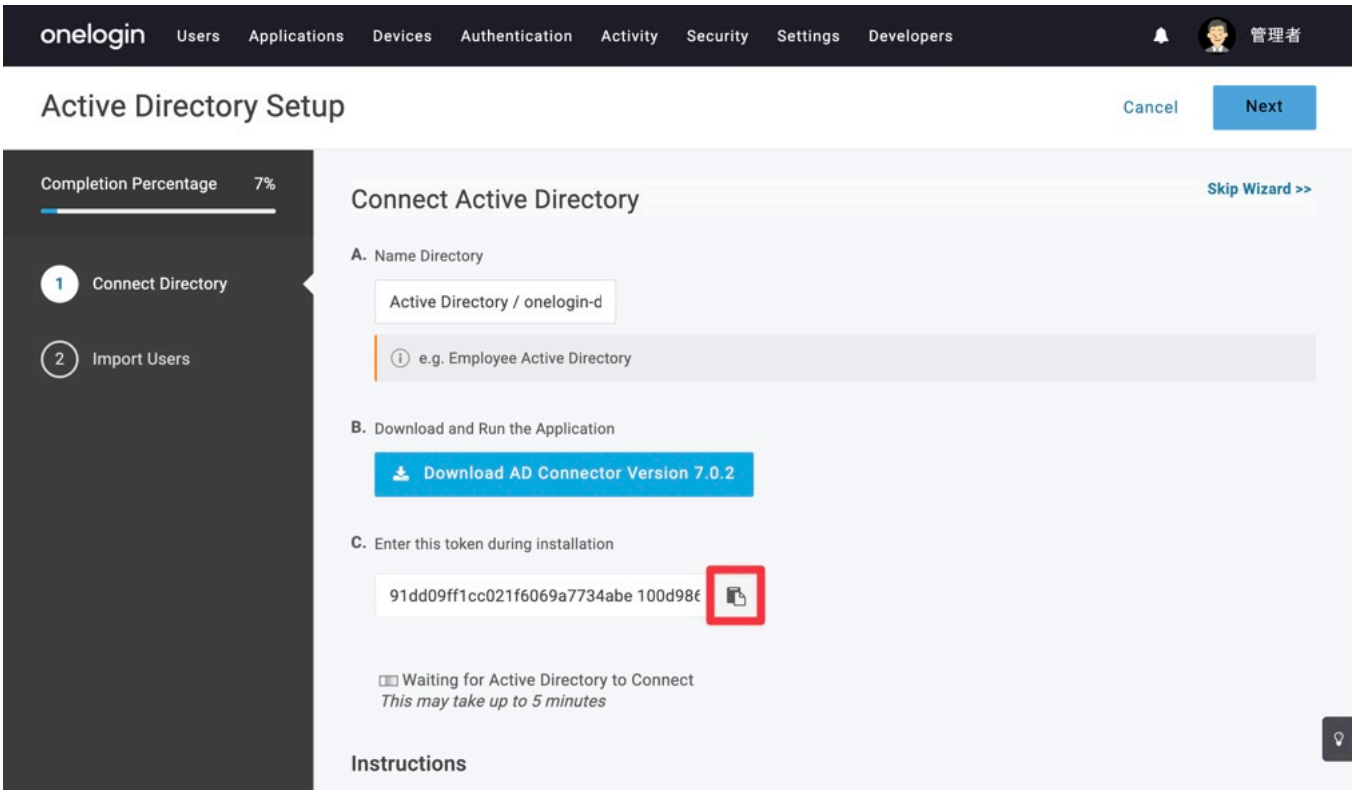
5. **Name Directory** にて設定するActive Directoryの識別名を入力します
例）Active Directory / onelogin-dev.local



6. ［**Download AD Connector Version 7.0.2**］をクリックします
** ボタン末尾のバージョンは実行時期により異なる場合がございます*



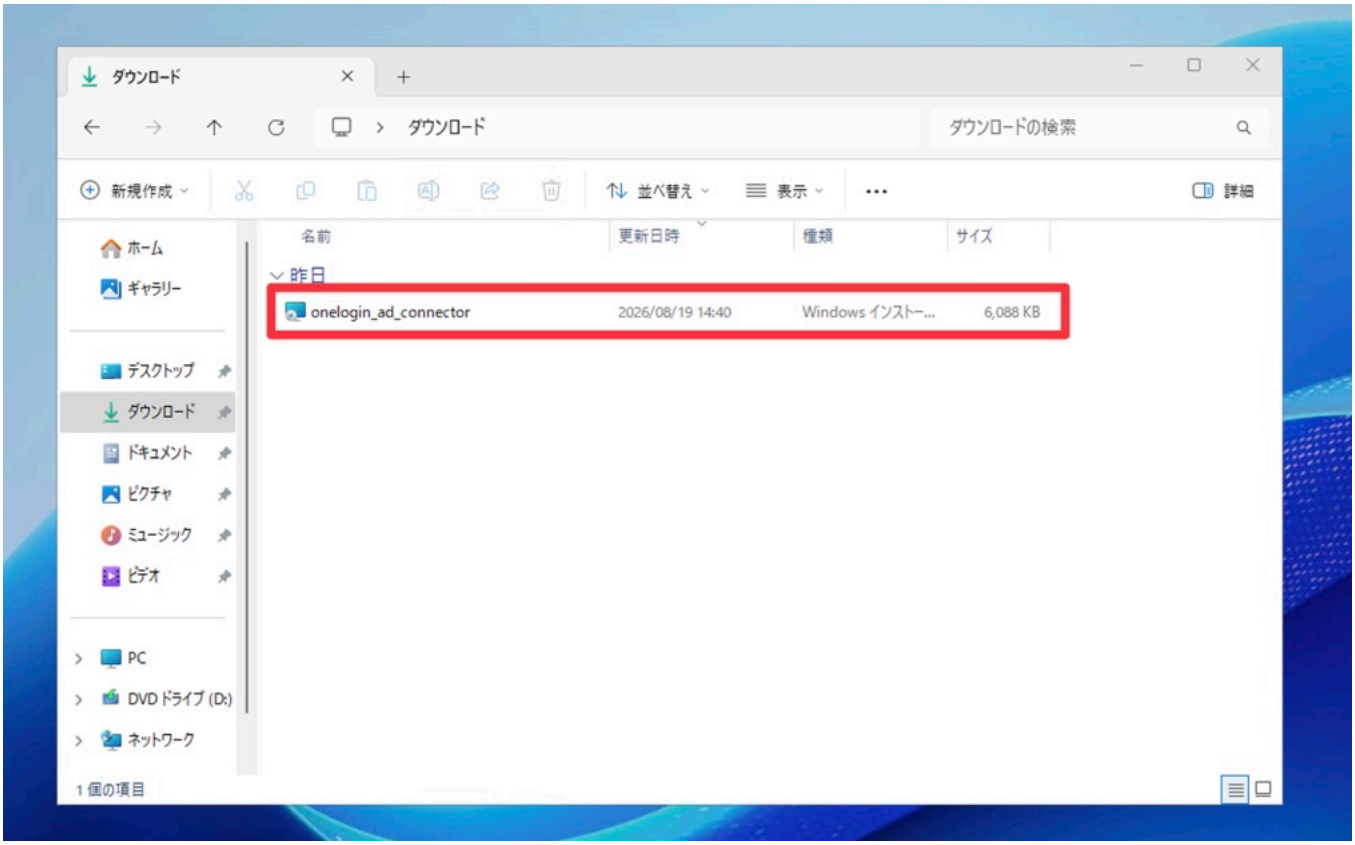
7. **Enter this token during installation** のコピーボタンをクリックし、トークンをクリップボードへコピーします



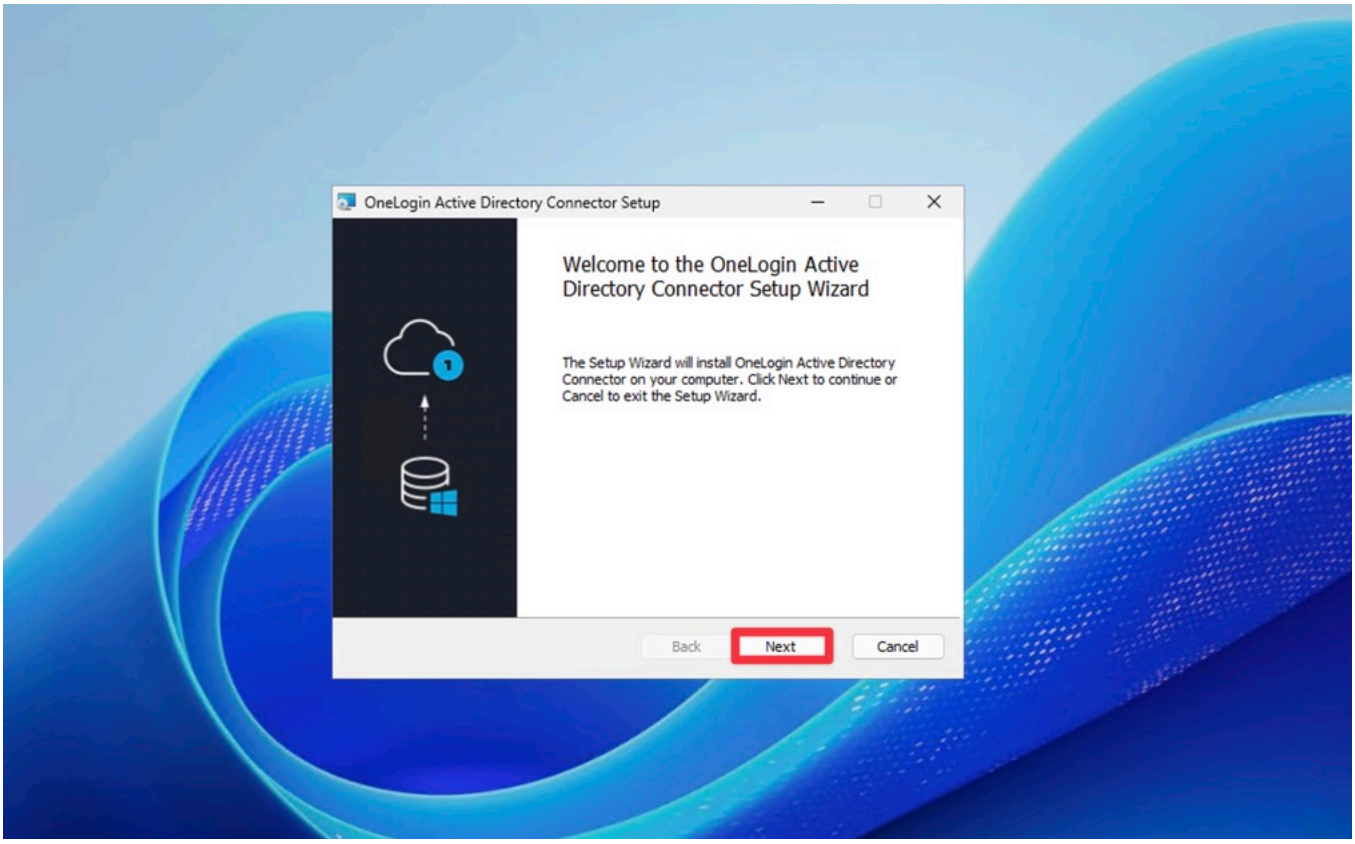
OneLoginにディレクトリ連携設定を追加する手順は以上です。

2. OneLogin Active Directory ConnectorをWindows Serverにインストールする

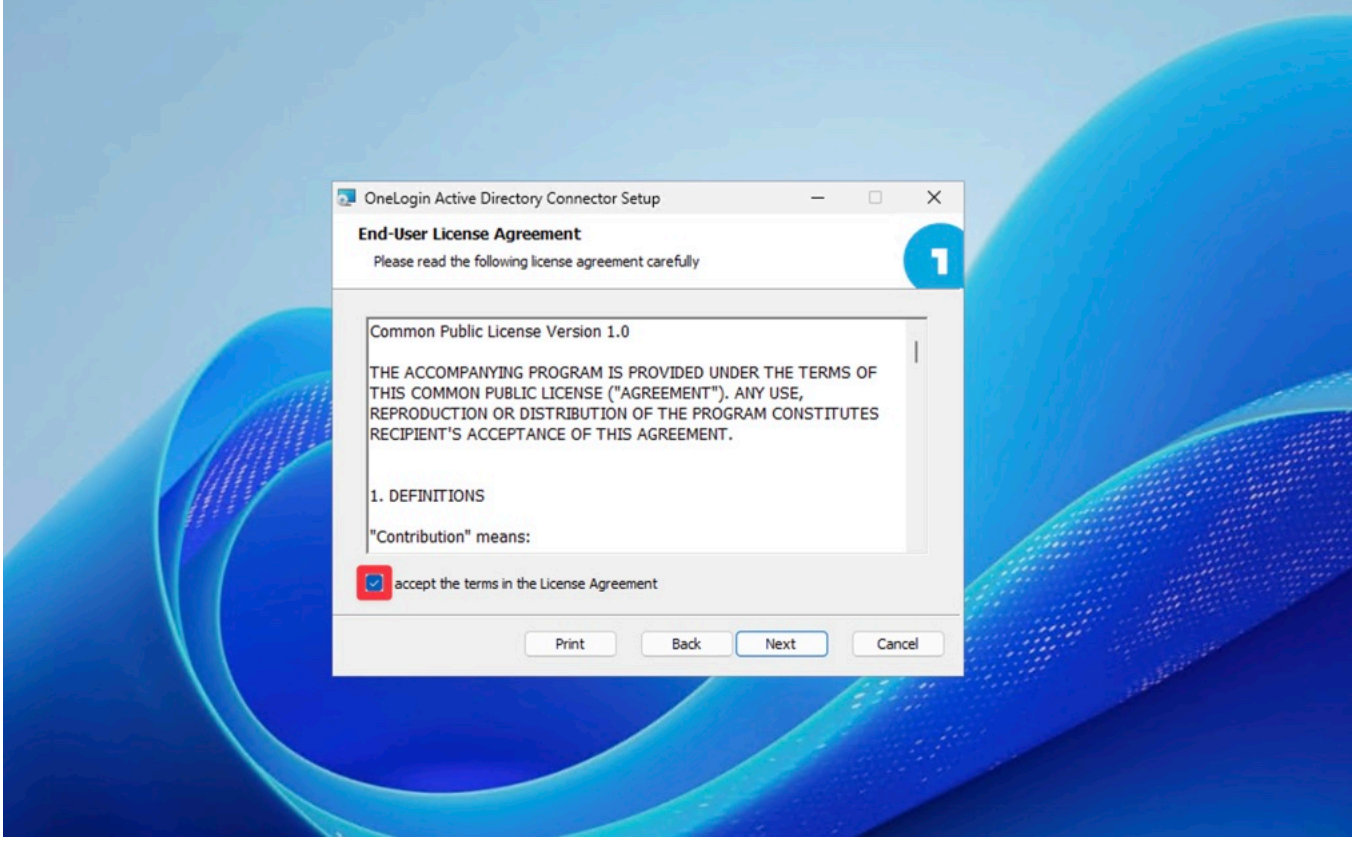
1. OneLogin ADCをインストールするサーバーへ接続し、1. OneLoginにディレクトリ連携設定を追加する 手順6でダウンロードした **onelogin_ad_connector** をダブルクリックで起動します
   ** 本手順はドメイン管理者でログインし実行してください。通常の管理者として実行とは異なるためご注意ください*



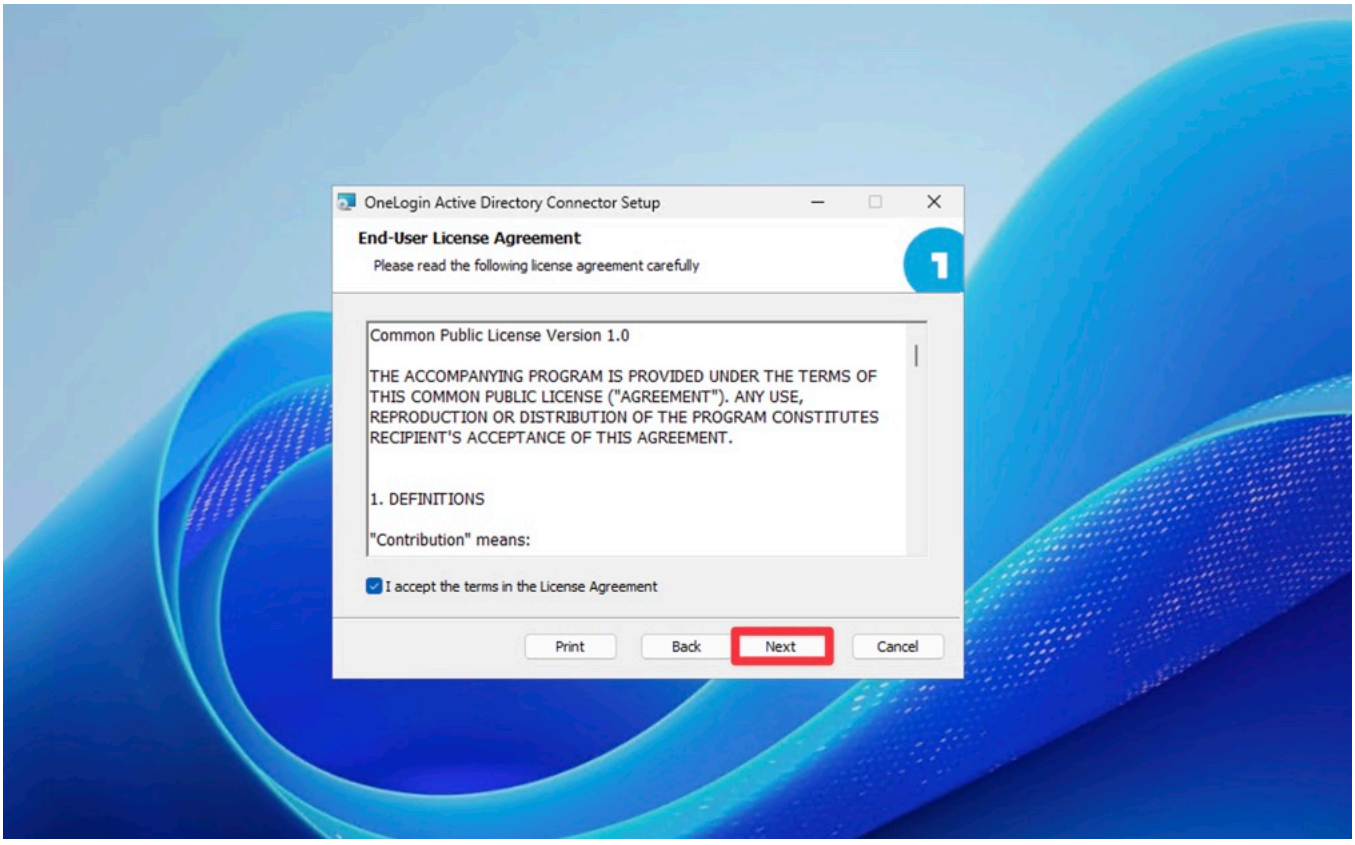
2. ［**Next**］をクリックします



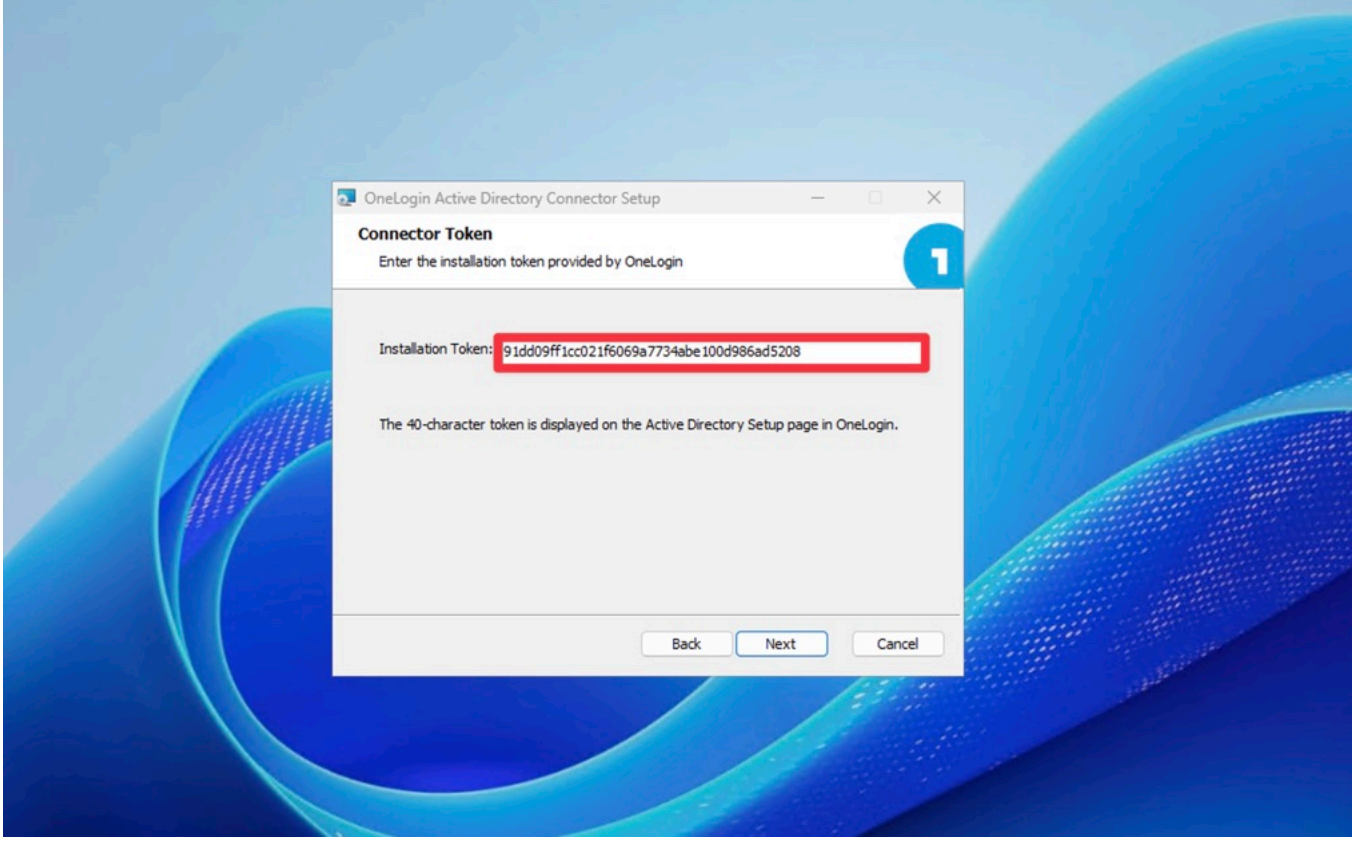
3. ライセンス規約を確認し、**accept the terms in the License Agreement** のチェックボックスにチェックを入れます



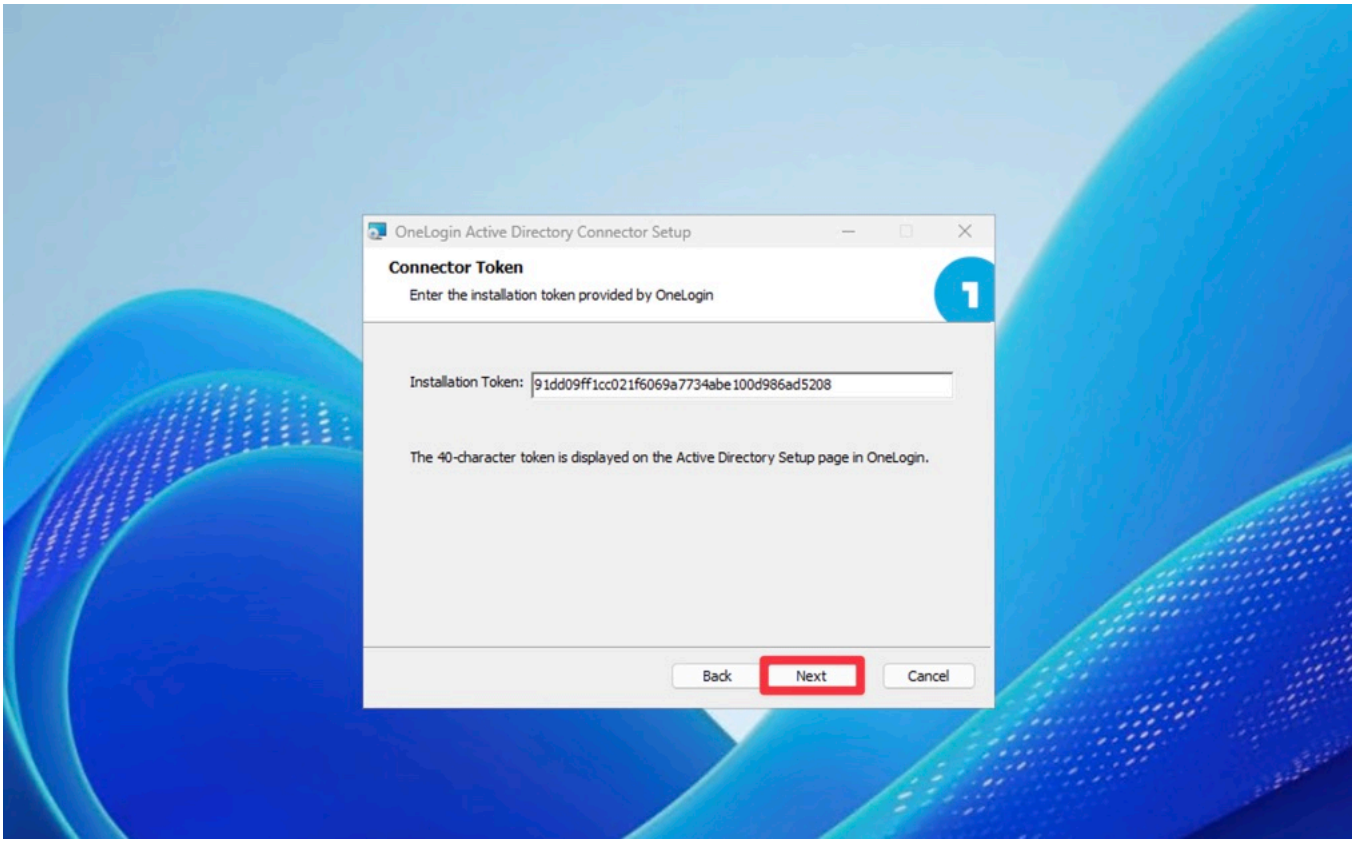
4. ［**Next**］をクリックします



5. Installation Tokenに1. OneLoginにディレクトリ連携設定を追加する 手順7でコピーしたトークンを入力します



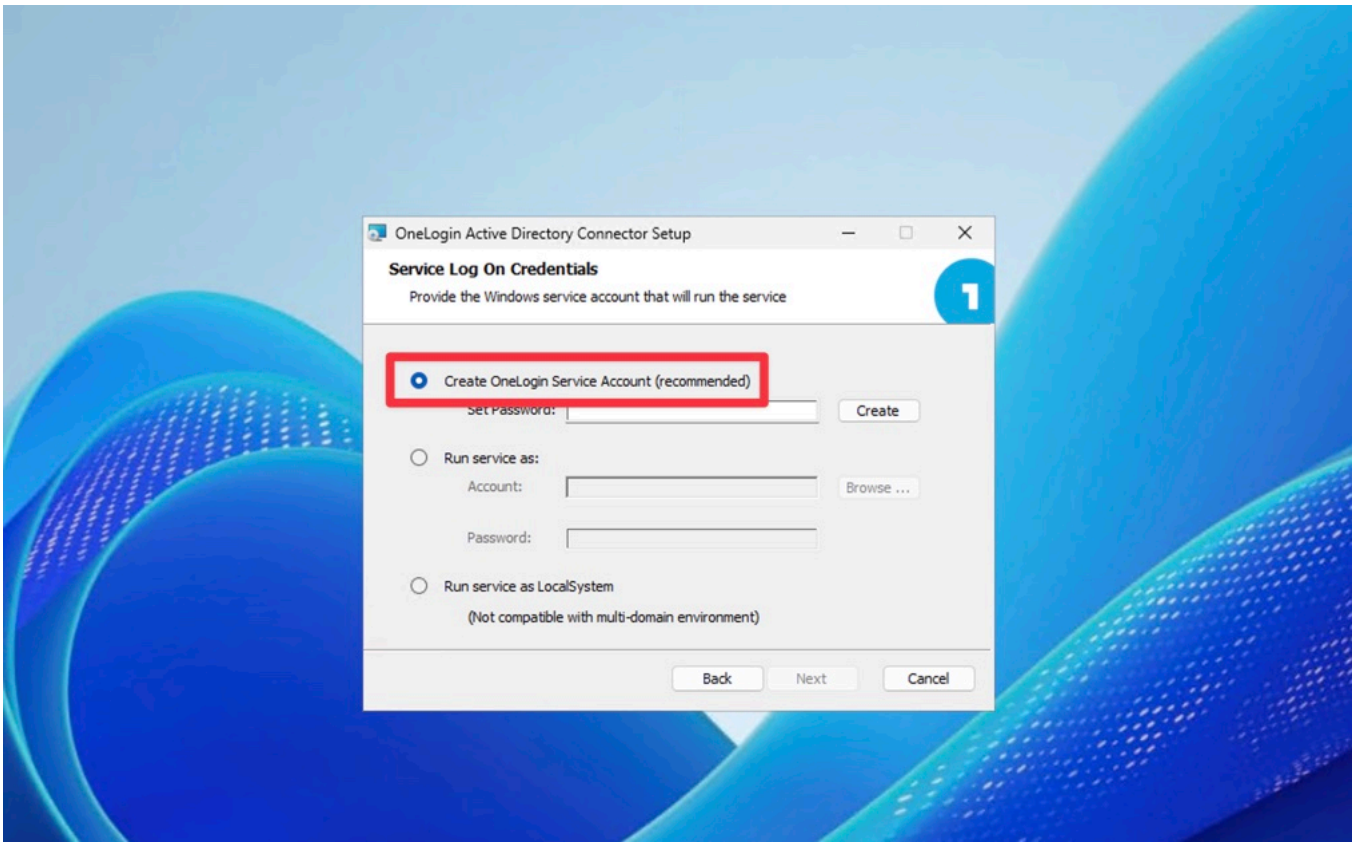
6. ［**Next**］をクリックします



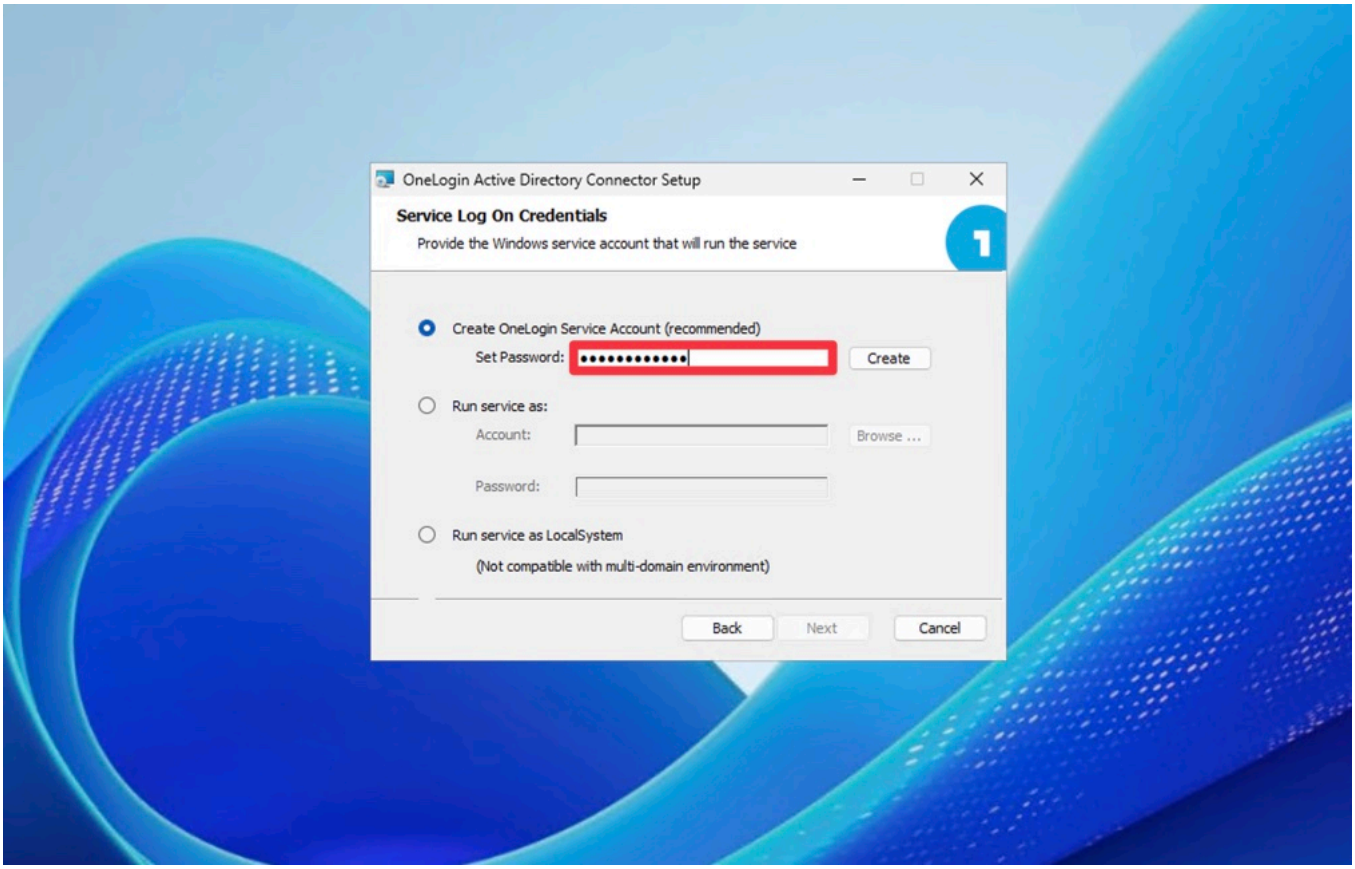
7. OneLogin ADCを実行するためのアカウントを以下の選択肢から選択します
   ** 本記事では **Create OneLogin Service Account** の選択を推奨いたします*

選択肢	実行する動作
Create OneLogin Service Account	OneLogin ADCアカウントを自動で新規作成し、そのアカウントでOneLogin ADCを実行する
Run service as	既存のアカウントを指定してOneLogin ADCを実行する *1*
Run service as LocalSystem	単一のドメインかつメンバーサーバーではなくドメインコントローラーにのみインストールする場合、LocalSystemアカウントでOneLogin ADCを実行する

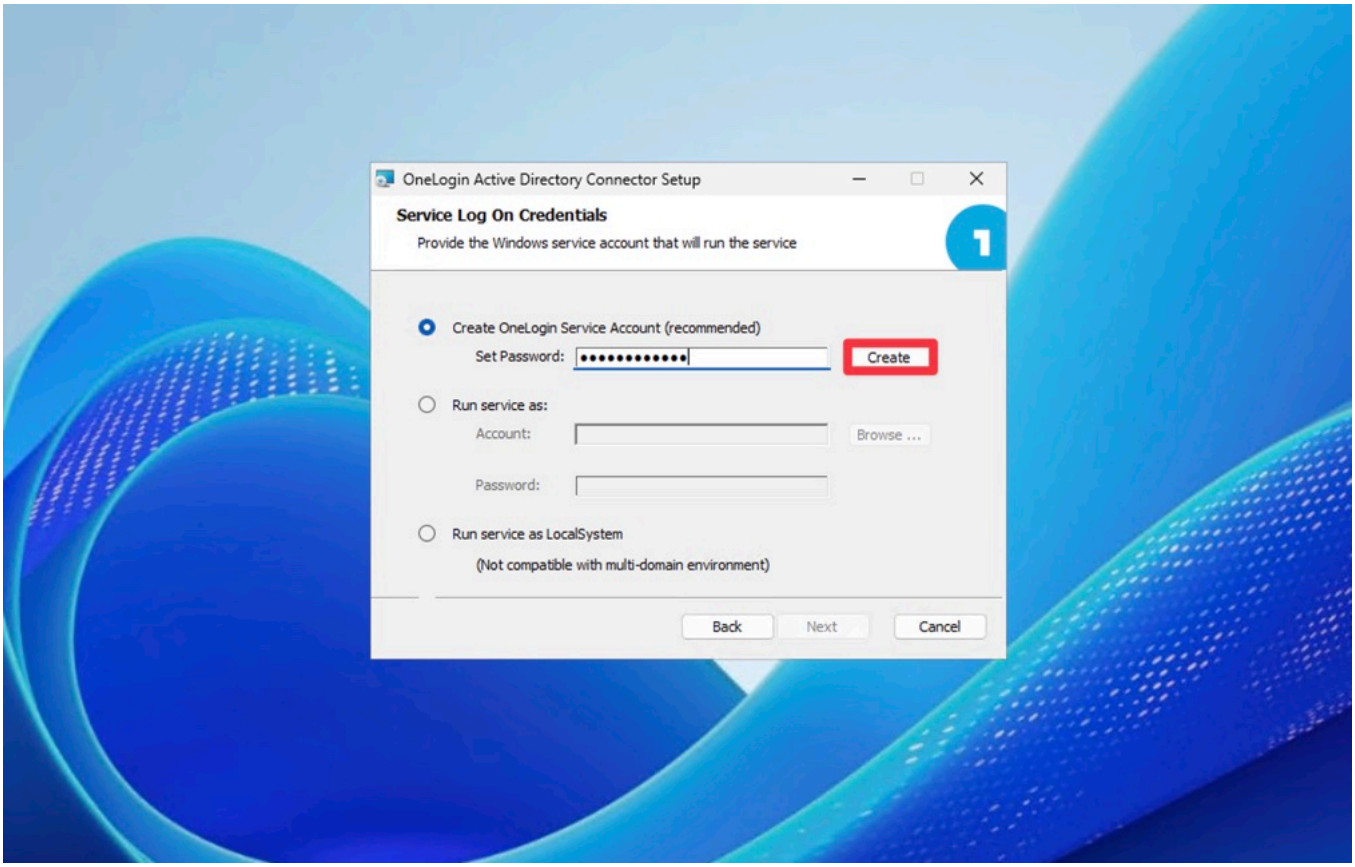
1 指定するユーザーがフォレストとドメイン全体のディレクトリツリーの読み取り権限およびパスワードのリセット権限を持つ必要があります。詳細はOneLogin ADCアカウントの設定をご参照ください



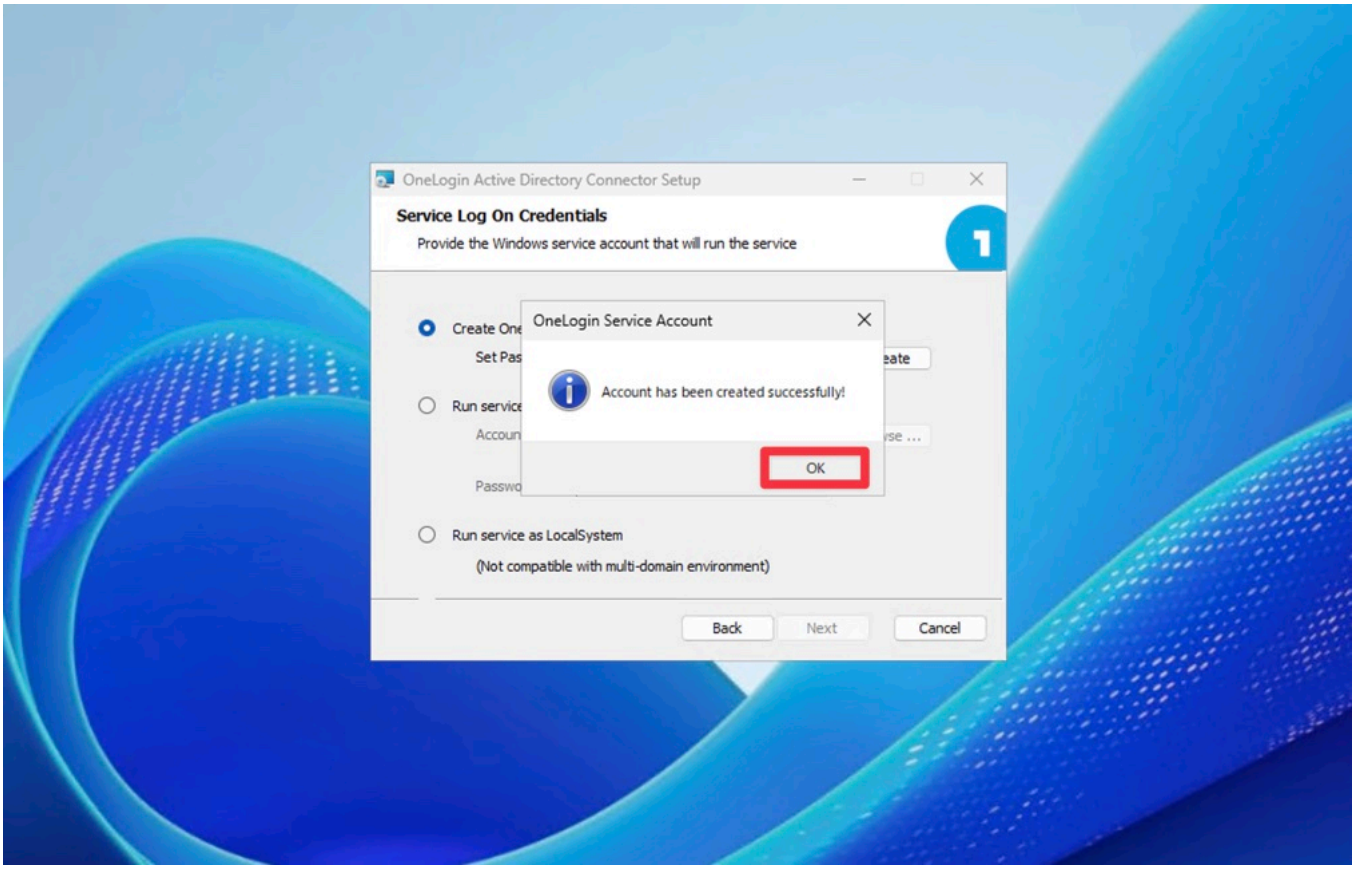
8. **Set Password** に新規作成するユーザーのパスワードを入力します



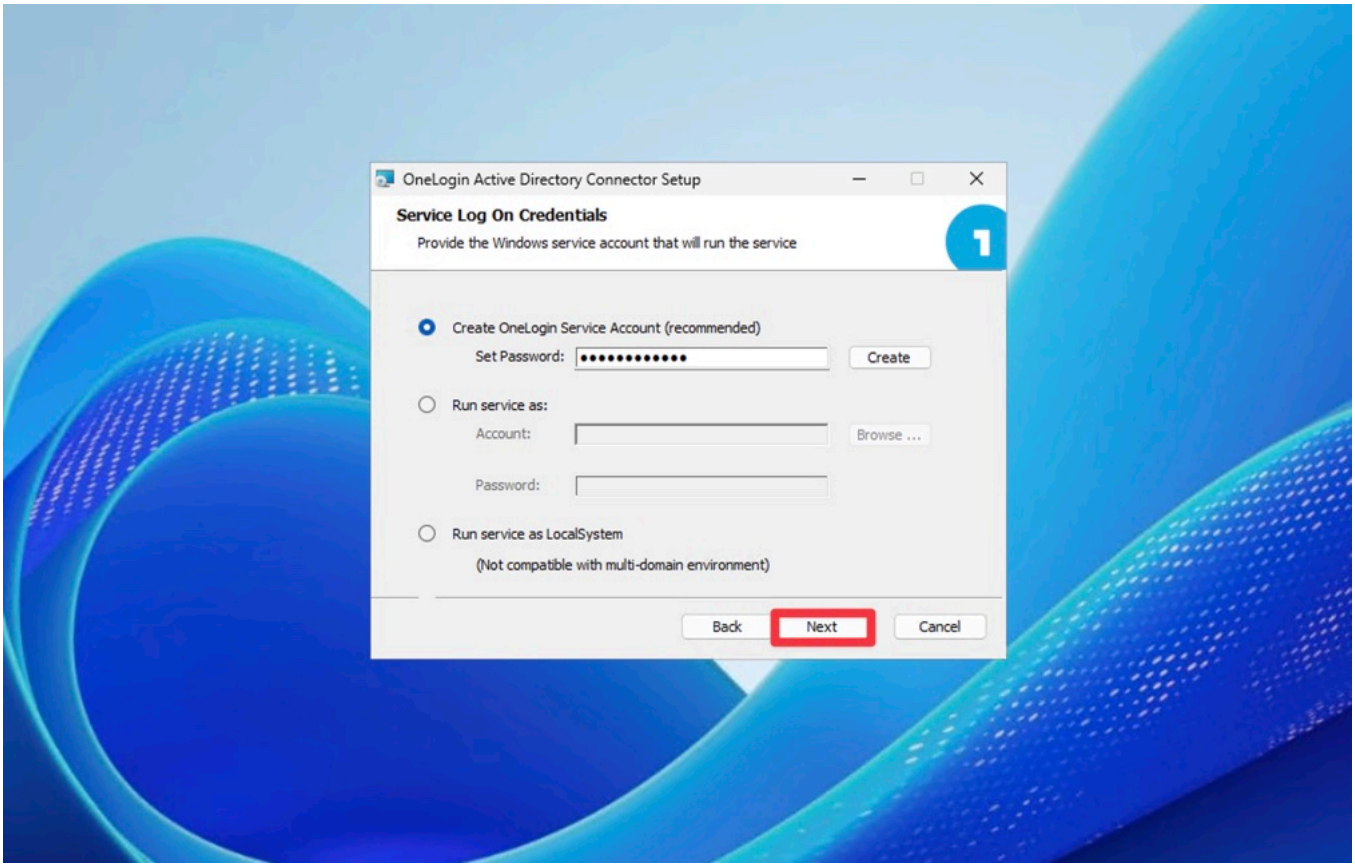
9. ［**Create**］をクリックします



10. **Account has been created successfully!** と表示されることを確認し、［**OK**］をクリックします



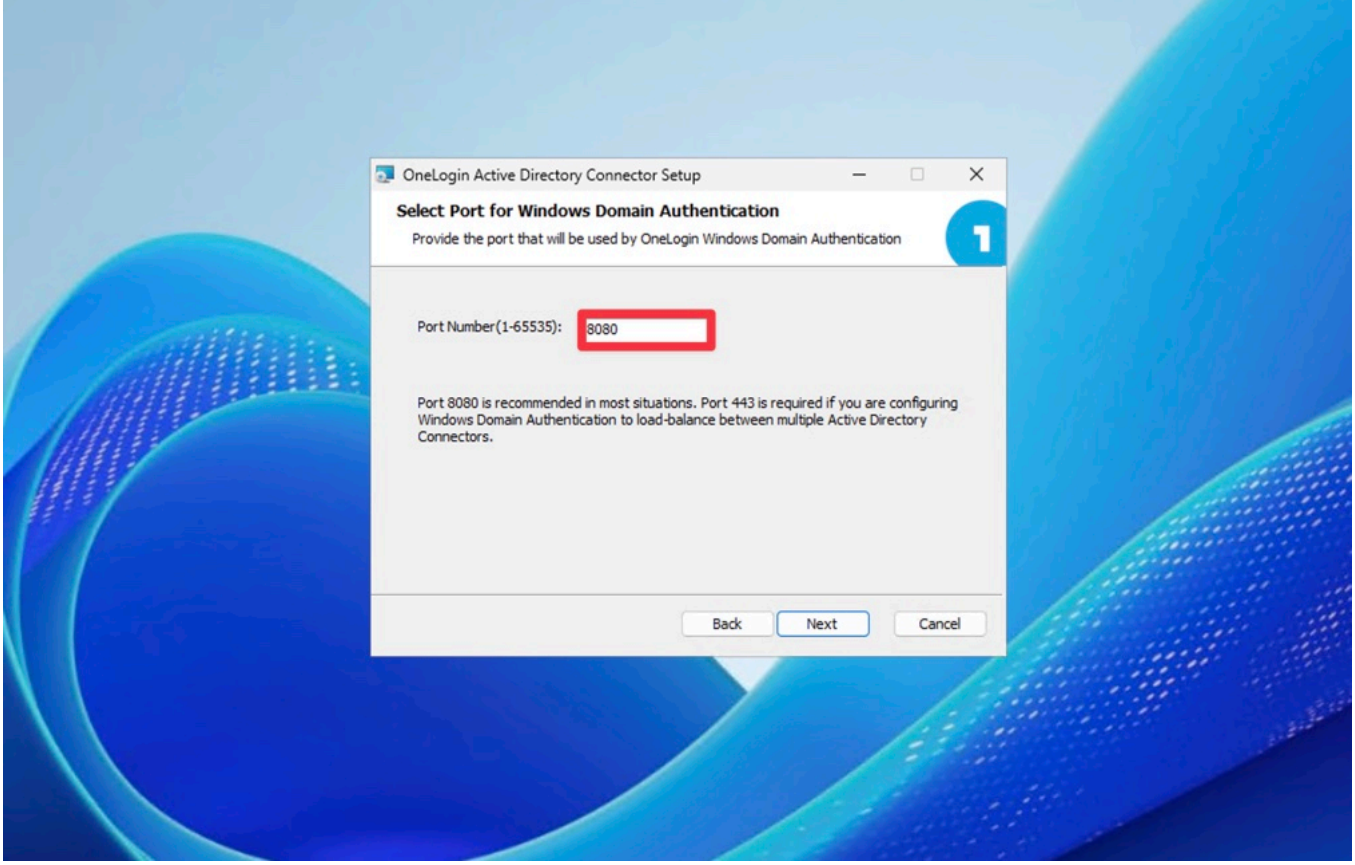
11. ［**Next**］をクリックします



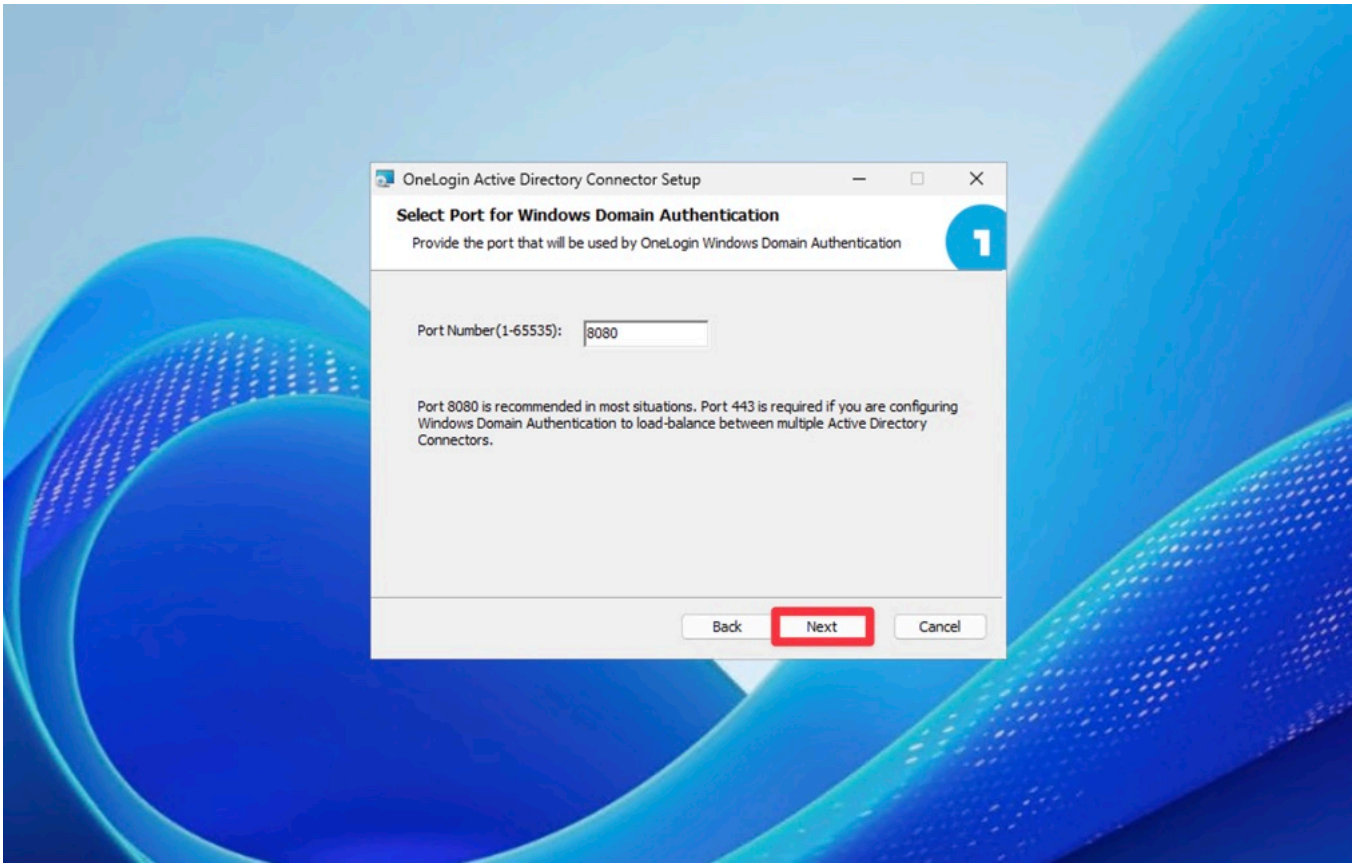
12. **Windows Domain Authentication** に利用するポート番号を選択します

** デフォルトでは8080が設定されていますが、Windows Domain Authenticationを利用する場合は実際に参加デバイスから通信できるポート番号を選択してください。*

また、Windows Domain Authenticationを利用しない場合はデフォルトのままで問題ありません

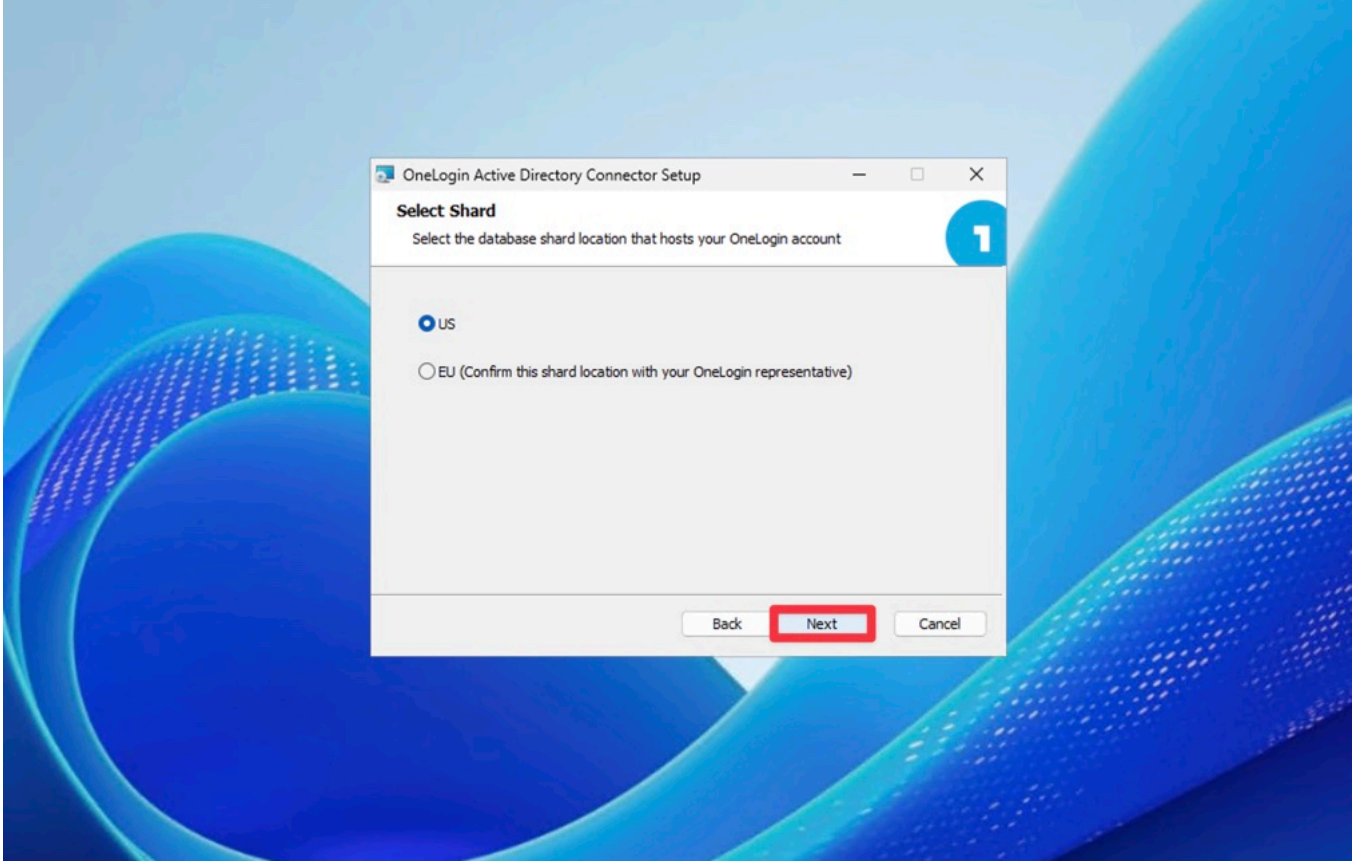


13. ［**Next**］をクリックします

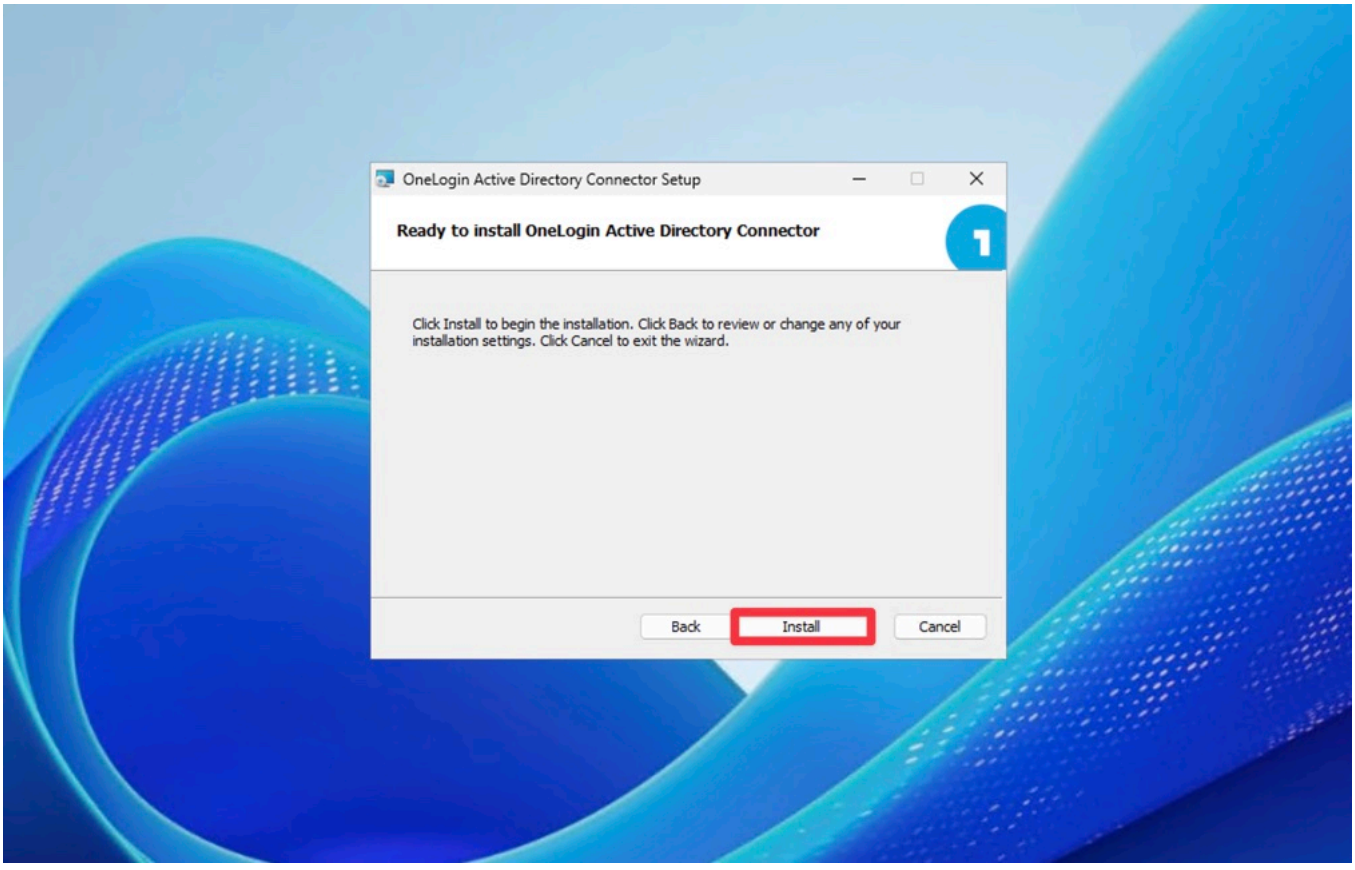


14. ご利用のOneLoginが管理されている **US** シャードが選択されていることを確認し、［**Next**］をクリックします

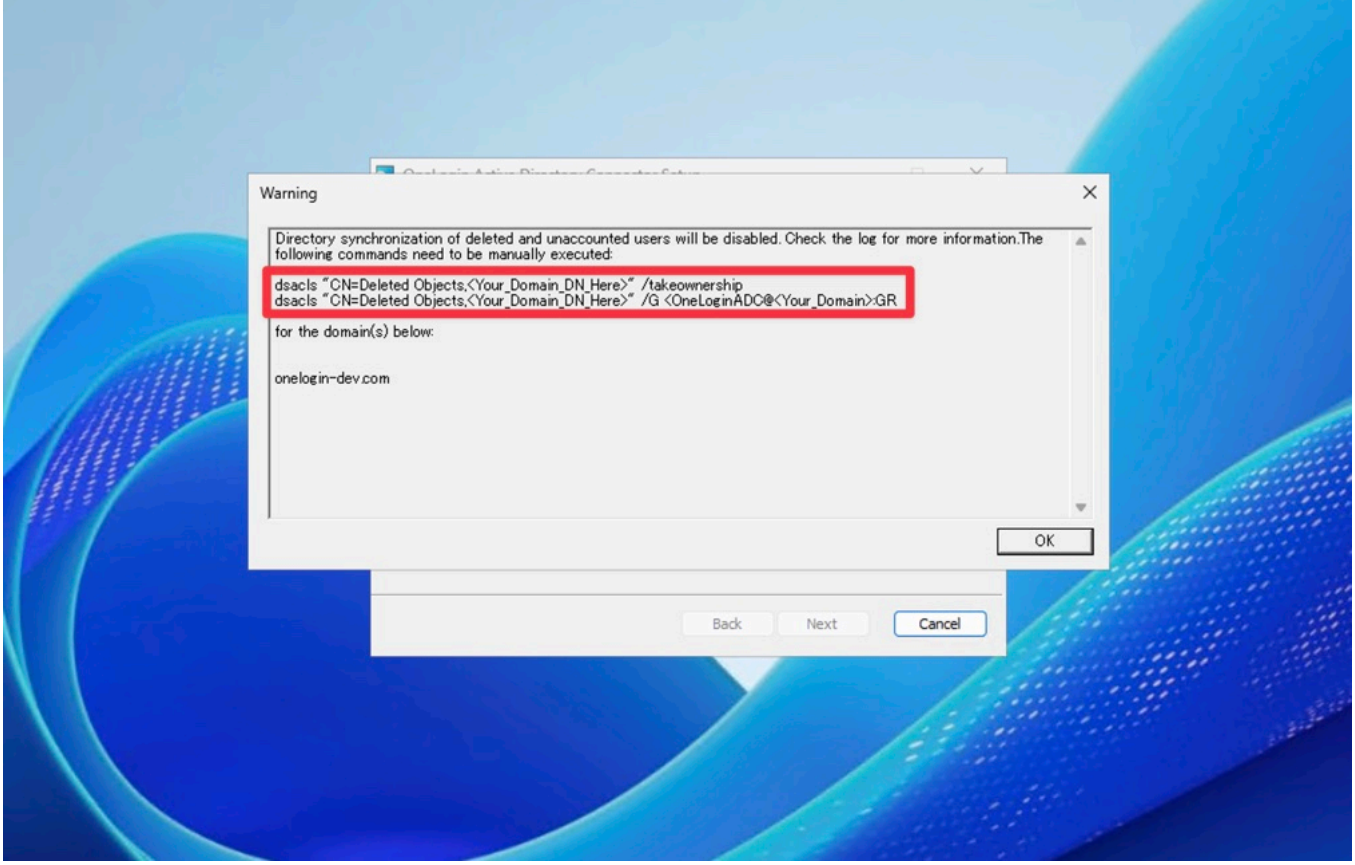
    ** ペンティオにてOneLoginをご契約のお客様は原則USをご選択ください*



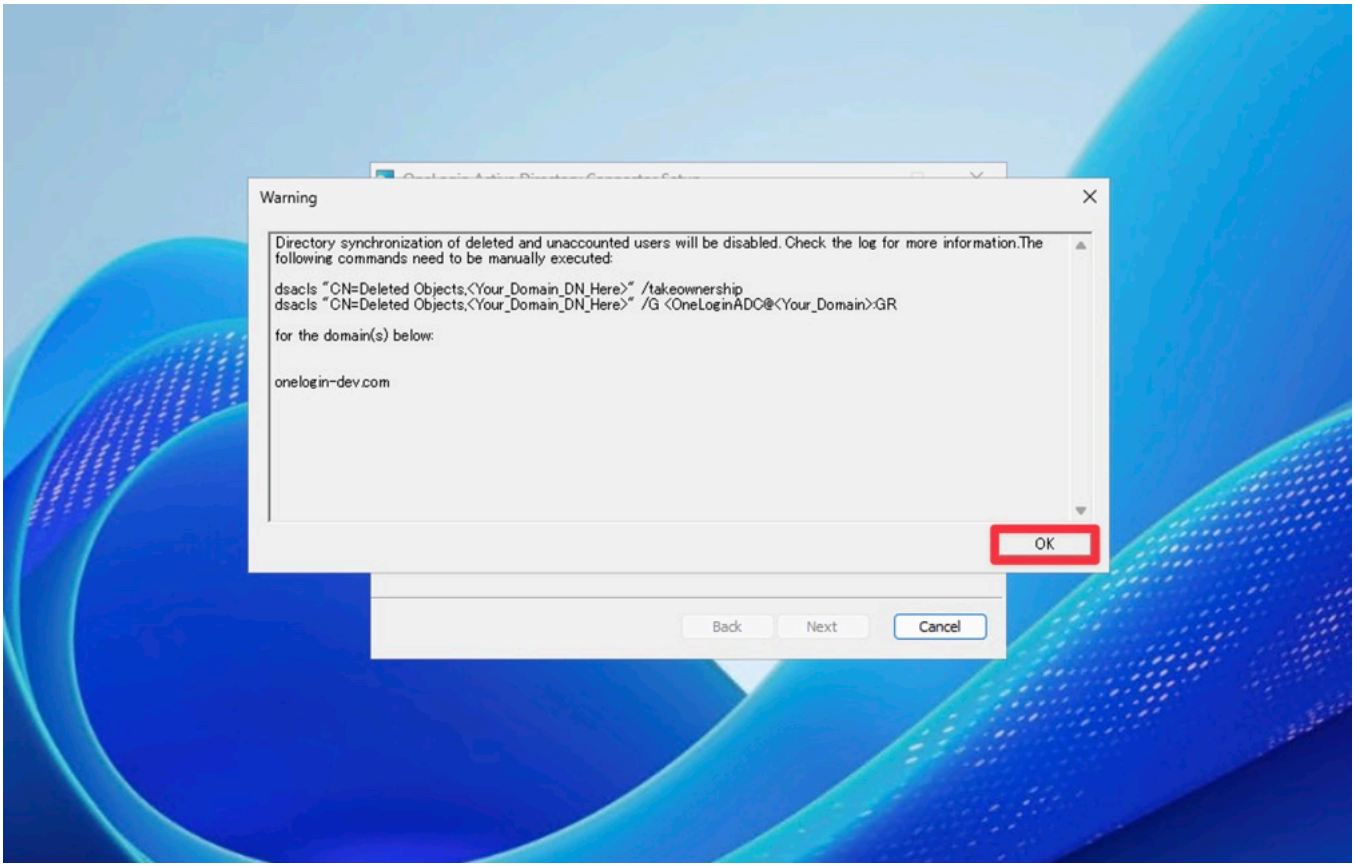
15. ［**Install**］をクリックし、インストールを開始します



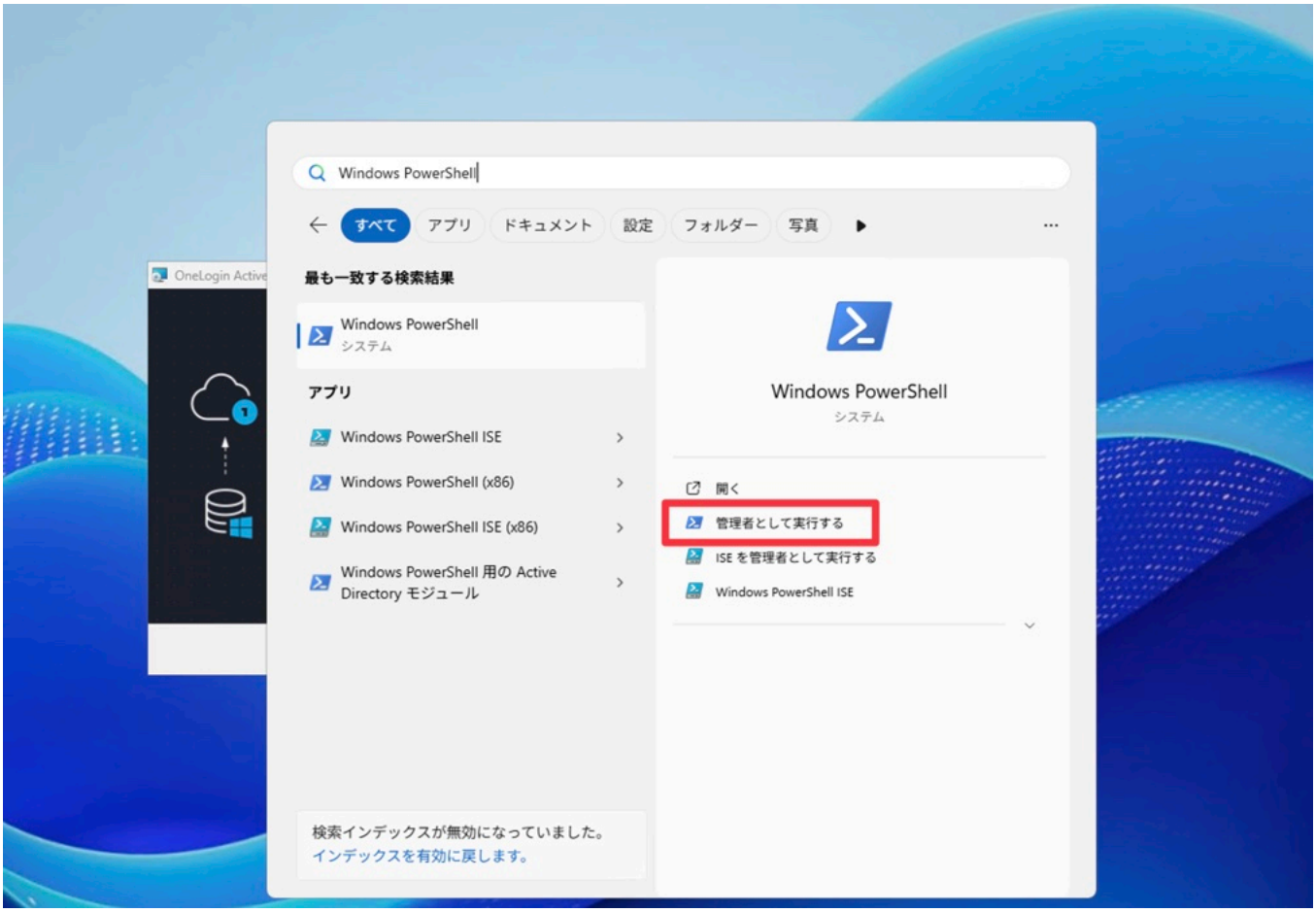
16. 表示されたポップアップに記載されている2つのコマンドをコピーします
    ** 本コマンドはActive Directory上の「削除済みオブジェクト」を参照できるようにOneLogin ADCへアクセス権限を付与するコマンドです*
    **** OneLogin ADCをメンバーサーバーにインストールする場合は、OneLogin Active Directory Connectorをメンバーサーバーにインストールする場合を必ずご確認ください***



17. ［**OK**］をクリックします



18. コマンドプロンプトまたは **Windows PowerShell** を管理者として実行します

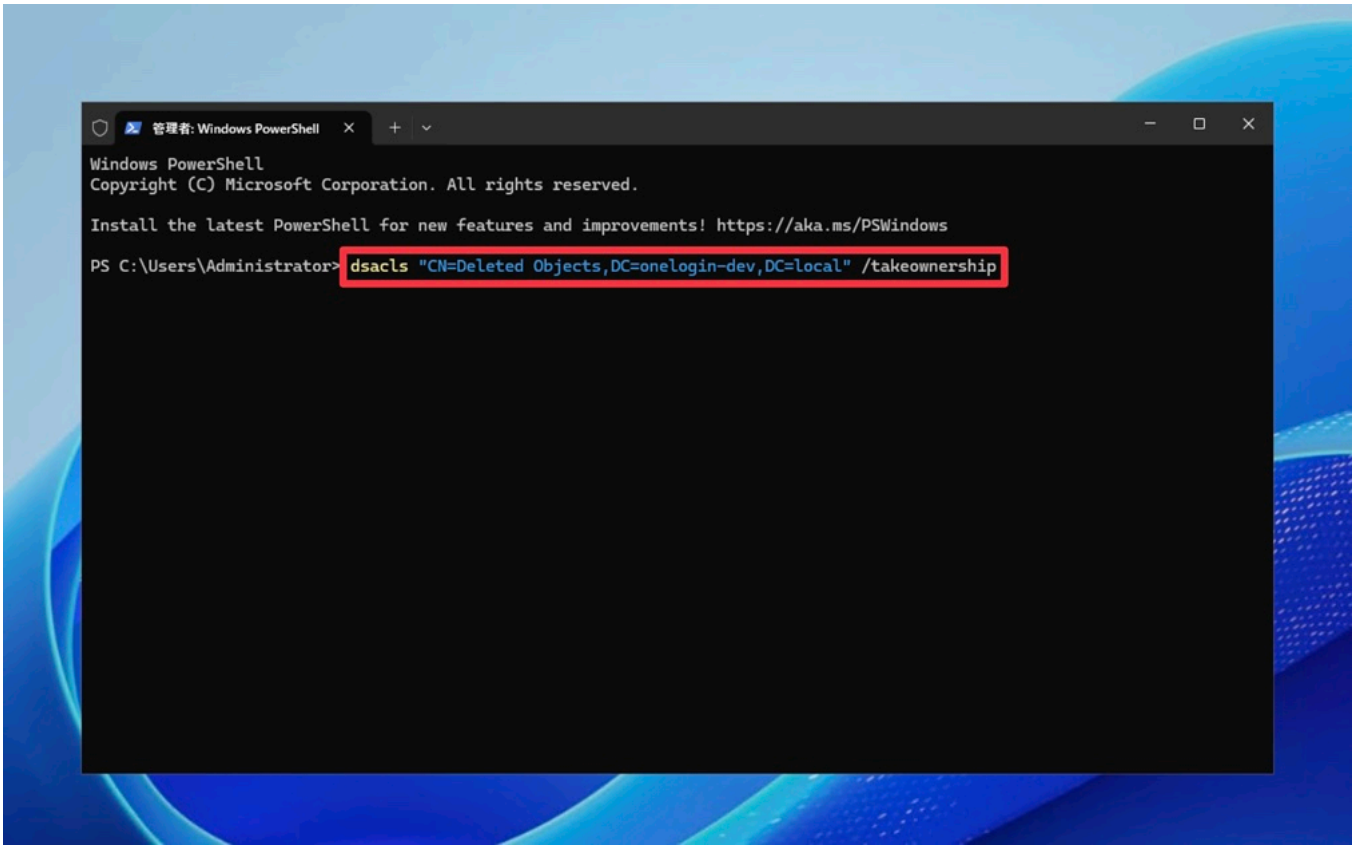


19.
```
dsacls "CN=Deleted Objects,<Your_Domain_DN_Here>" /takeownership
```

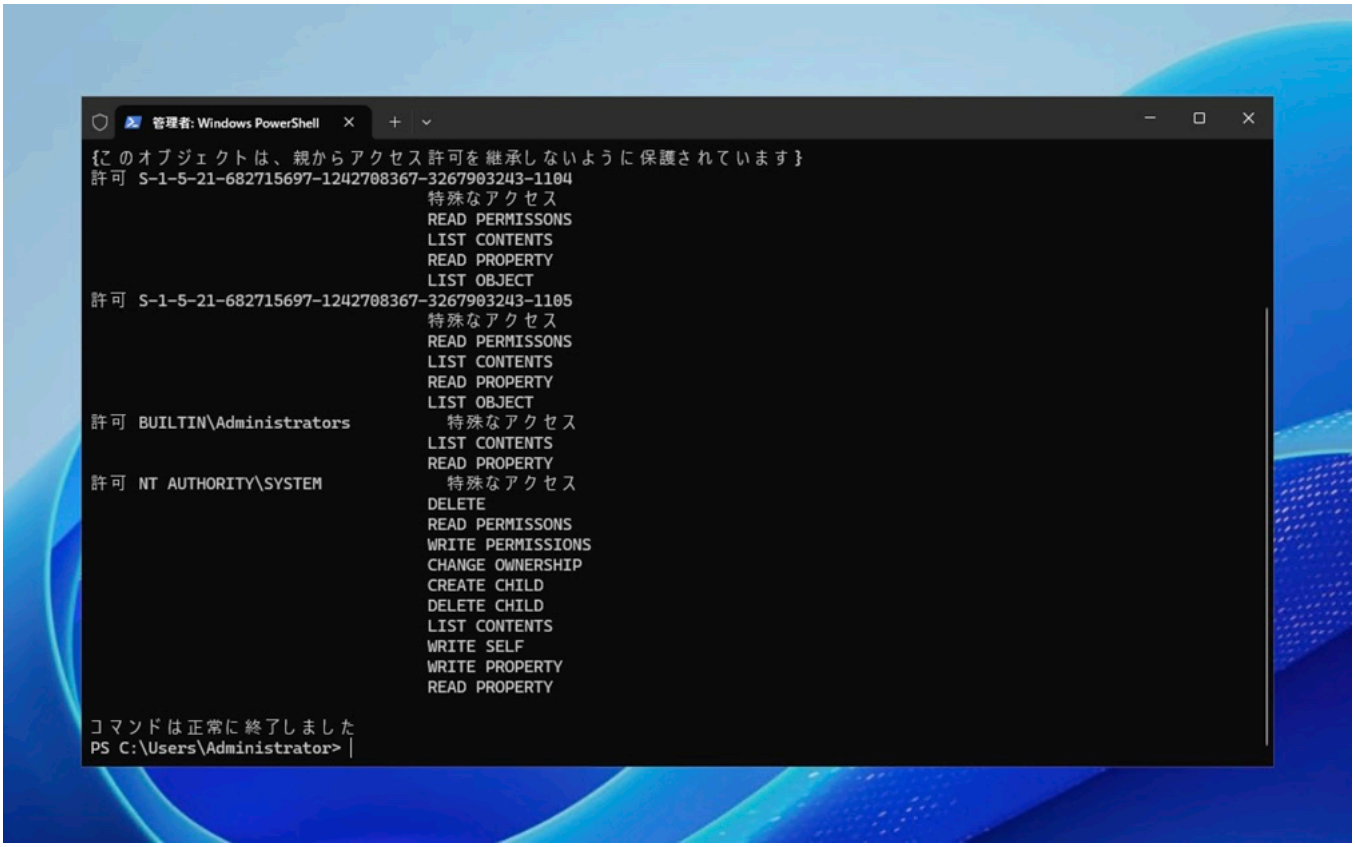
の<Your_Domain_DN_Here>の部分を **ドメイン識別名** に置き換えて実行します
例）Active Directoryドメインが onelogin-dev.localの場合は、下記を実行します

```
dsacls "CN=Deleted Objects,DC=onelogin-dev,DC=local" /takeownership
```

* ドメイン識別名の確認方法はドメイン名とドメイン識別名の確認をご参照ください



20. **コマンドが正常に終了しました** と表示されることを確認します



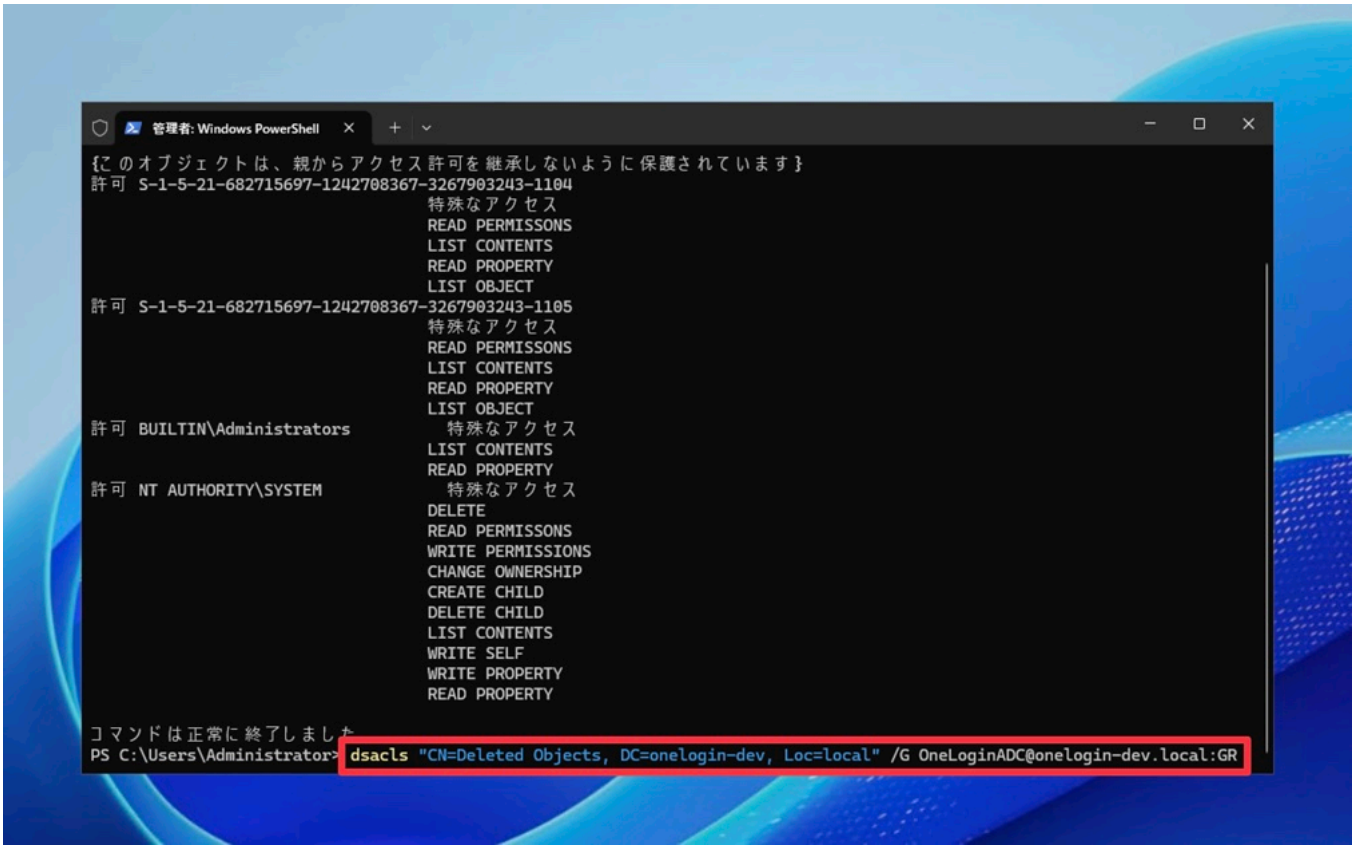
21. `dsacls "CN=Deleted Objects, <Your_Domain_DN_Here>" /G OneLoginADC@<Your_Domain>:GR`

の<Your_Domain_DN_Here>を **ドメイン識別名** に、<Your_Domain>を **ドメイン名** に置き換えて実行します

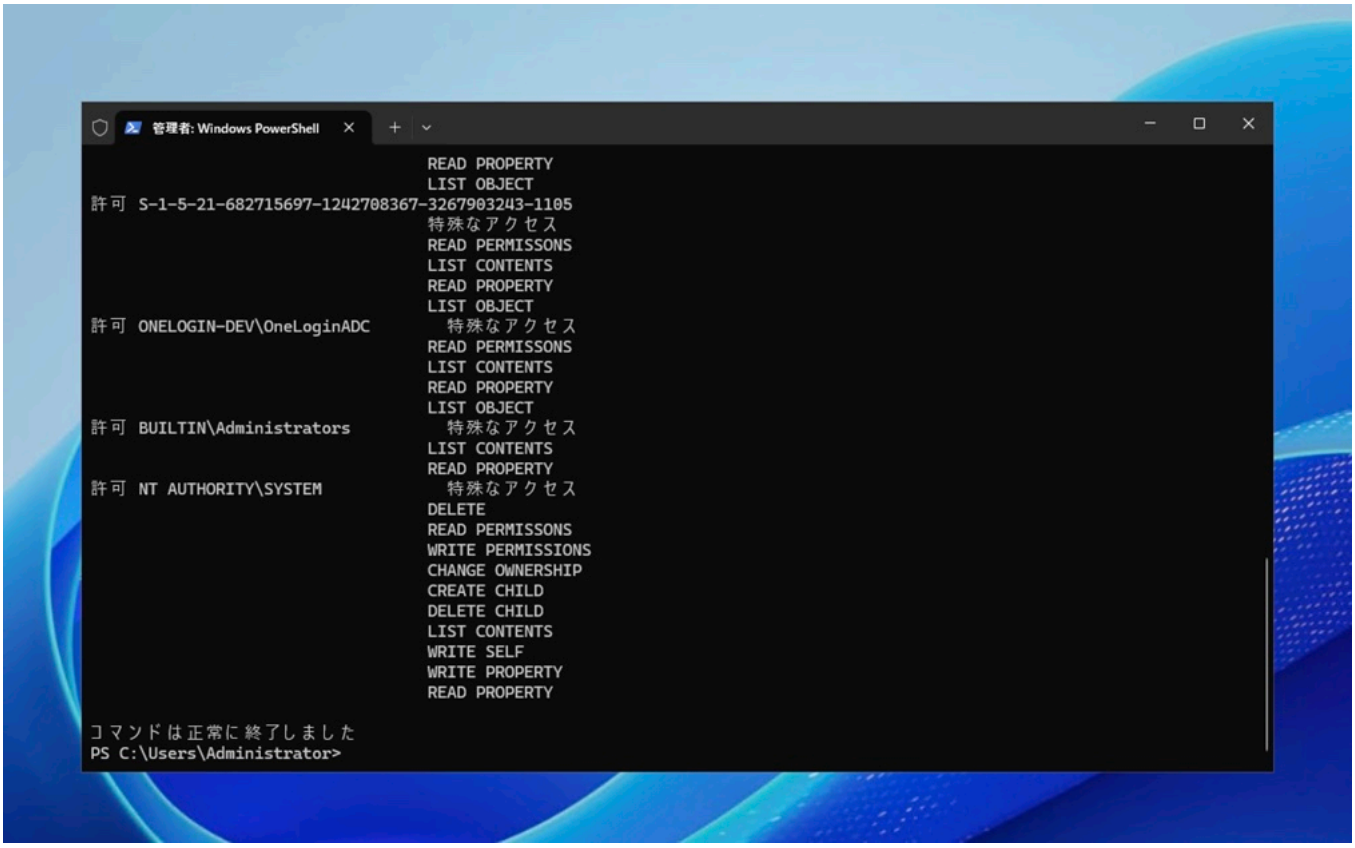
例）Active Directoryドメインが onelogin-dev.localの場合は、下記を実行します

```
dsacls "CN=Deleted Objects, DC=onelogin-dev, DC=local" /G OneLoginADC@onelogin-dev.local
```

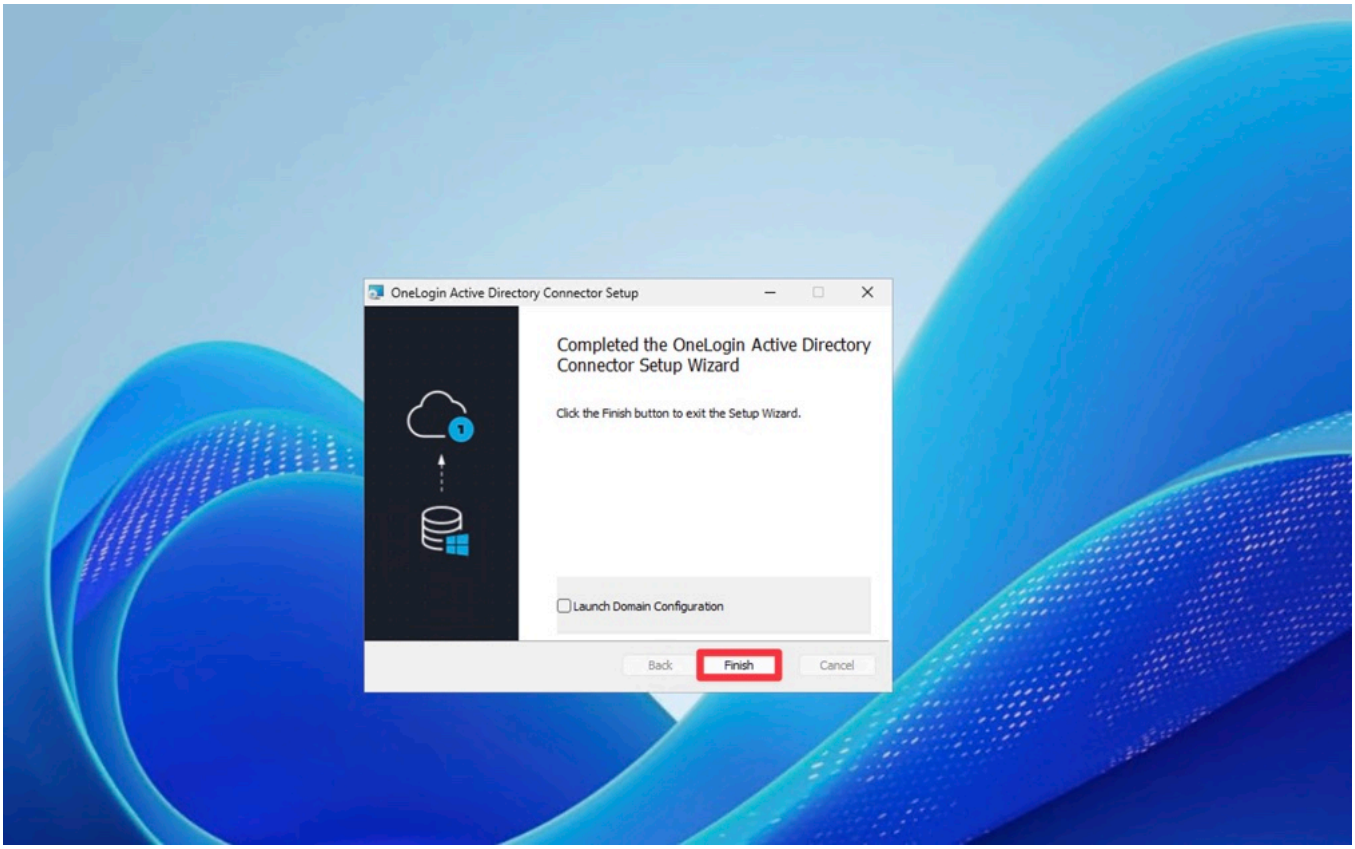
** ドメイン名、ドメイン識別名の確認方法はドメイン名とドメイン識別名の確認をご参照ください*



22. 同様に、**コマンドは正常に終了しました** と表示されることを確認します



23. ［**Finish**］をクリックします



OneLogin Active Directory ConnectorをWindows Serverにインストールする手順は以上です。

3. 同期対象OUを設定する

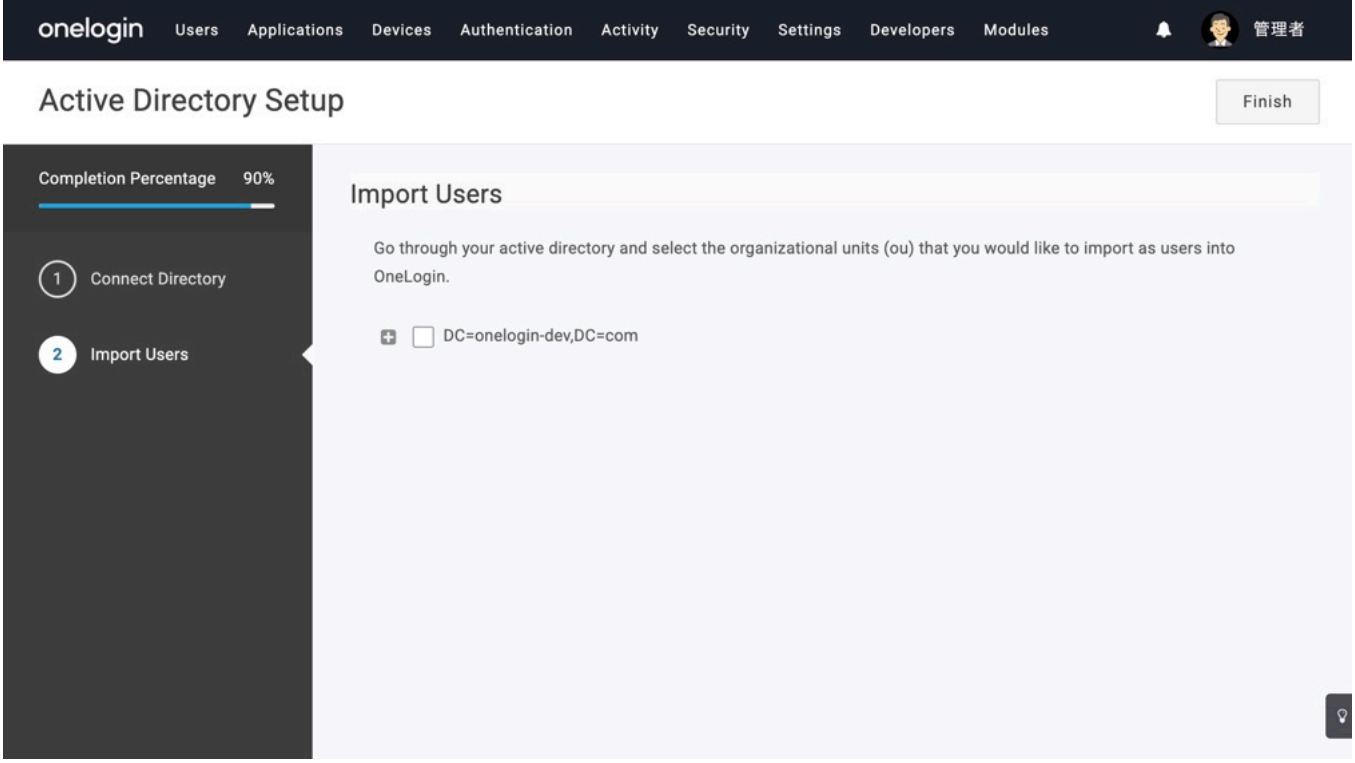
OneLoginのActive Directory 連携では、Base OUの指定とは別に同期対象OUの選択が可能です。同期対象OUの選択には以下の2通りが指定可能です。

a. 同期対象OU内の全ユーザーを同期する
b. 同期対象OU内の同期対象グループに所属する全ユーザーを同期する

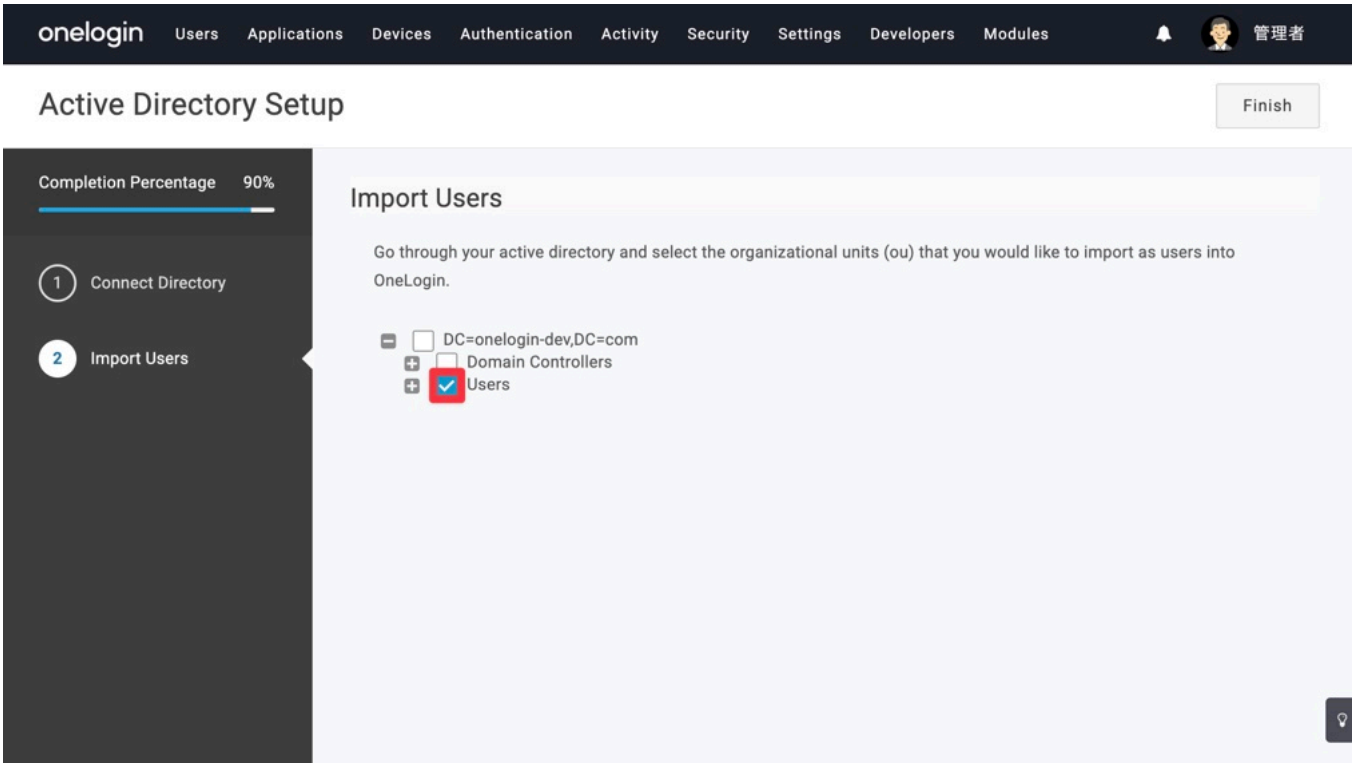
通常、a. 同期対象OU内の全ユーザーを同期する場合が多いですが、テスト運用時や、同期によりOneLoginのご契約ライセンス数を超過してしまう場合などはb. 同期対象OU内の同期対象グループに所属する全ユーザーを同期するを指定するケースもございます。

a. 同期対象OU内の全ユーザーを同期する

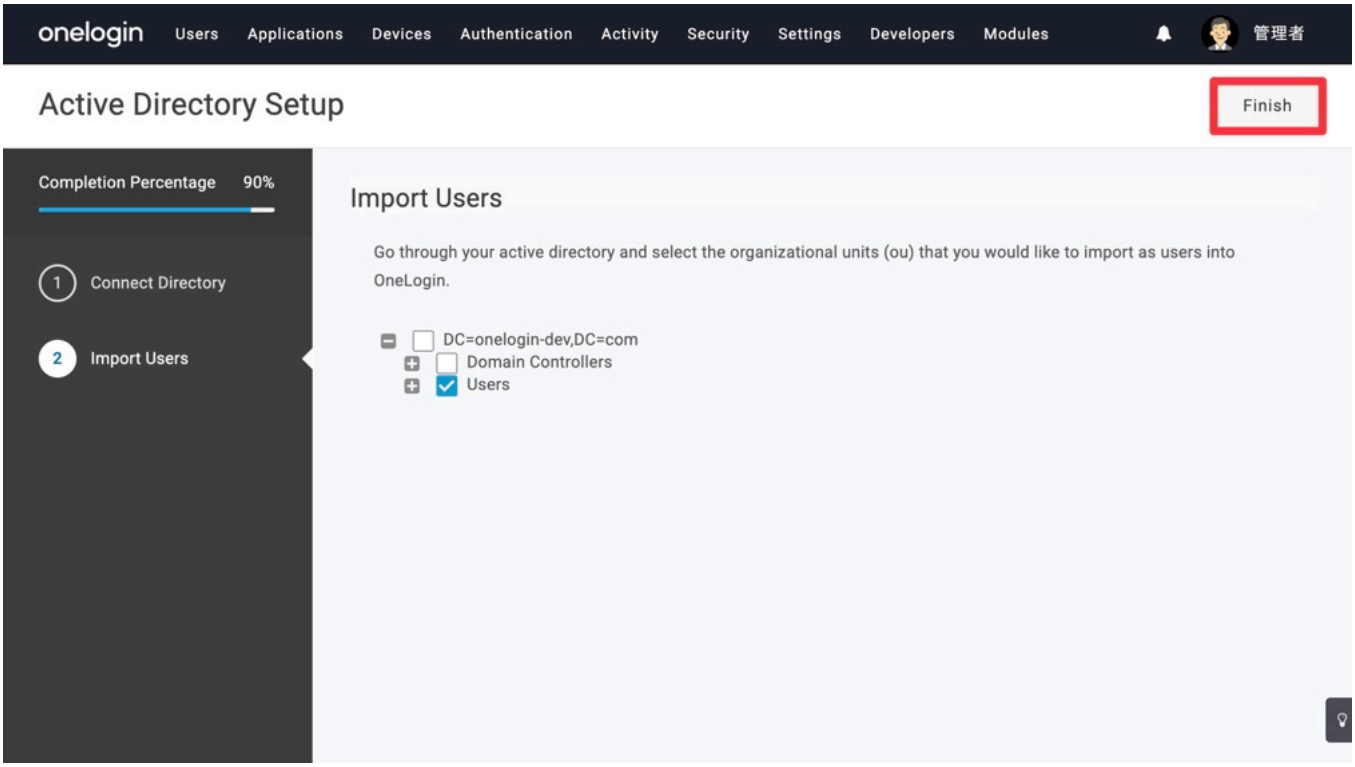
1. 1. OneLoginにディレクトリ連携設定を追加するで設定していた **Directory** を開き、同期するOUの選択の画面へ移動することを確認します
   ** こちらの画面に移動しない場合はページをリロードすることで移動する場合がございます*



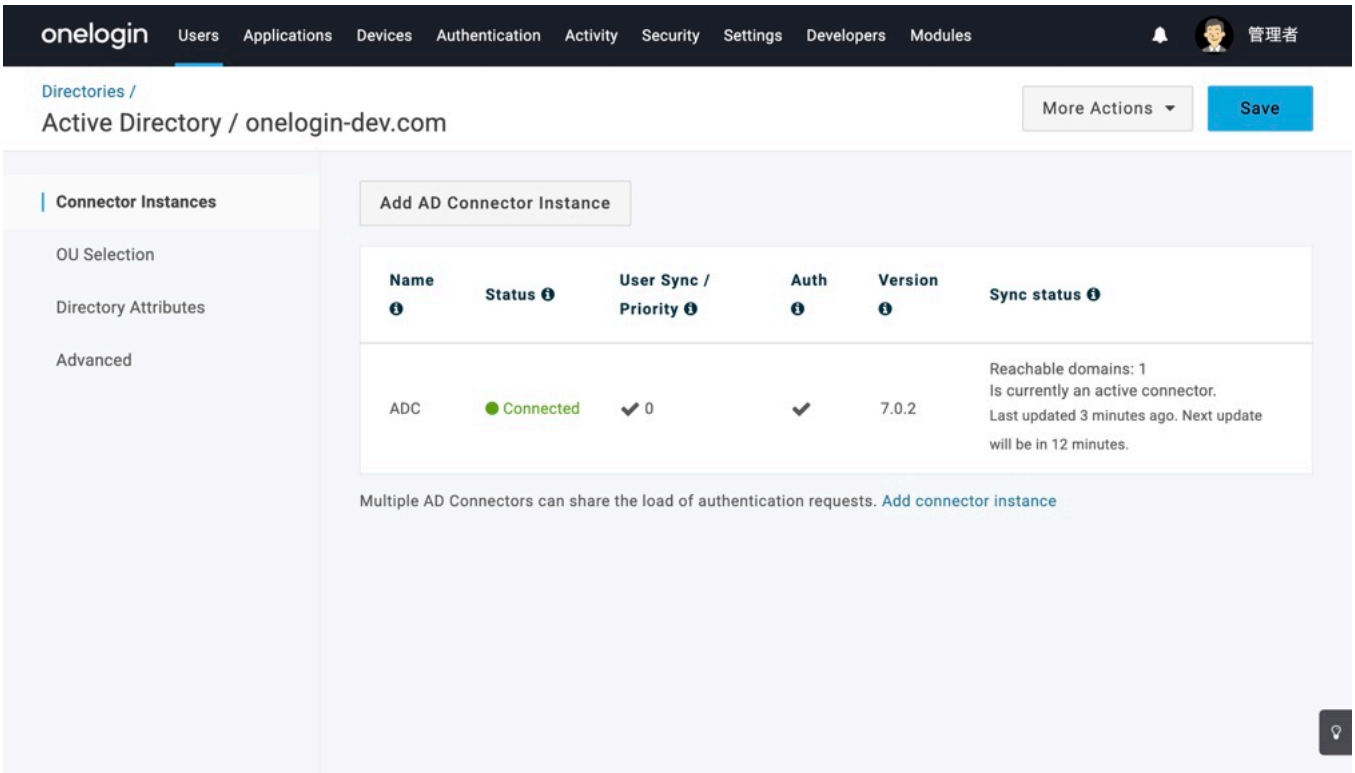
2. OUがツリー構造で表示されるため、同期の対象とするOUを選択します
例）Users



3. ［**Finish**］をクリックします

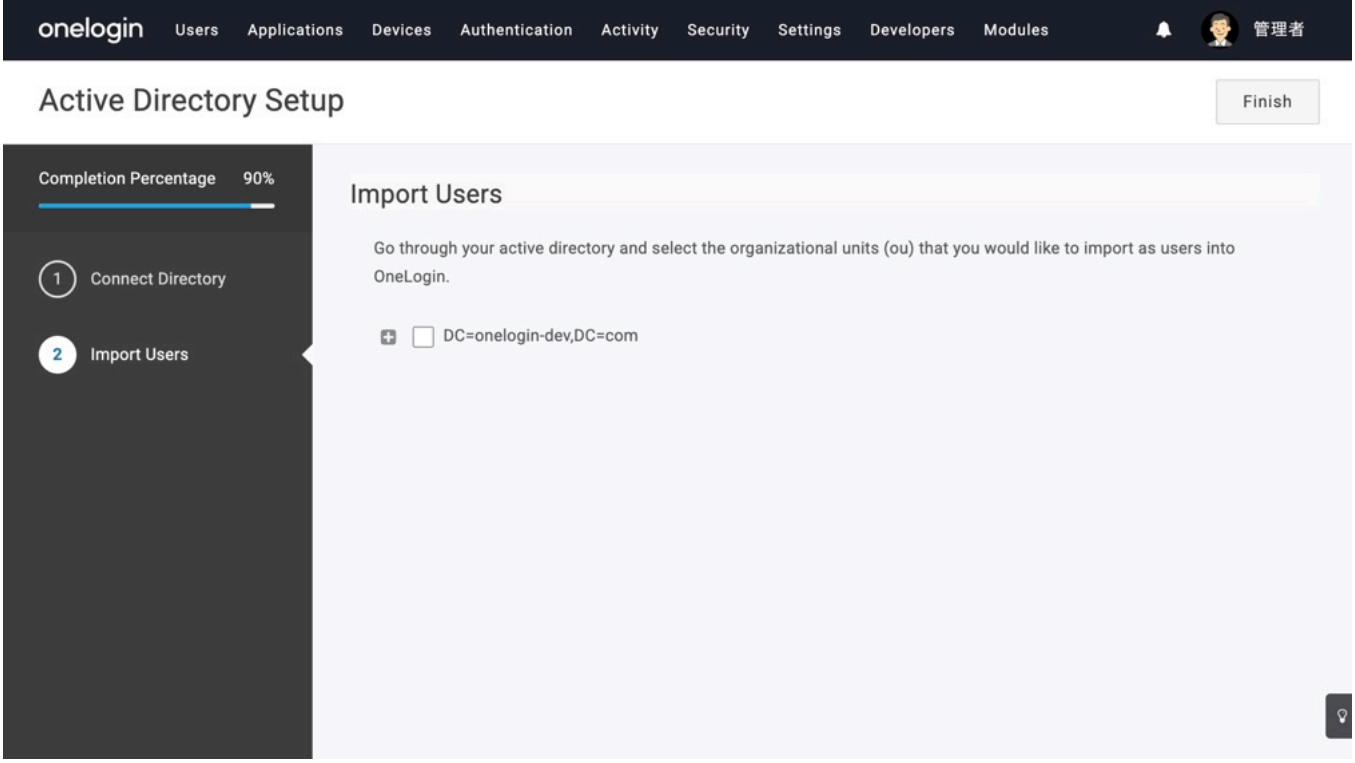


4. Statusが **Connected** と表示されていることを確認します。**Connected** と表示されていればActive Directoryとの連携が完了しユーザーの同期が開始されます
** 連携するユーザー数によっては時間がかかる場合がございます*

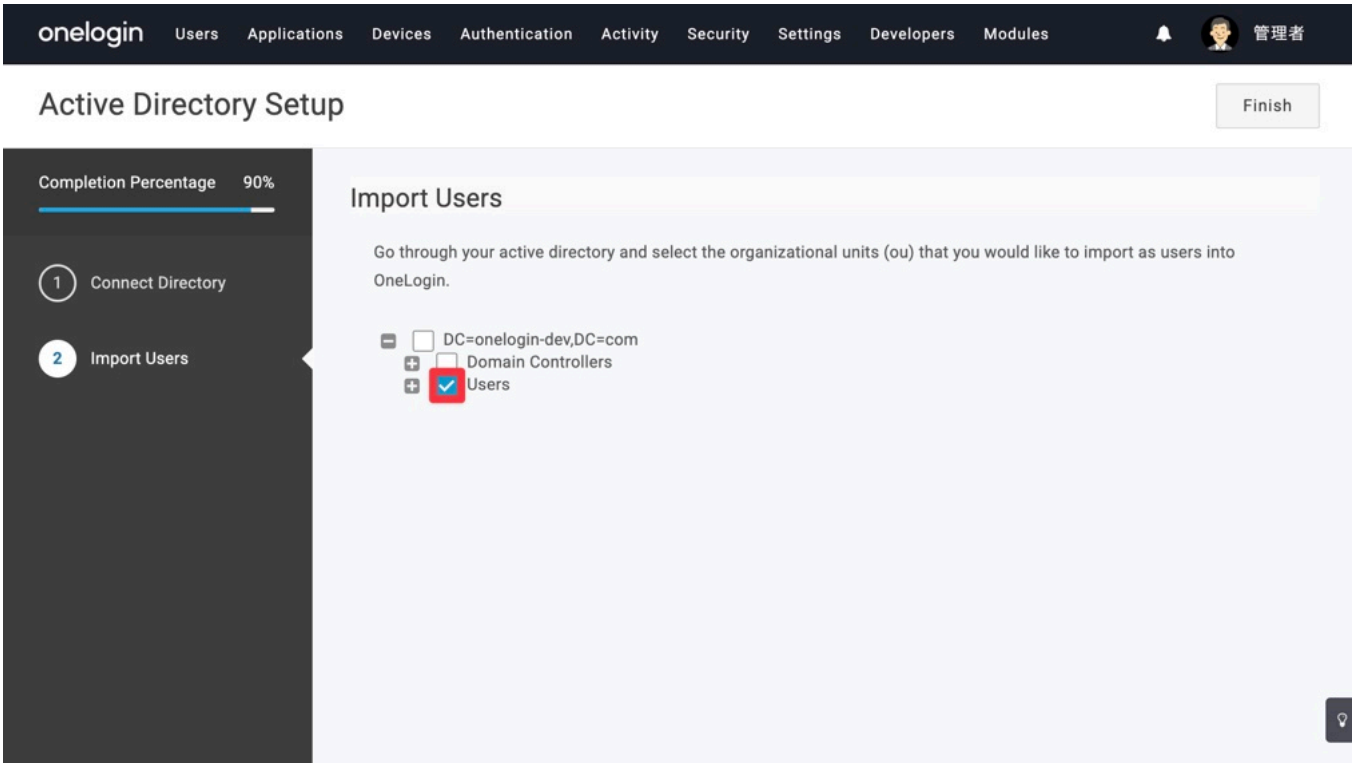


b. 同期対象OU内の同期対象グループに所属する全ユーザーを同期する

1. 1. OneLoginにディレクトリ連携設定を追加するで設定していたDirectoryを開き、同期するOUの選択の画面へ移動することを確認します
** こちらの画面に移動しない場合はページをリロードすることで移動する場合もございます*



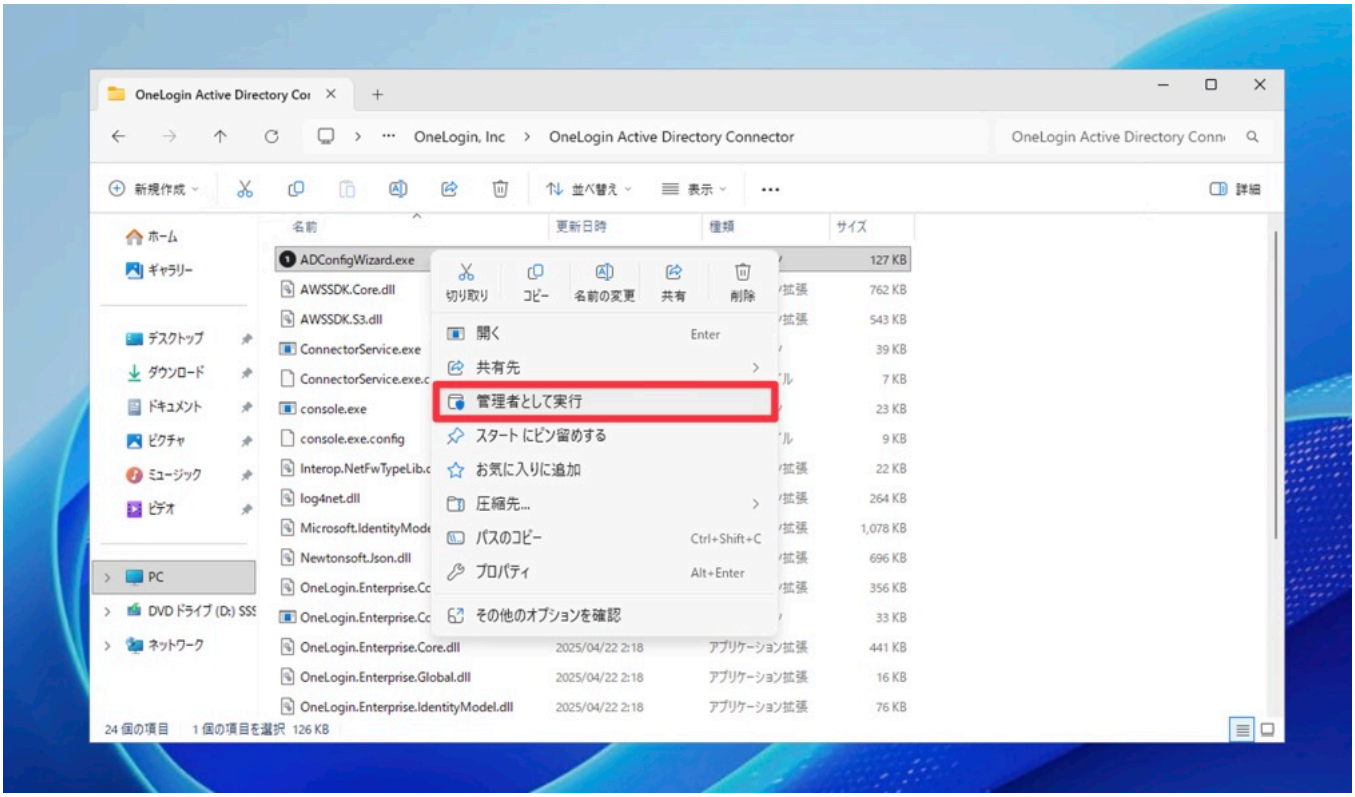
2. OUがツリー構造で表示されるため、同期の対象とするOUを選択します
   例）Users



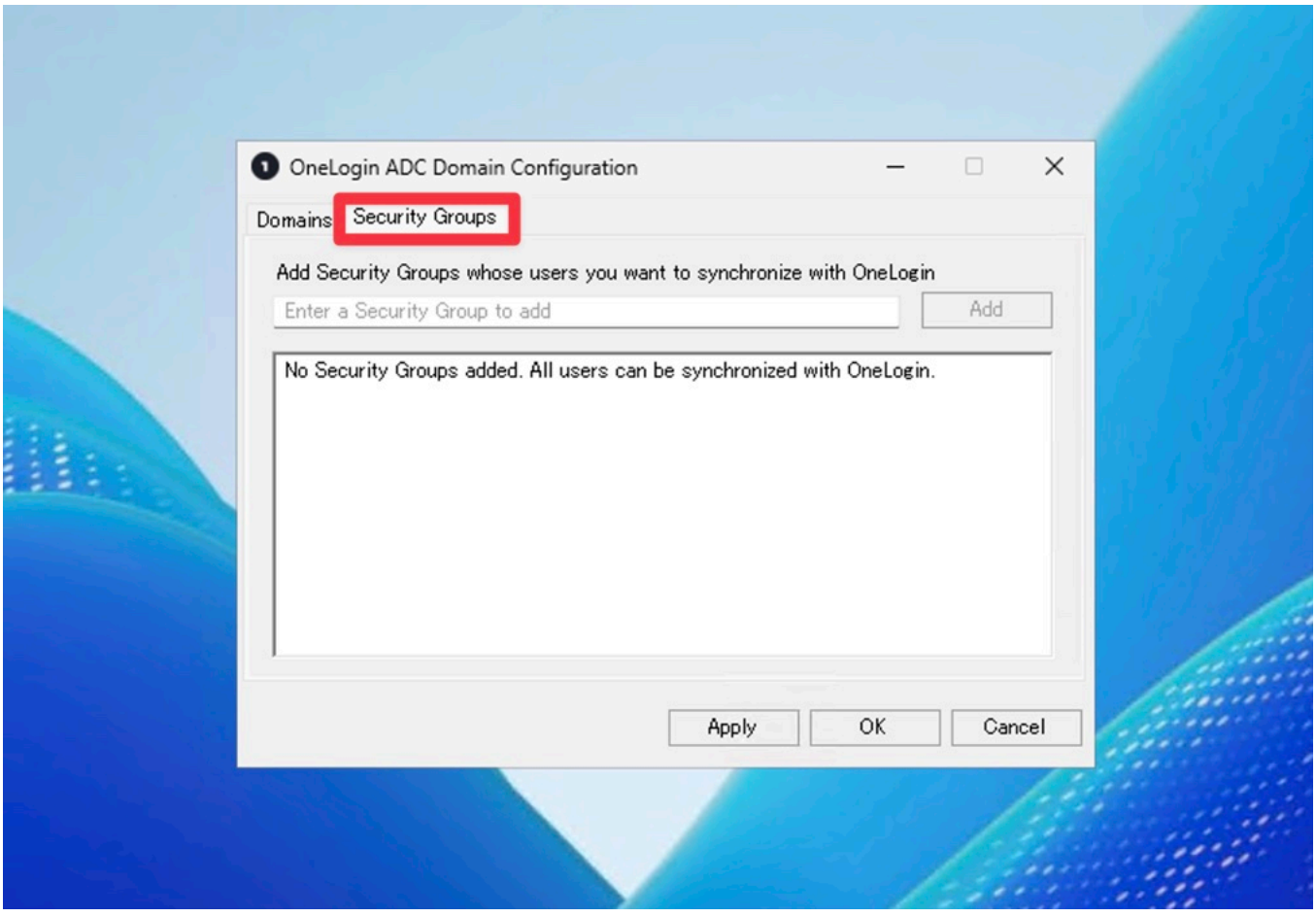
3. Active Directoryがインストールされたサーバーへ接続し、以下を管理者で実行します

```
C:\Program Files (x86)\OneLogin, Inc\OneLogin Active Directory Connector\ADConfigWizard.
```

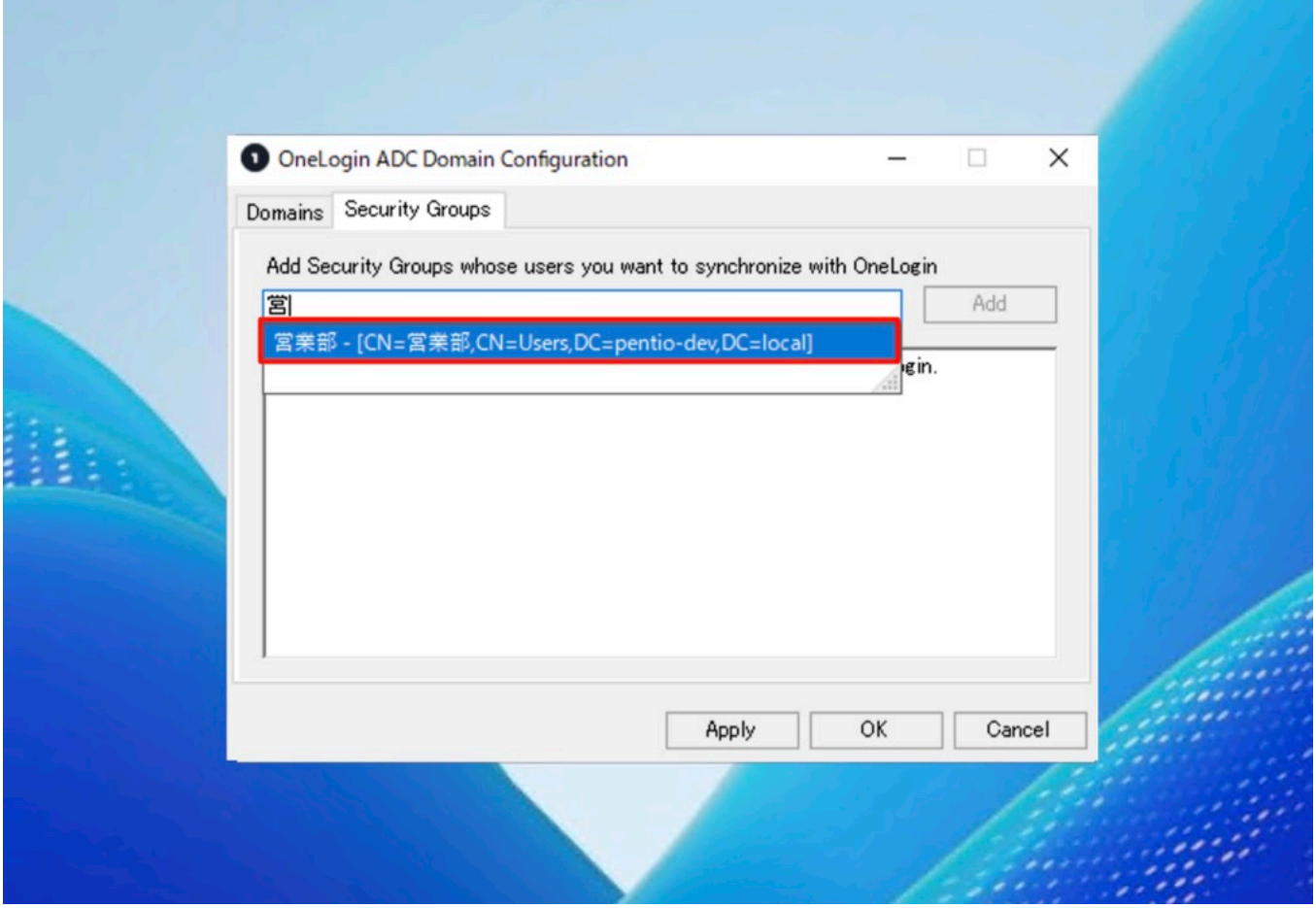
** 環境によりパスは異なる場合がございます*



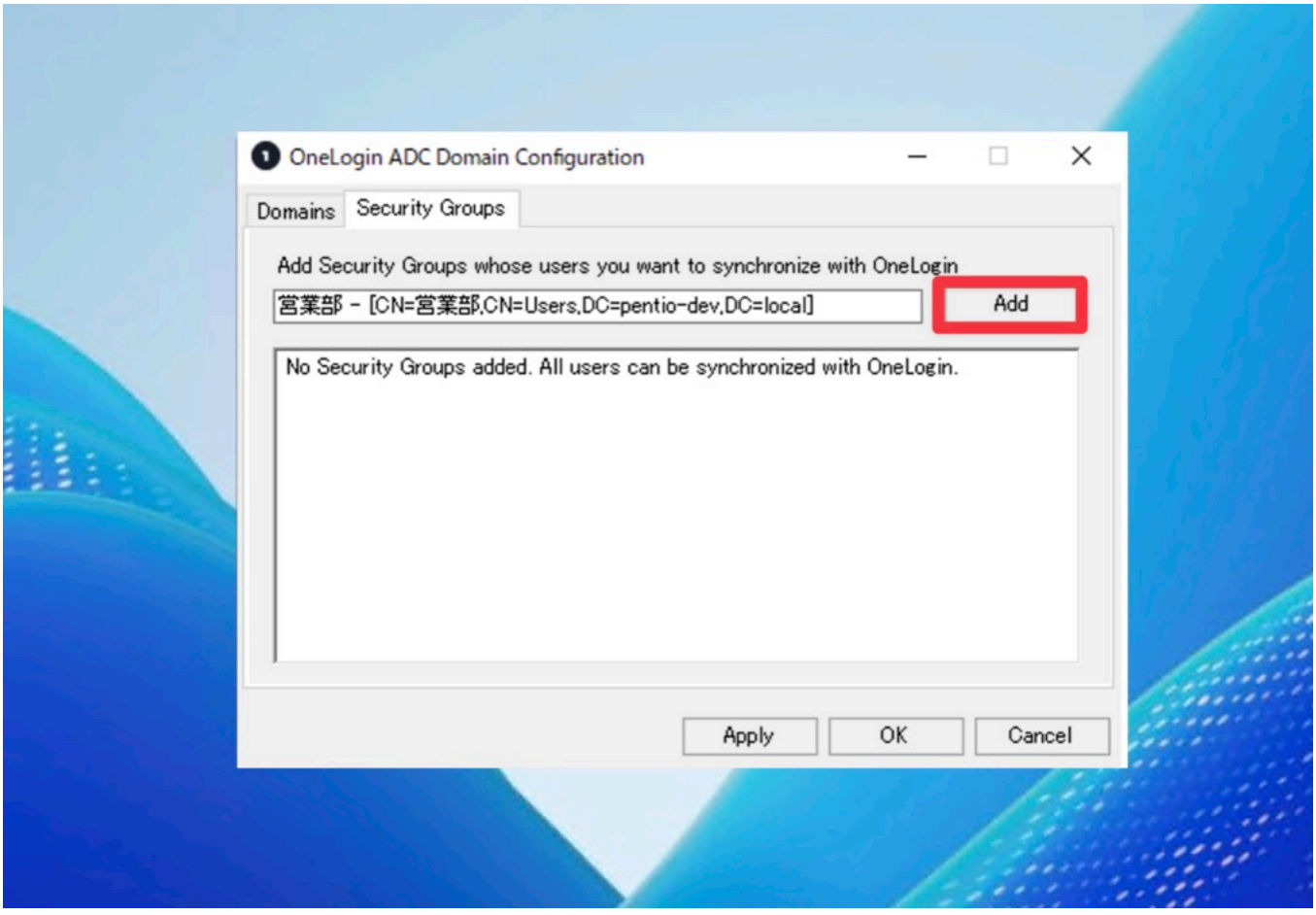
4. ［**Security Groups**］をクリックします



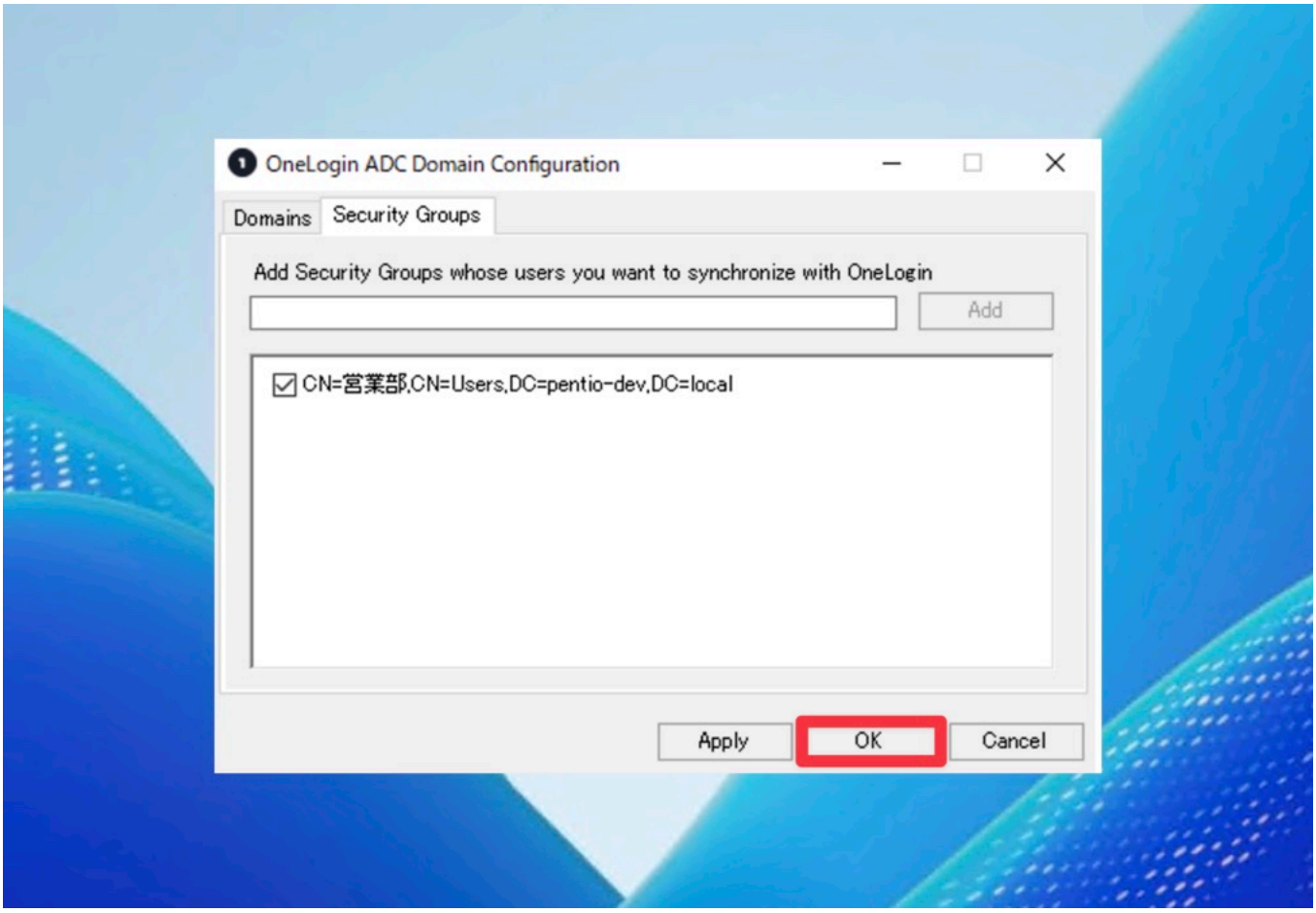
5. 検索窓にユーザーが所属するグループの名称を入れ入力補完により表示されたグループから対象のグループを選択します



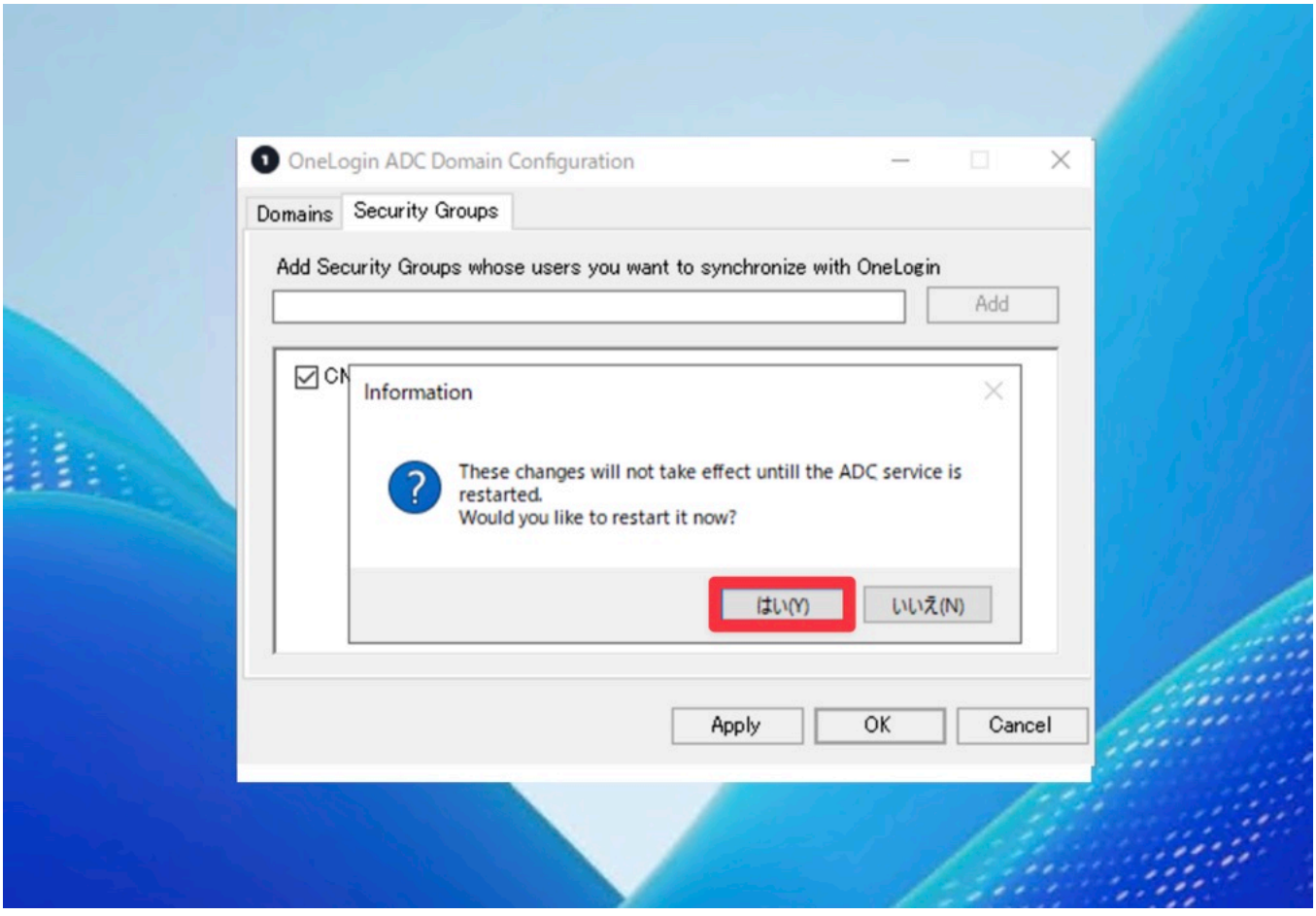
6. ［**Add**］をクリックします



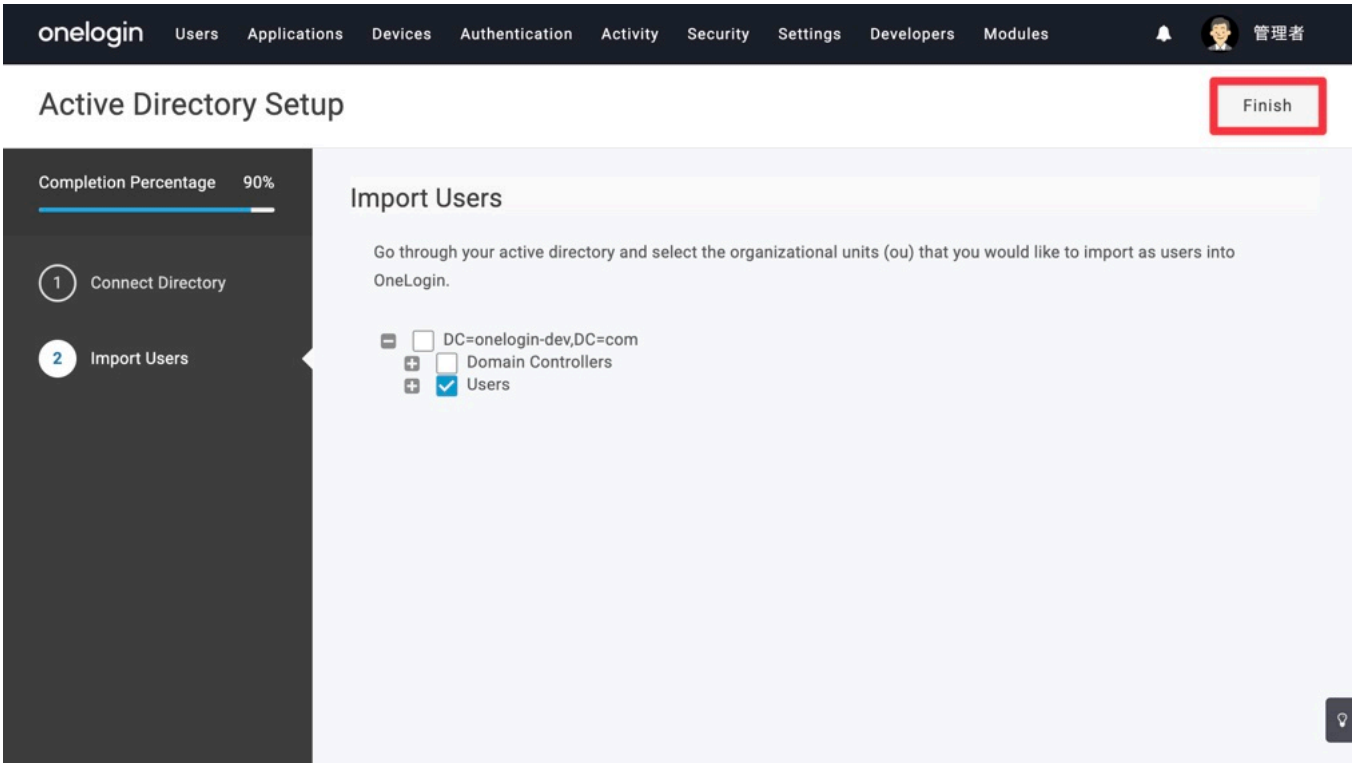
7. ［**OK**］をクリックします



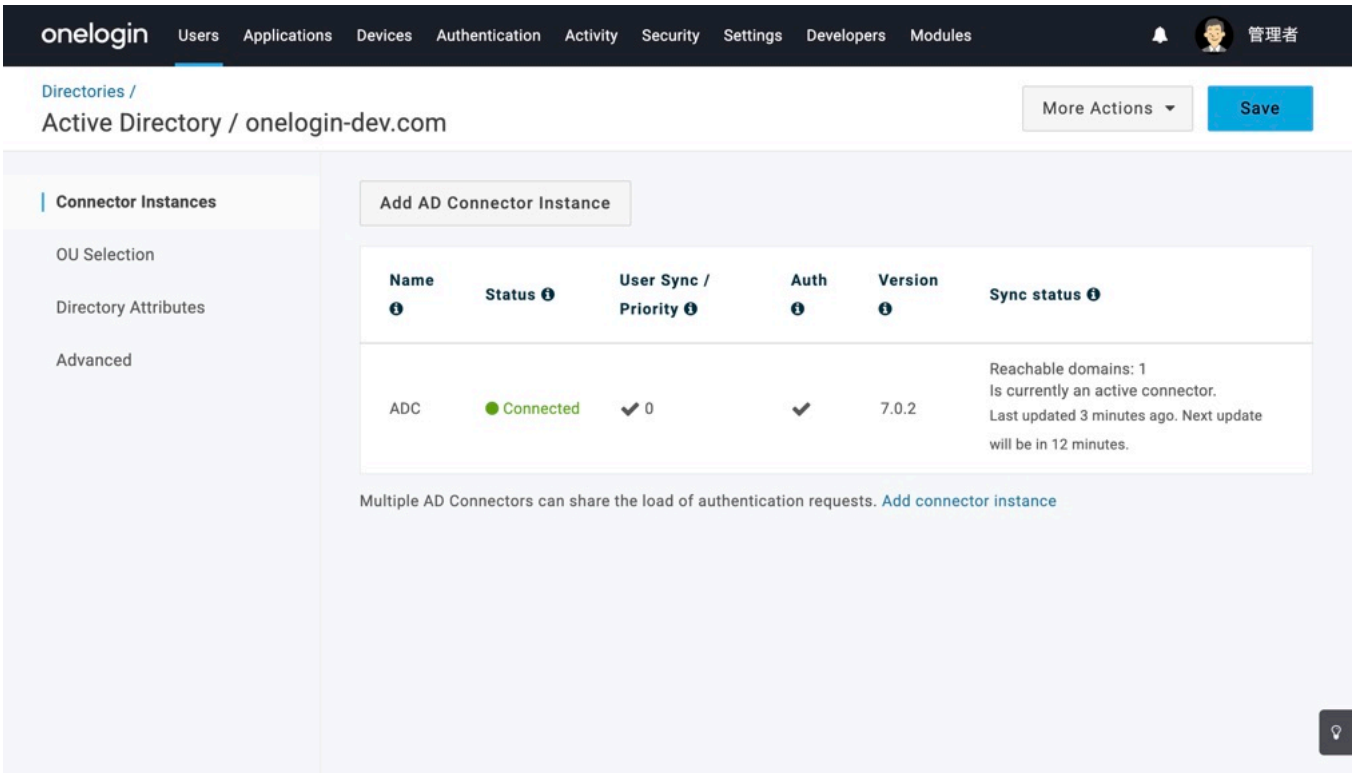
8. 表示されたポップアップで［**はい**］をクリックします



9. OneLoginのDirectory設定に戻り、［**Finish**］をクリックします



10. Statusが **Connected** と表示されていることを確認します。**Connected** と表示されていればActive Directoryとの連携が完了しユーザーの同期が開始されます
** 連携するユーザー数によっては時間がかかる場合がございます*

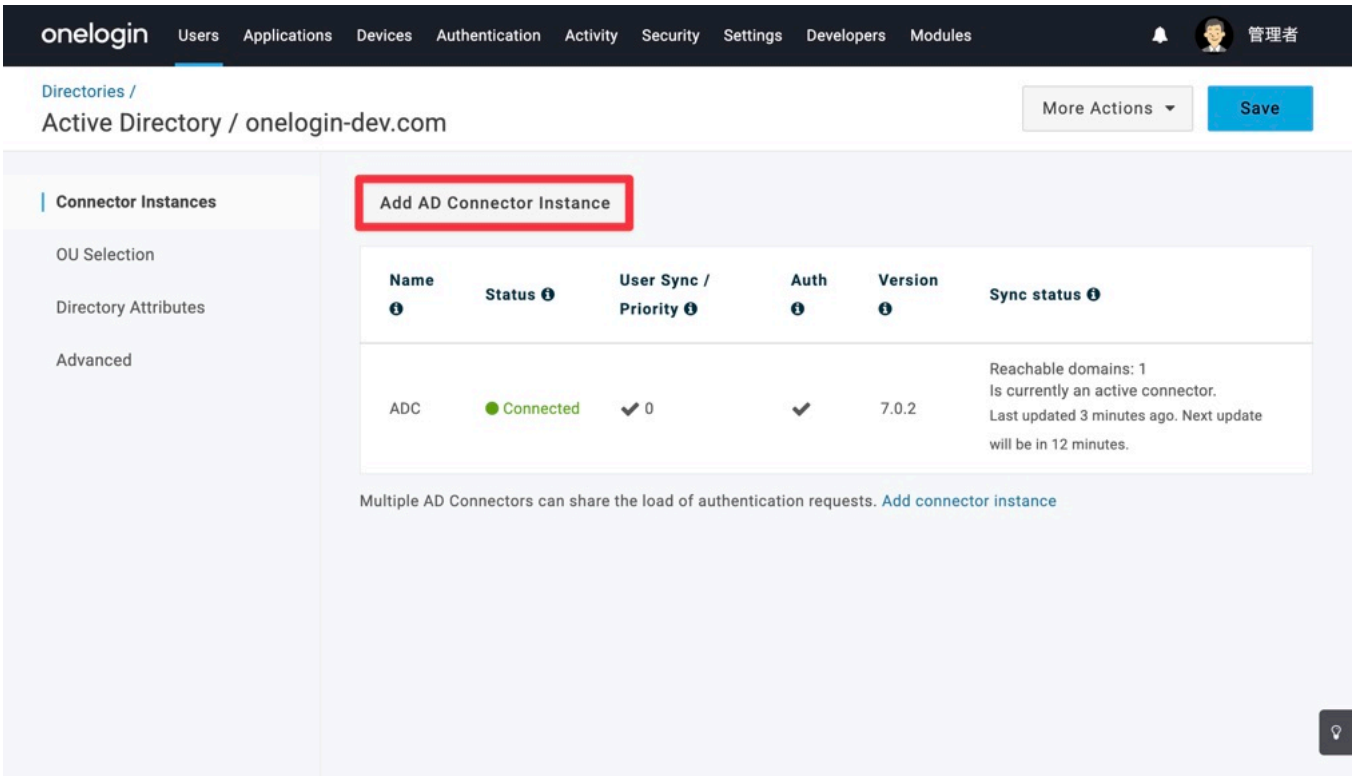


同期対象OUを設定する手順は以上です。

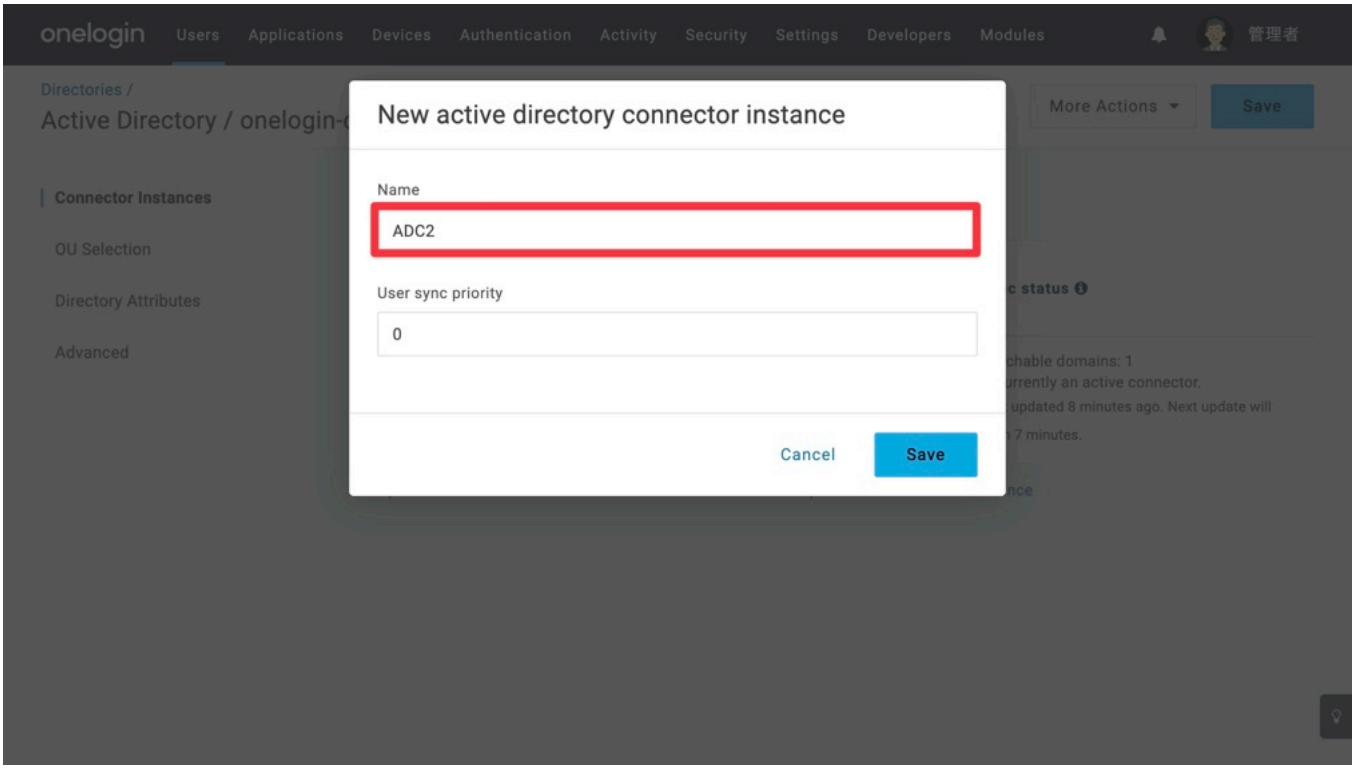
4. セカンダリサーバーを追加する（オプション）

ここでは、認証・同期の冗長化を目的として複数台のActive Directoryインスタンスの接続を追加する方法を解説いたします。

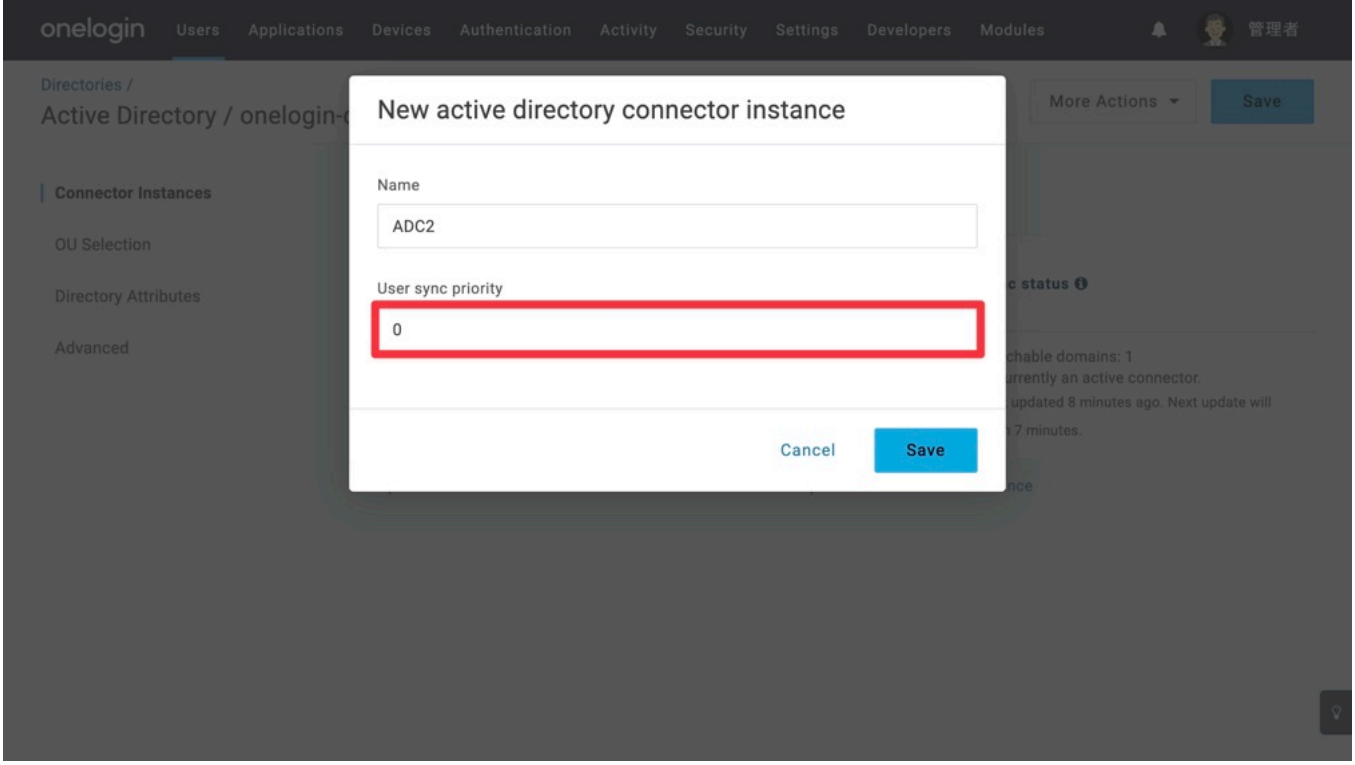
1. ［**Add AD Connector Instance**］をクリックします



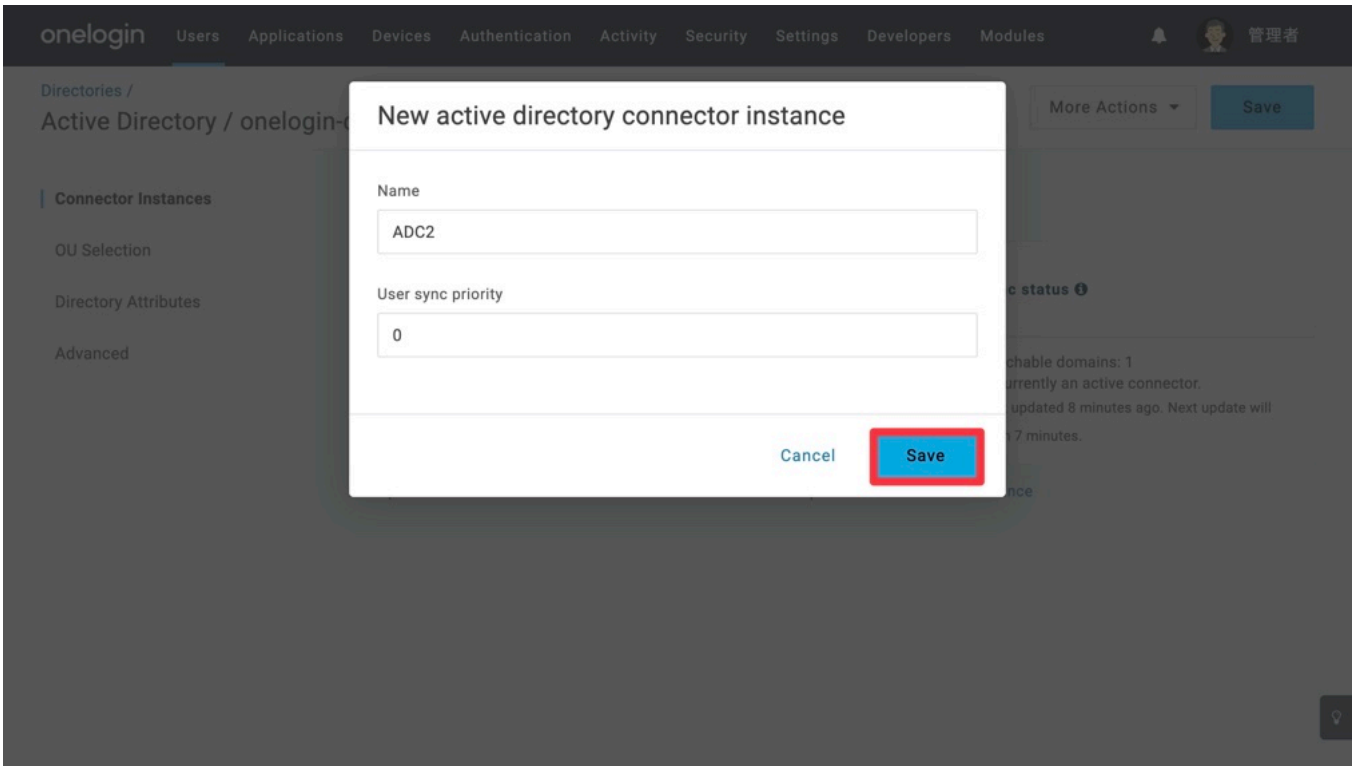
2. **Name** にインスタンスを識別する名前を入力します
   例）ADC2



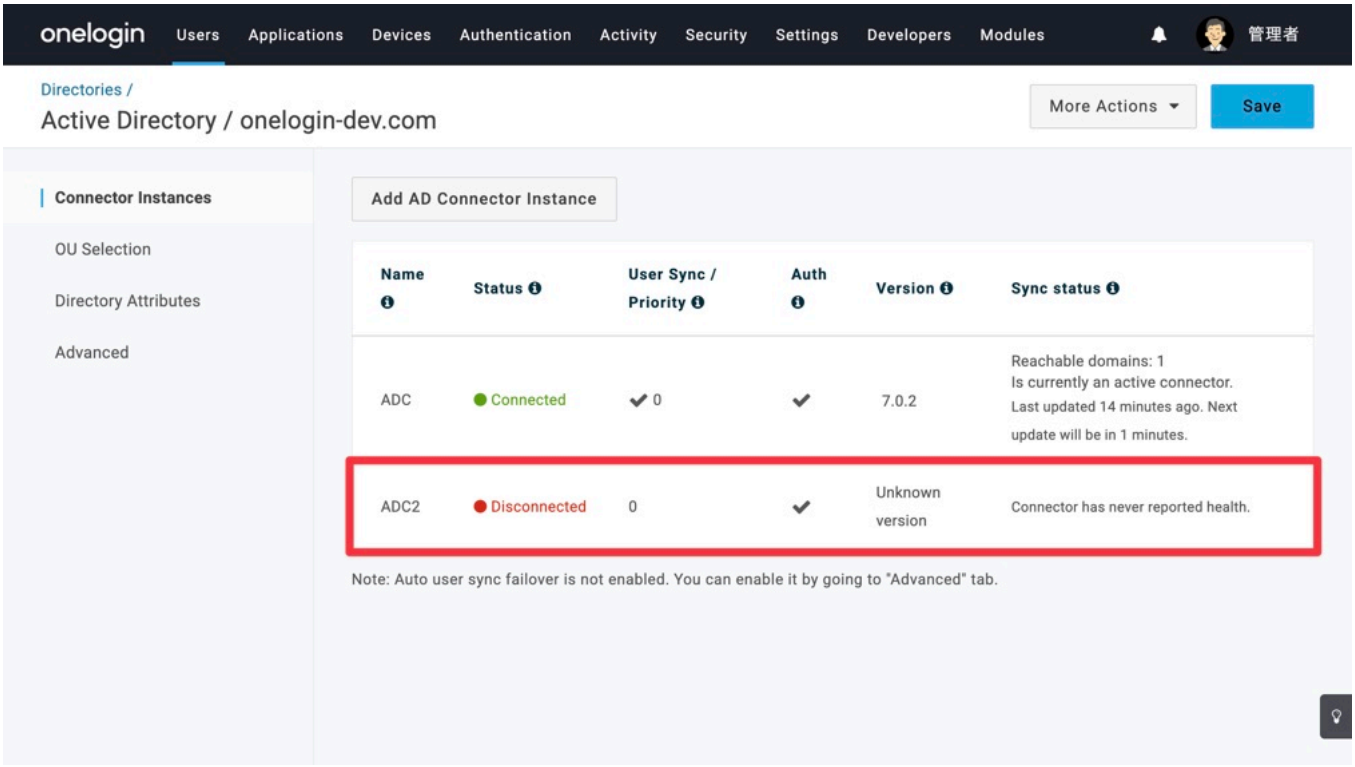
3. **User sync priority**で優先度を設定します
   例）0
   ** 設定項目の詳細は Connector Instancesタブの各項目について をご覧ください*



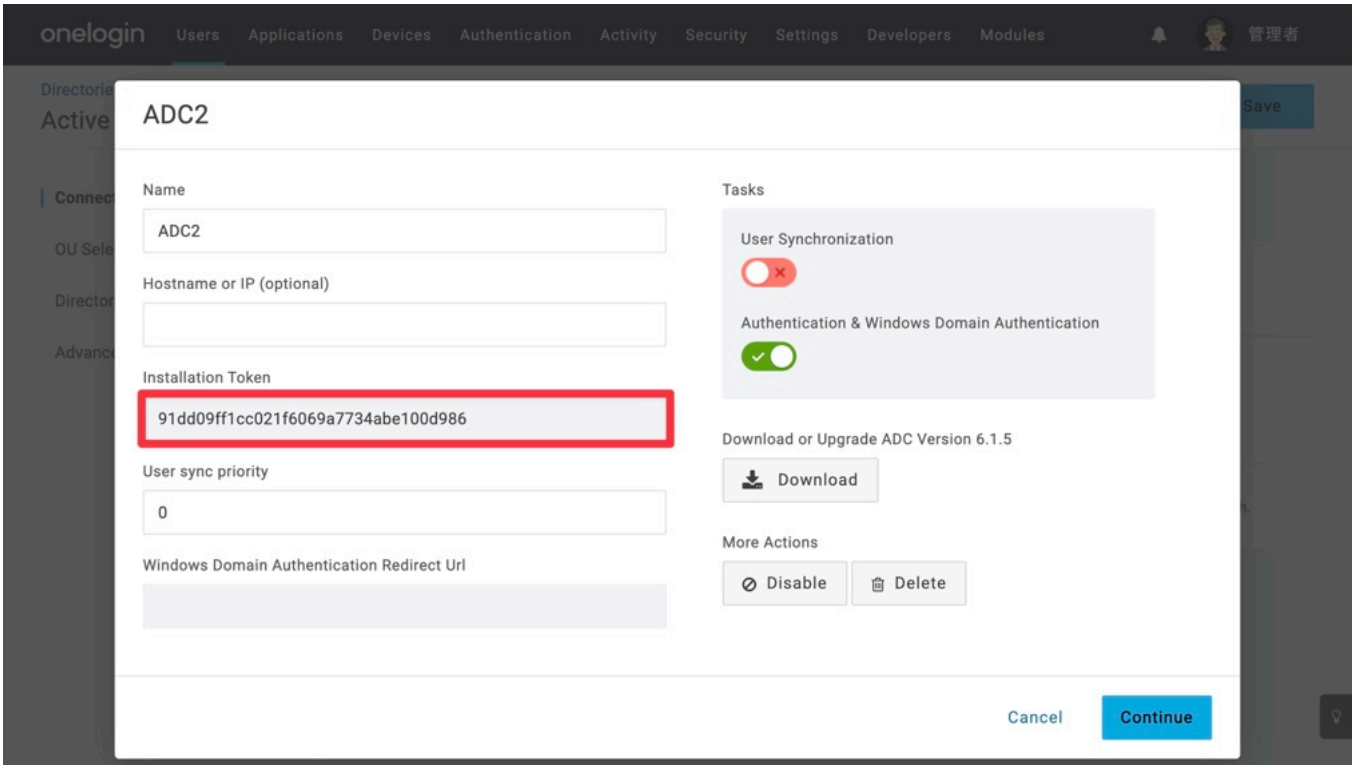
4. ［**Save**］をクリックします



5. 作成したインスタンスをクリックします



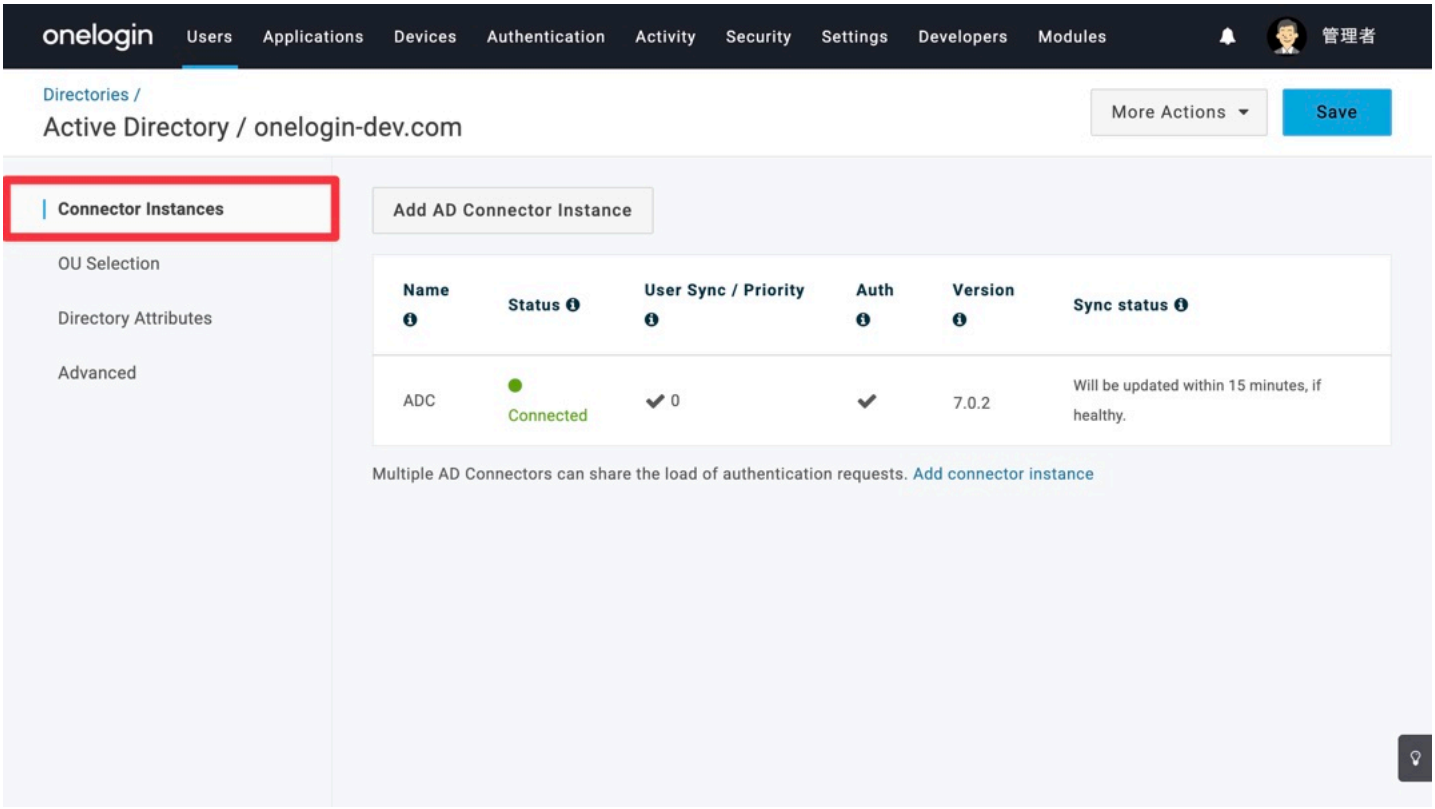
6. **Installation Token** をコピーし、2. OneLogin Active Directory ConnectorをWindows Serverにインストールするを参考に設定を進めます



セカンダリサーバーを追加する手順は以上です。

Connector Instancesタブの各項目について

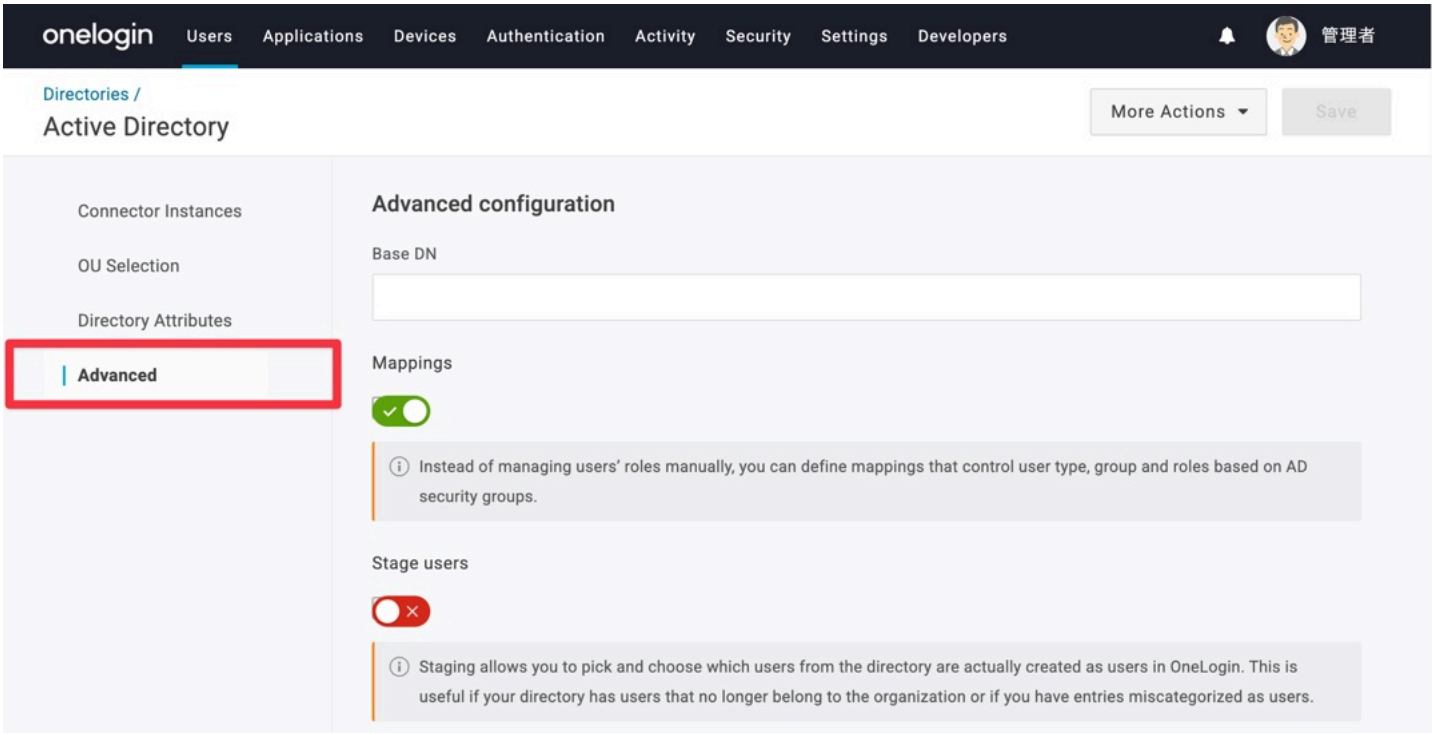
本章では、Connector Instancesタブの各項目について解説いたします。



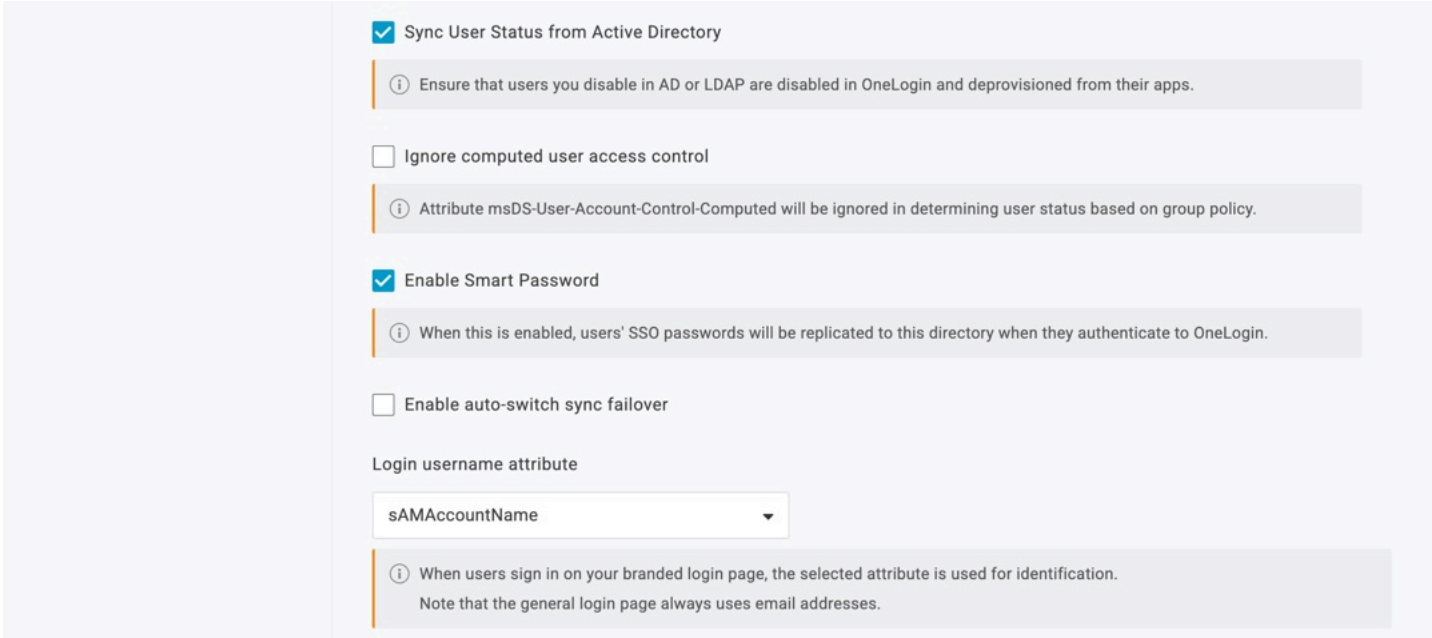
- ［**Add AD Connector instance**］
  Active Directoryインスタンスの追加を行います。詳細は4. セカンダリサーバーを追加する（オプション）をご参照ください
- **Name**
  OneLogin管理画面上でActive Directoryを識別するインスタンス名を表します
- **Status**
  OneLogin ADCとOneLogin間の接続状態を表します。各Statusの状態は以下の通りです
  1. **Connected** : OneLogin ADCとOneLogin間の通信が正常に確立している状態
  2. **Disconnected** : OneLogin ADCとOneLogin間の通信が未確立、または切断されている状態
- **User Sync / Priority**
  ☑ が表示されているインスタンスは、現在ユーザー同期を担当していることを表します
  数字は、ユーザー同期を担当しているインスタンスが利用できなくなった場合に、他のインスタンスへ同期処理を切り替える際の優先度を表します。数字が大きいインスタンスほど優先度が高くなります
- **Auth**
  ☑ が表示されているインスタンスは、Active Directoryの認証要求を処理するインスタンスであることを表します
- **Version**
  接続しているOneLogin ADCのバージョンを表します
- **Sync status**
  ユーザー同期に関するステータス情報を表します

ディレクトリ連携のアドバンスド設定を行う

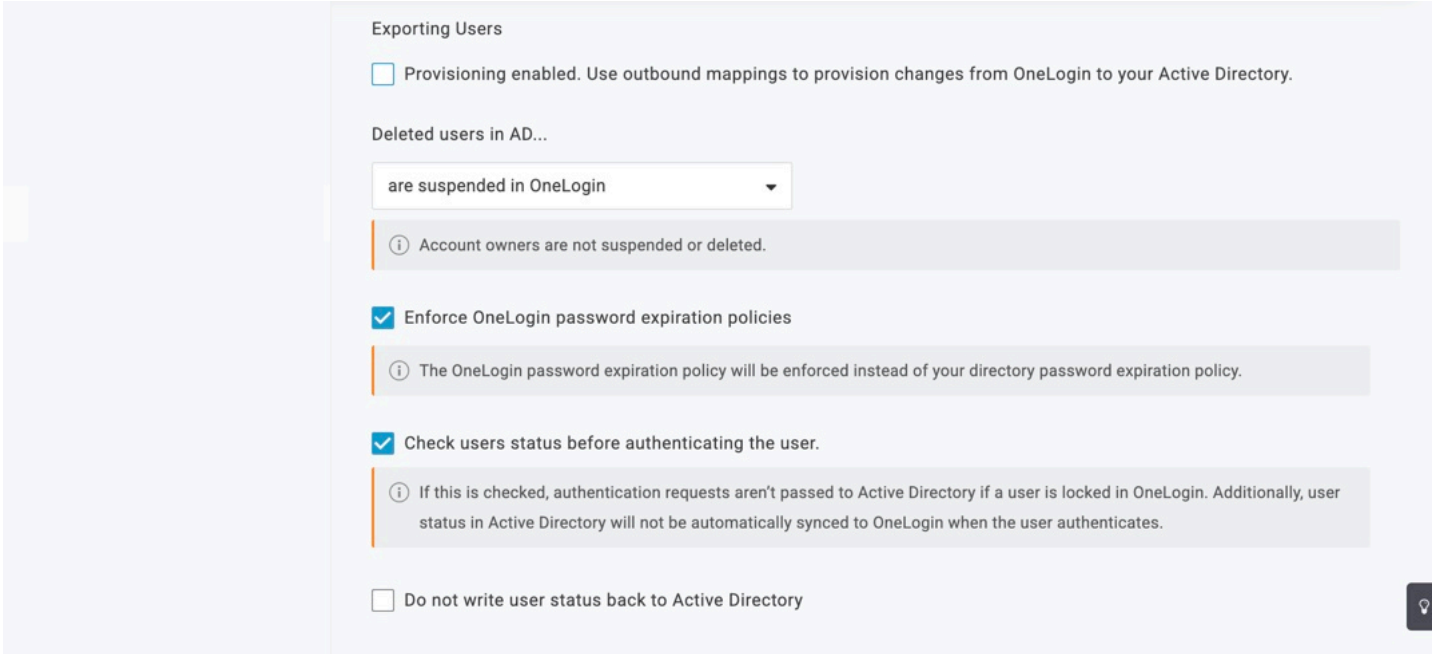
ディレクトリ連携のうち、**Advanced** タブ内では以下の詳細な設定が可能です。



- **Base DN**
  OneLogin ADC Version 3.x以降は廃止されたためご設定いただく必要はございません
- **Mapping**
  有効にすることで、設定中のActive Directoryから同期されたユーザーに対してもMapping機能を実行します。
  デフォルト: 有効
  推奨: 有効
- **Stage users**
  有効にすることで、設定中のActive Directoryから同期されたユーザーのアクティベートに管理者の手動承認が求められます
  デフォルト: 無効
  推奨: 無効



- **Sync User Status from Active Directory**
  有効にすることでActive Directory側のユーザーステータスの同期を行います
  デフォルト: 無効
  推奨: 有効
- **Ignore computed user access control**
  Windows Server 2003以降は廃止されたためご設定いただく必要はございません
- **Enable Smart Password**
  有効にすることで、他ディレクトリからユーザーのパスワードを取得し、設定中のActive Directoryのユーザーのパスワードを上書きすることを許可します
  デフォルト: 無効
  推奨: 無効
  詳しくはSmart Passwordsをご覧ください
- **Enable auto-switch sync failover**
  有効にすることで、複数のActive Directoryインスタンスを登録している際に、プライマリインスタンスと疎通が取れなくなった場合に自動でユーザー同期をセカンダリインスタンスにフェイルオーバーします
  デフォルト: 無効
  推奨: 有効
- **Login username attribute**
  プルダウンで選択した項目がOneLoginのユーザーのUsernameとして同期されます
  デフォルト: Email
  推奨: sAMAccountName



- **Provisioning enabled. Use outbound mappings to provision changes from OneLogin to your Active Directory.**
  有効にすることで、OneLoginから設定中のActive Directoryへユーザープロビジョニングを行います
  ** ご利用の場合、設定のミスなどで致命的な不具合が発生する可能性がありますので、有効にする場合は有償のプロフェッショナルサービスをご活用ください*
  デフォルト: 無効
  推奨: 無効

- **Deleted users in AD...**
  Active Directoryでユーザーを削除した際にOneLogin側のアカウントをどのように処理するかを決定します

  are unaffected in OneLogin: ユーザーは変更せずに、連携を切断する
  are suspended in OneLogin : OneLoginのユーザーを無効化
  are deleted in OneLogin : OneLoginのユーザーも削除

  デフォルト: are unaffected in OneLogin
  推奨: are deleted in OneLogin

  Active Directoryとのディレクトリ連携におけるユーザーの削除は以下の3パターンです
  1. Active Directoryでユーザーを削除した場合
     Active Directoryの管理画面からユーザーオブジェクトを完全に削除した場合
  2. Security Groupから外れた場合
     b. OU内の特定のグループに所属するユーザーを同期するの設定を行った場合に、ユーザーがそのグループから外れた場合
  3. 同期対象外のOUに移動した場合
     a. 同期対象OU内の全ユーザーを同期するの **OU Selection** タブでチェックを入れていないOUへユーザーを移動した場合
- **Enforce OneLogin password expiration policies**
  有効にすることで、OneLoginにログインする際に、パスワードの失効判定にOneLogin側のパスワードポリシーが適用されます
  デフォルト: 有効
  推奨: 無効
- **Check users status before authenticating the user.**
  有効にすることで、Active Directoryでの認証前にOneLogin側のユーザーステータスを確認し、ロックされている場合は認証のリクエストを送信しなくなります
  デフォルト: 有効
  推奨: 有効
- **Do not write user status back to Active Directory**
  有効にすることで、Active Directory側のステータスに関わらず、OneLogin側のステータスをOneLogin側で管理することができます
  デフォルト: 有効
  推奨: 無効

高度な設定について

プロキシ認証、HA構成（ロードバランシング・フェイルオーバー）、Windows Domain Authentication（統合 Windows 認証）については担当営業またはサポートにご相談ください。有償のプロフェッショナルサポートで充実した導入支援をご提供しております。

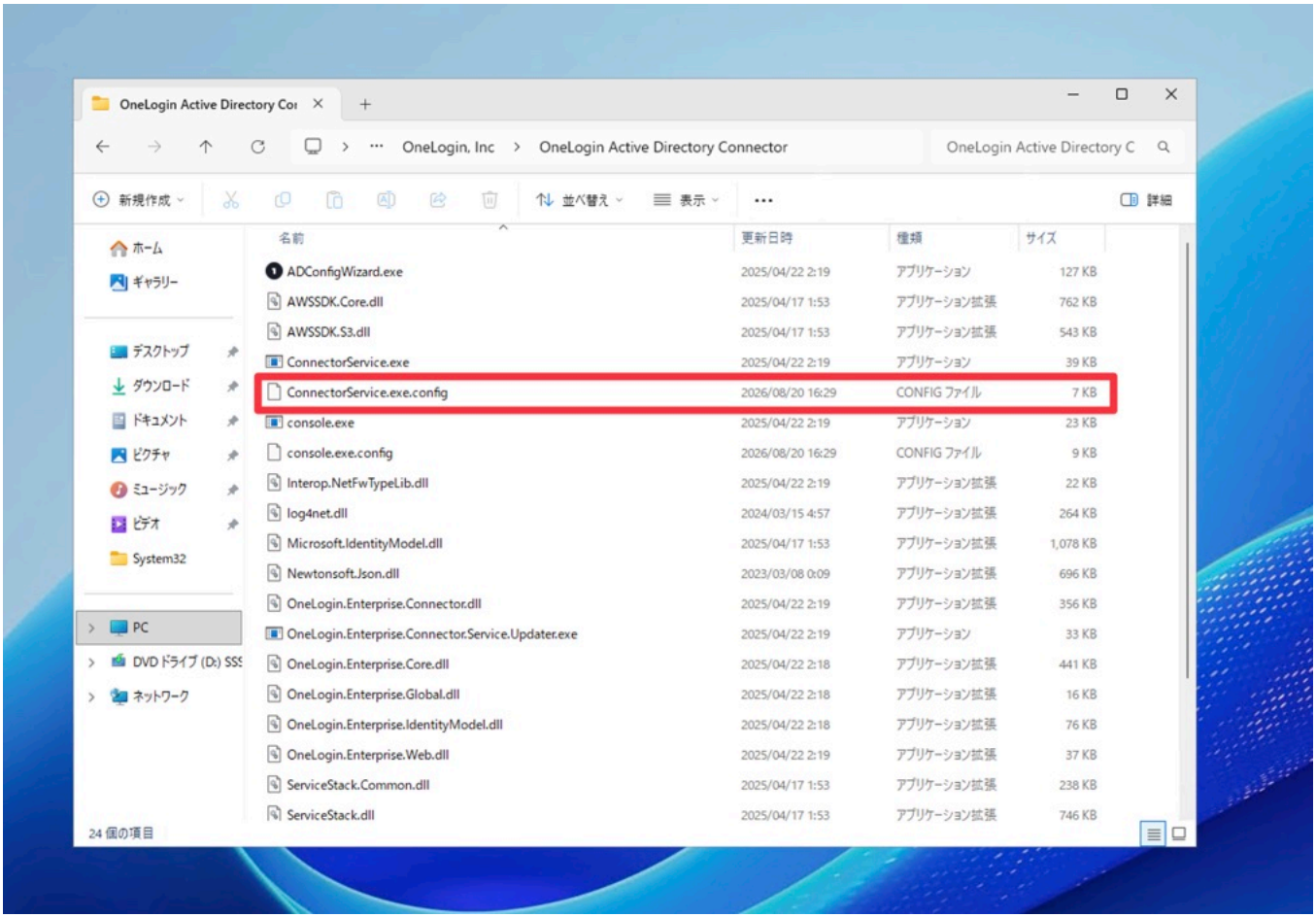
ユーザー同期間隔の変更

OneLogin ADCはリアルタイムの同期に加え、デフォルトでは15分毎に通信エラー等で取りこぼした変更を確実に反映させるためディレクトリ全体の同期が自動実行されます。
同期の対象となるユーザーが非常に多い場合などは、一度の全体同期に15分以上かかってしまうケースがございます。これにより、システムの不具合やさらなる遅延が発生する可能性があります。これを防ぐため、余裕を持って一度の全体同期を完了できる時間に全体同期の間隔を伸ばす必要がございます。

1. Active Directoryが稼働するサーバーへ接続し、以下のファイルを管理者として、メモ帳等で開きます

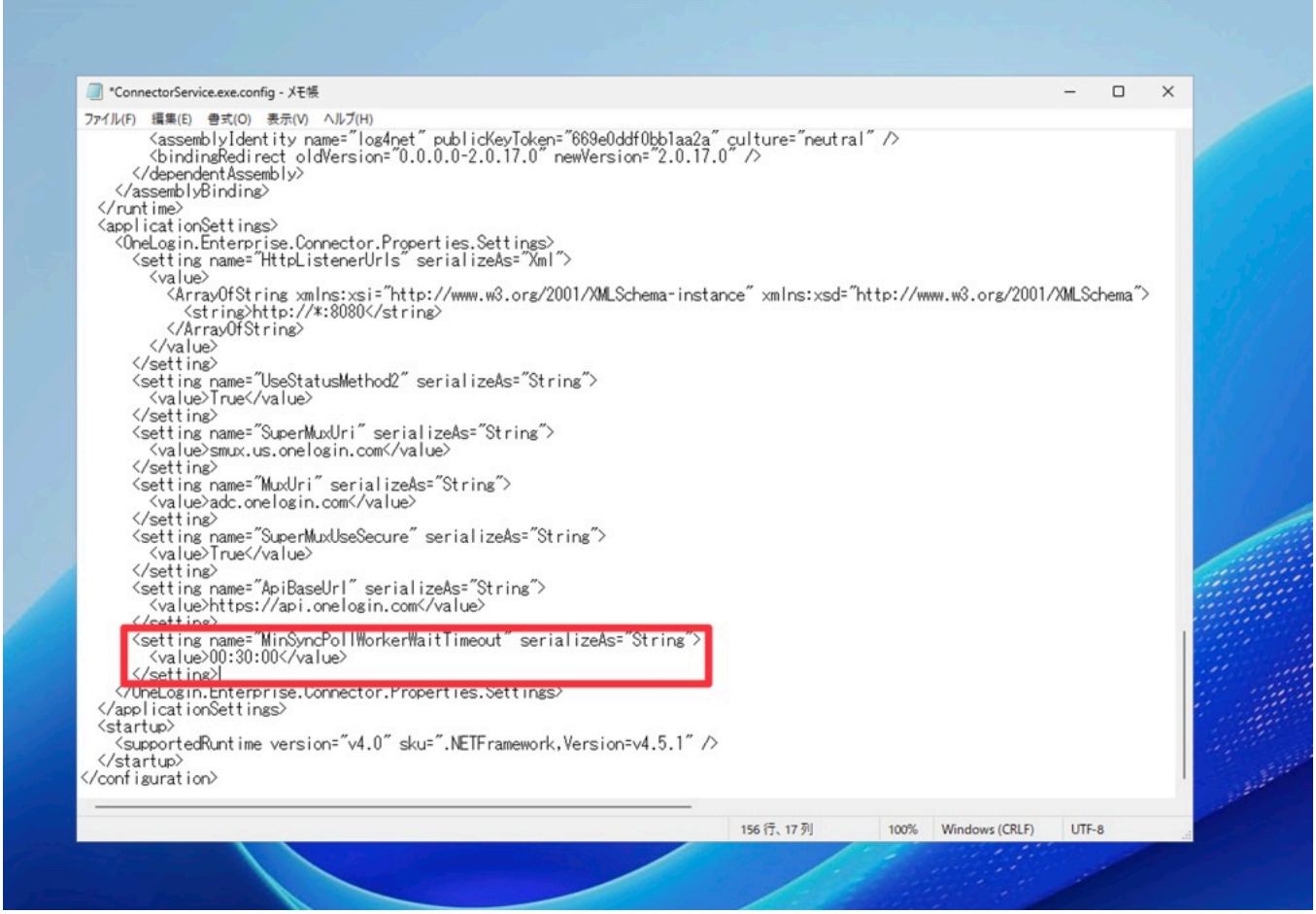
   ```
   C:\Program Files (x86)\OneLogin, Inc\OneLogin Active Directory Connector\ConnectorServic
   ```

   ** 環境によりパスは異なる場合がございます*

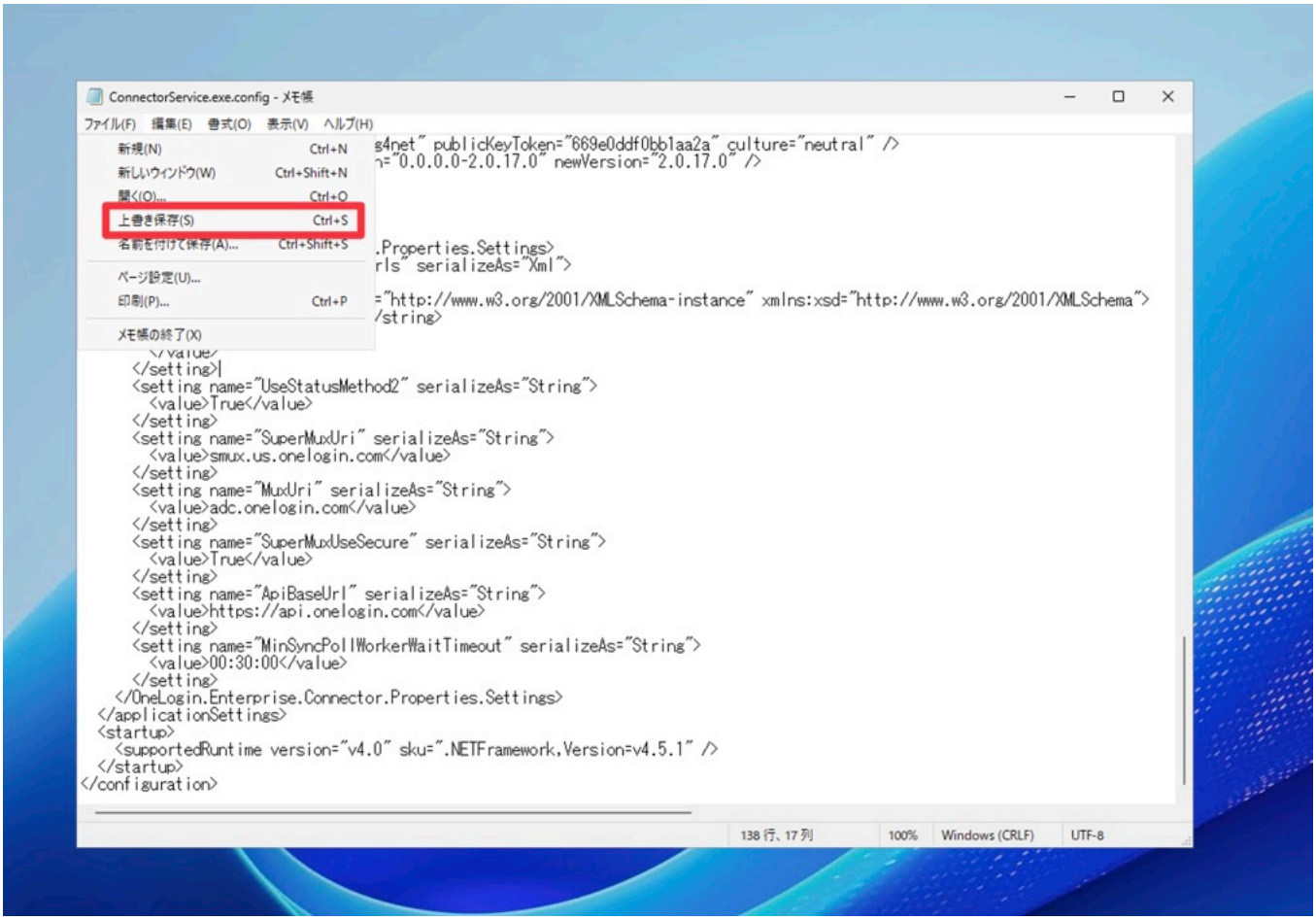
   

2. **</OneLogin.Enterprise.Connector.Properties.Settings>** の直前に、設定したい全体同期間隔を HH:MM:SS の形式で設定します
   例）全体同期間隔を30分とする場合、以下の内容を追加します

   ```
   <setting name="MinSyncPollWorkerWaitTimeout" serializeAs="String">
           <value>00:30:00</value>
    </setting>
   ```



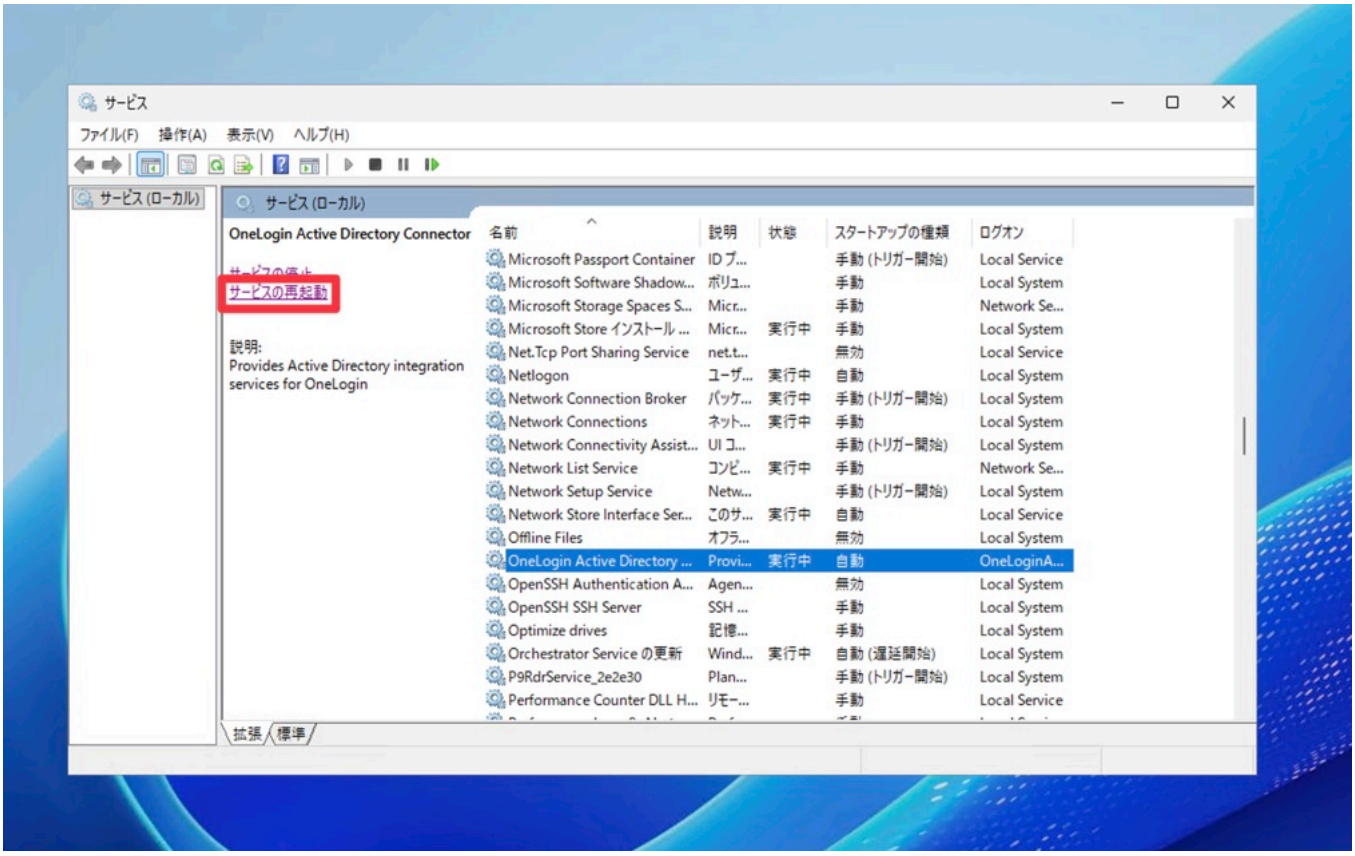
3. ファイル > **上書き保存** をクリックし、変更内容を保存します



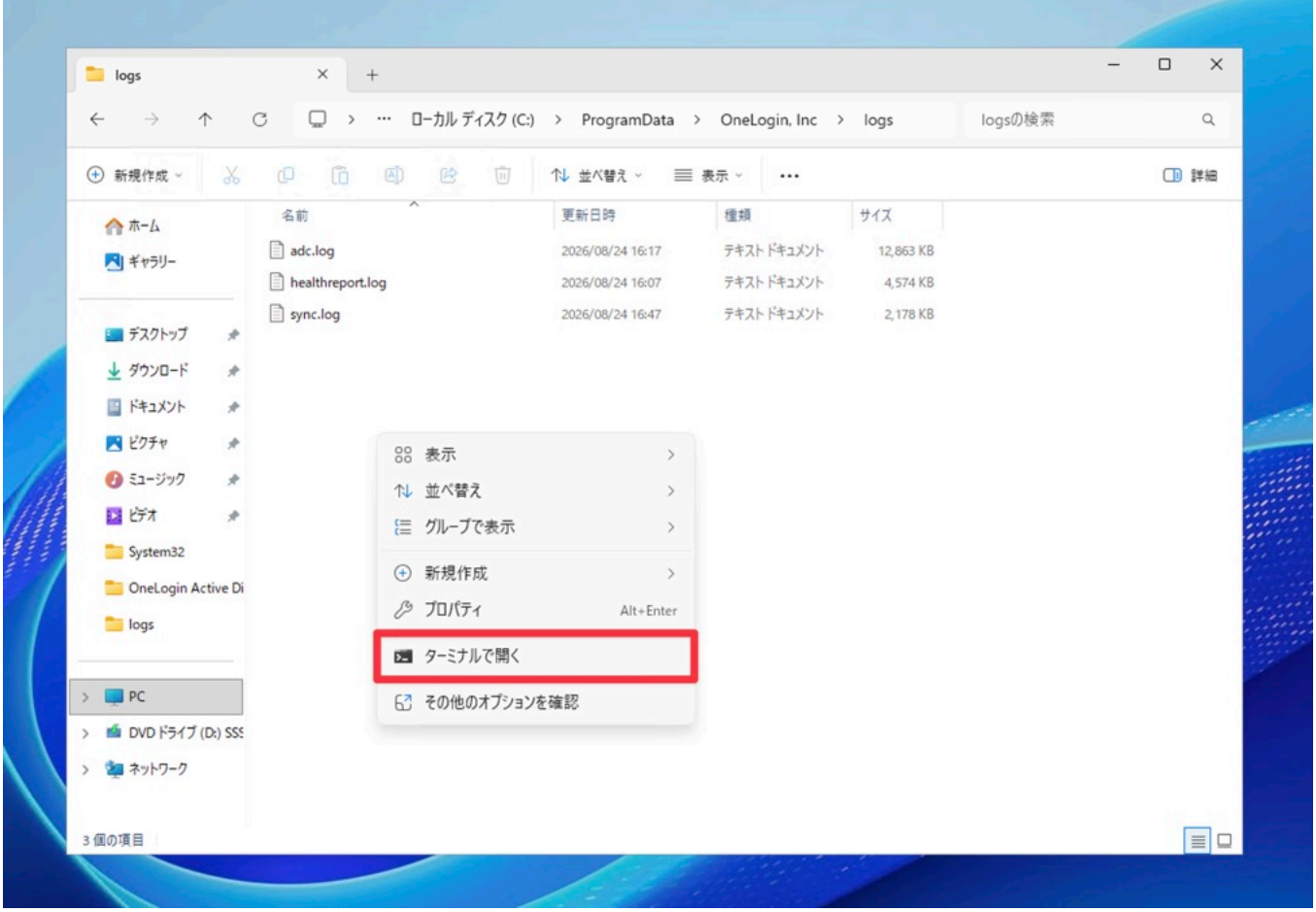
4. ［**Win**］＋［**R**］で **services.msc** を実行します



5. **サービスの再起動** をクリックします

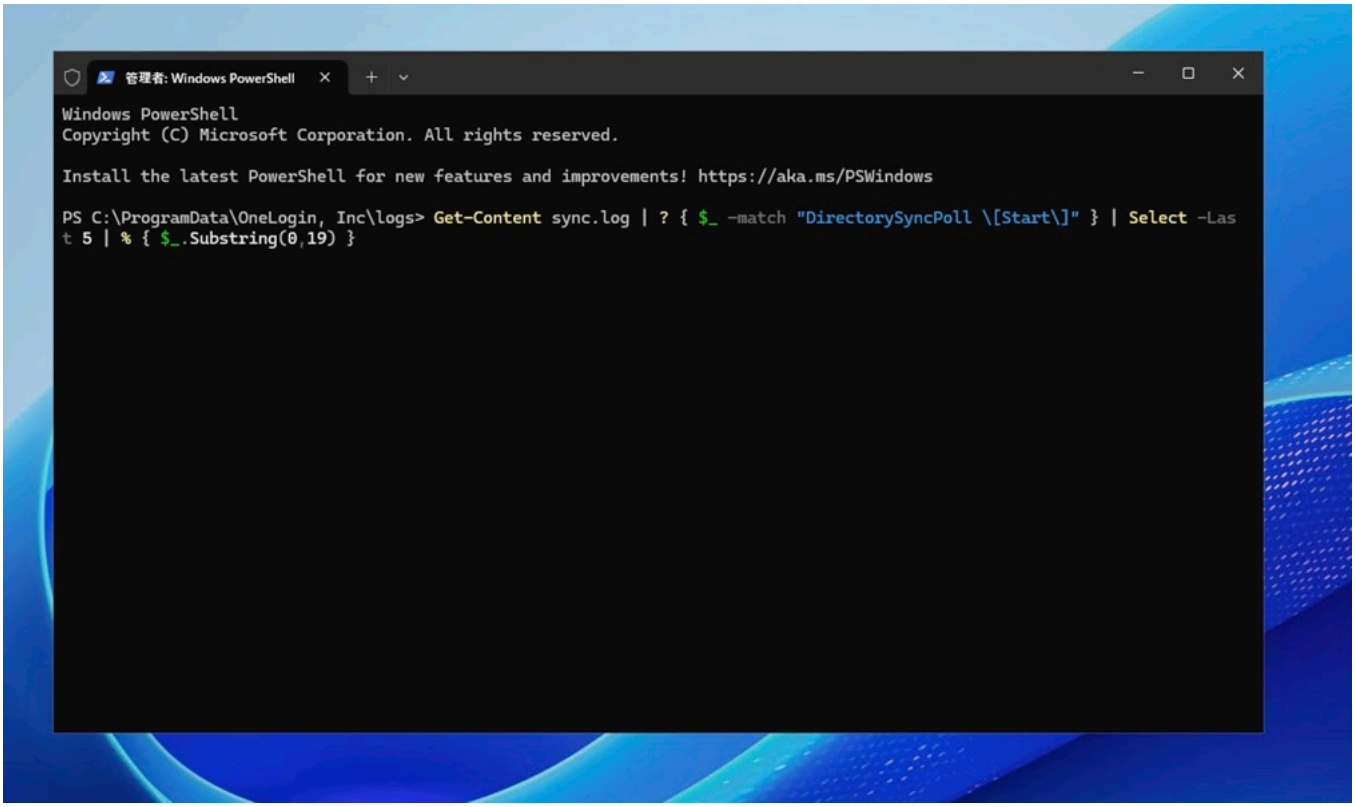


6. 設定が反映されていることを確認するため、一定時間が経過後に、`C:\ProgramData\OneLogin, Inc\logs` フォルダにて **ターミナル** を開きます
   ** 環境によりパスは異なる場合がございます*

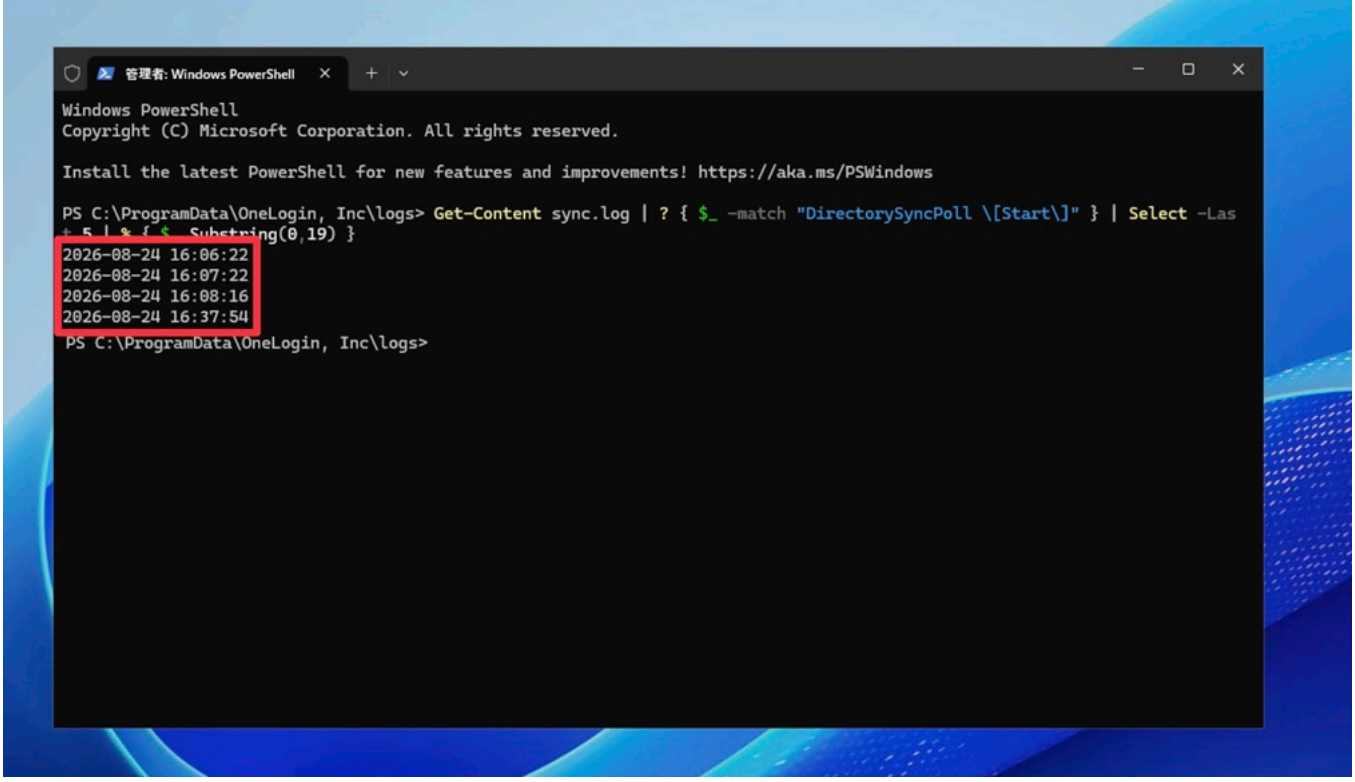


7. 以下のコマンドを実行します

```
Get-Content sync.log | ? { $_ -match "DirectorySyncPoll \[Start\]" } | Select -Last 5 |
```



8. 同期の間隔が正常に変更されていることを確認します
   例）同期間隔を1分から30分に変更した場合



OneLogin ADCアカウントの設定

ここでは2. OneLogin Active Directory ConnectorをWindows Serverにインストールする 手順7で **Run service as** を選択した際の設定方法をユーザーの作成からご紹介いたします。既存のユーザーをご利用いただく場合は2. 作成したユーザーに権限を付与より設定を進めてください。

1. ユーザーの作成

1. OneLogin ADCをインストールするサーバーへ接続し、［**Win**］＋［**R**］で **servermanager** を実行します



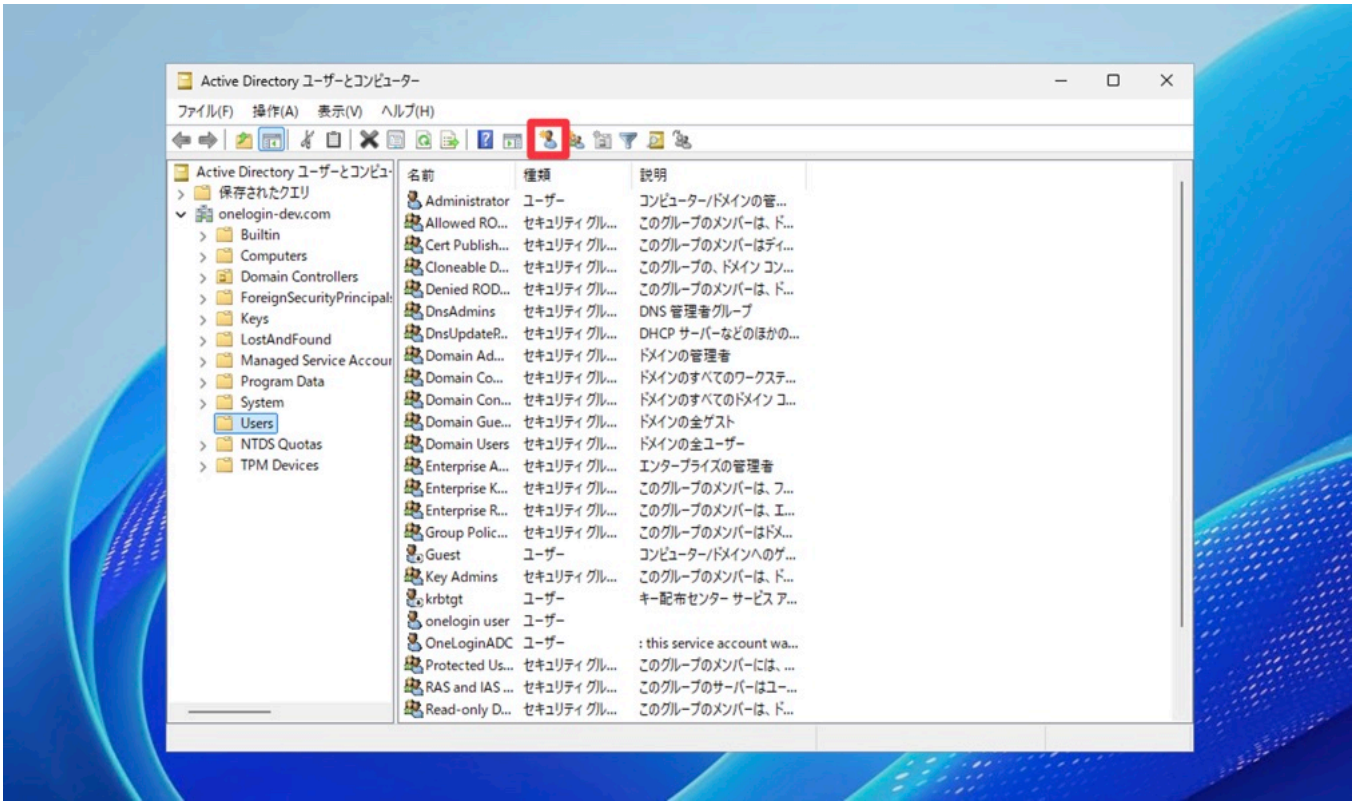
2. ［**ツール**］をクリックします



3. ［**Active Directory ユーザーとコンピューター**］をクリックします

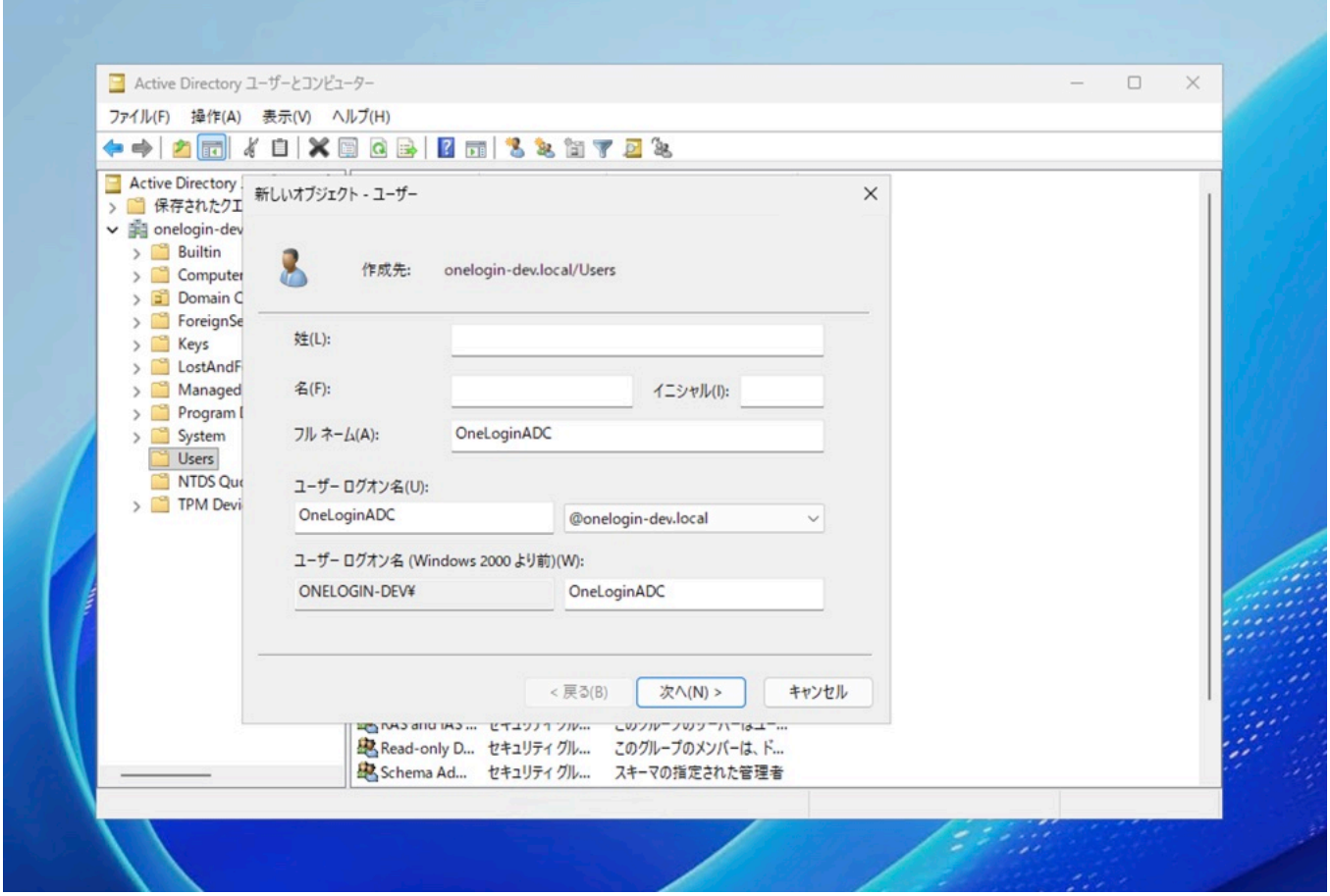


4. 人型アイコンの［**現在のコンテナーに新しいユーザーを作成**］をクリックします

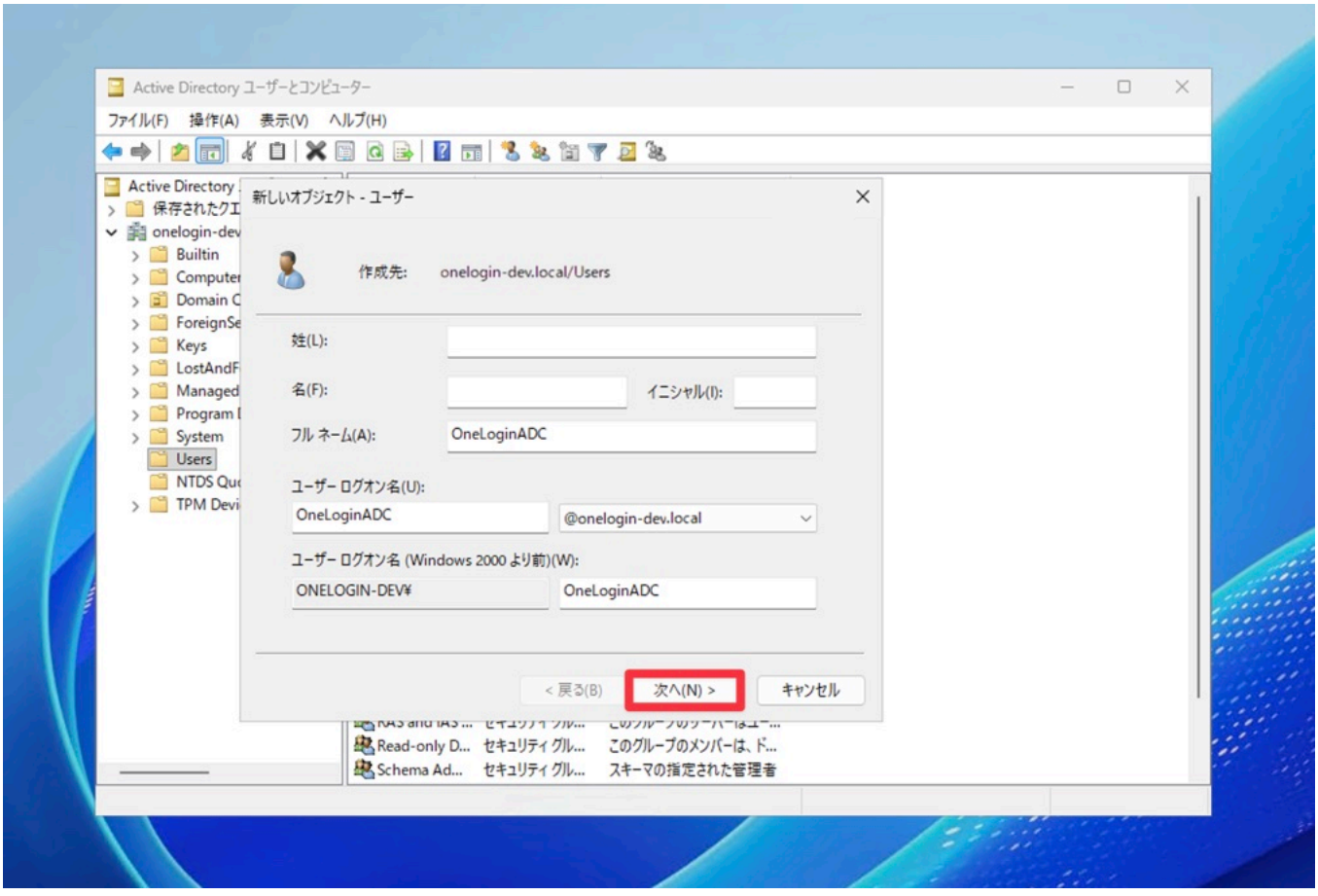


5. OneLogin ADCのサービス実行用ユーザーを作成します

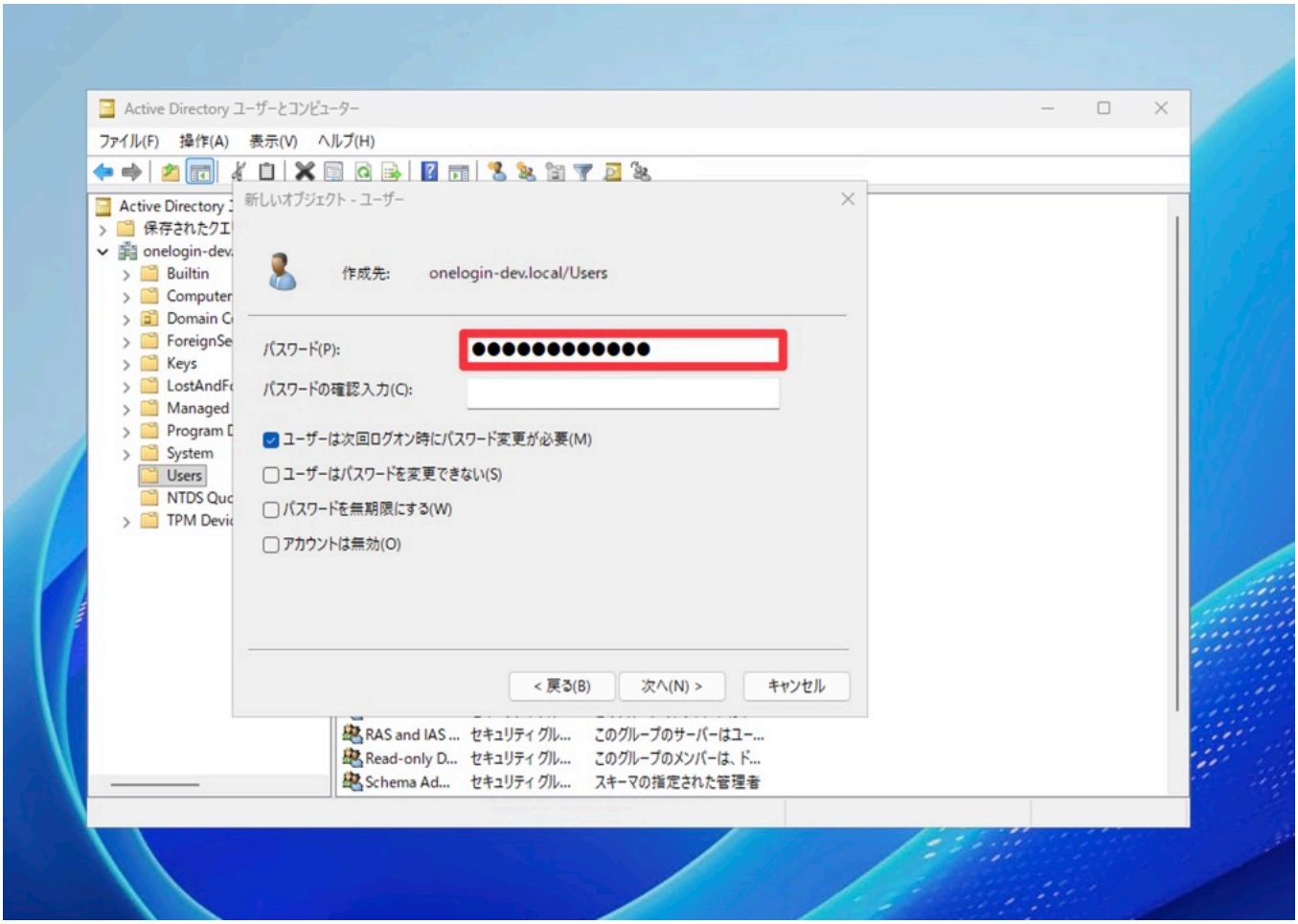
   * *2. OneLogin Active Directory ConnectorをWindows Serverにインストールする 手順7* で ***Create OneLogin Service Account*** *を選択した場合は、OneLoginADC@<Your Domain>が生成されますので、以下のように設定することを推奨いたします*



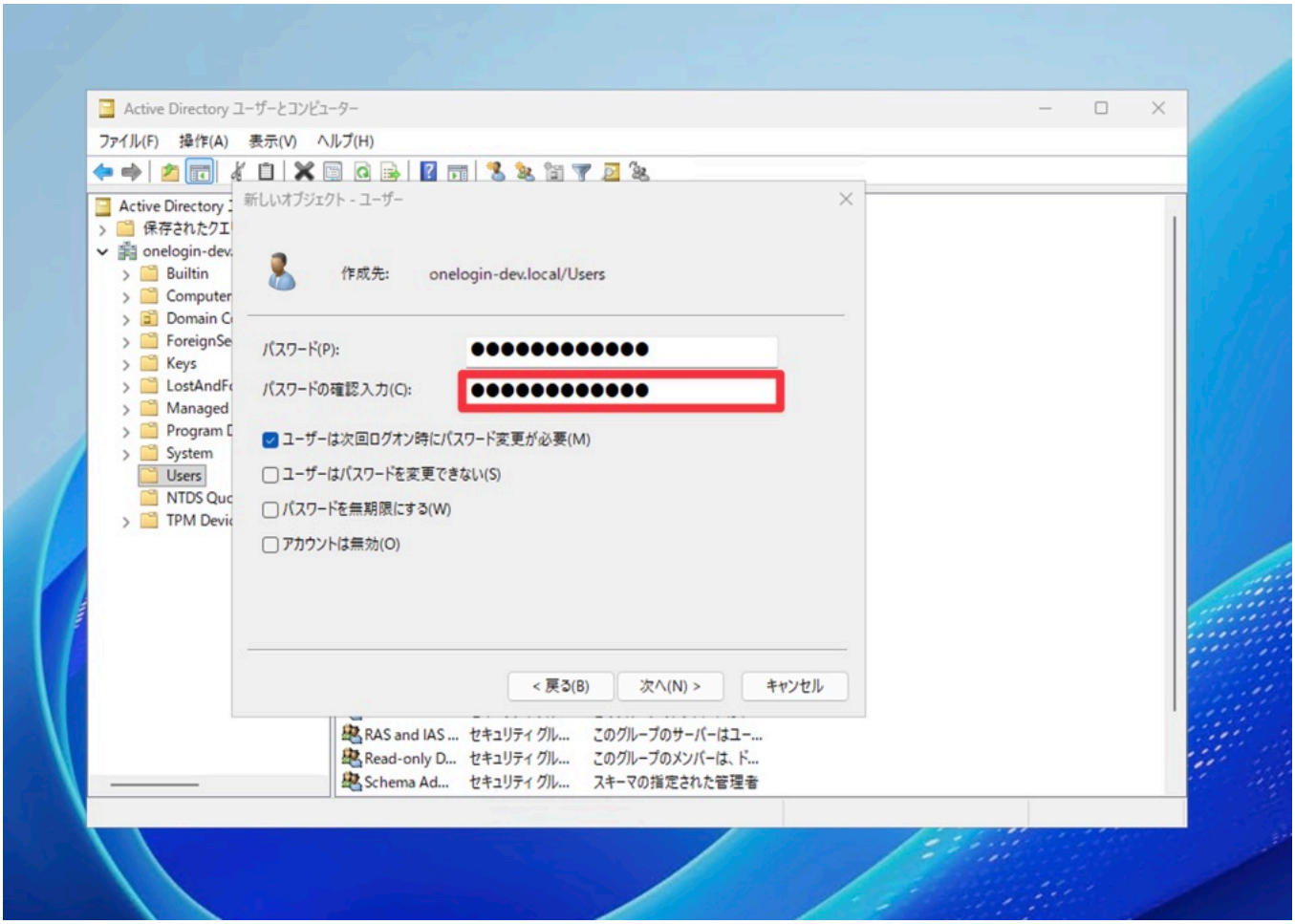
6. ユーザー情報の設定後、［**次へ**］をクリックします



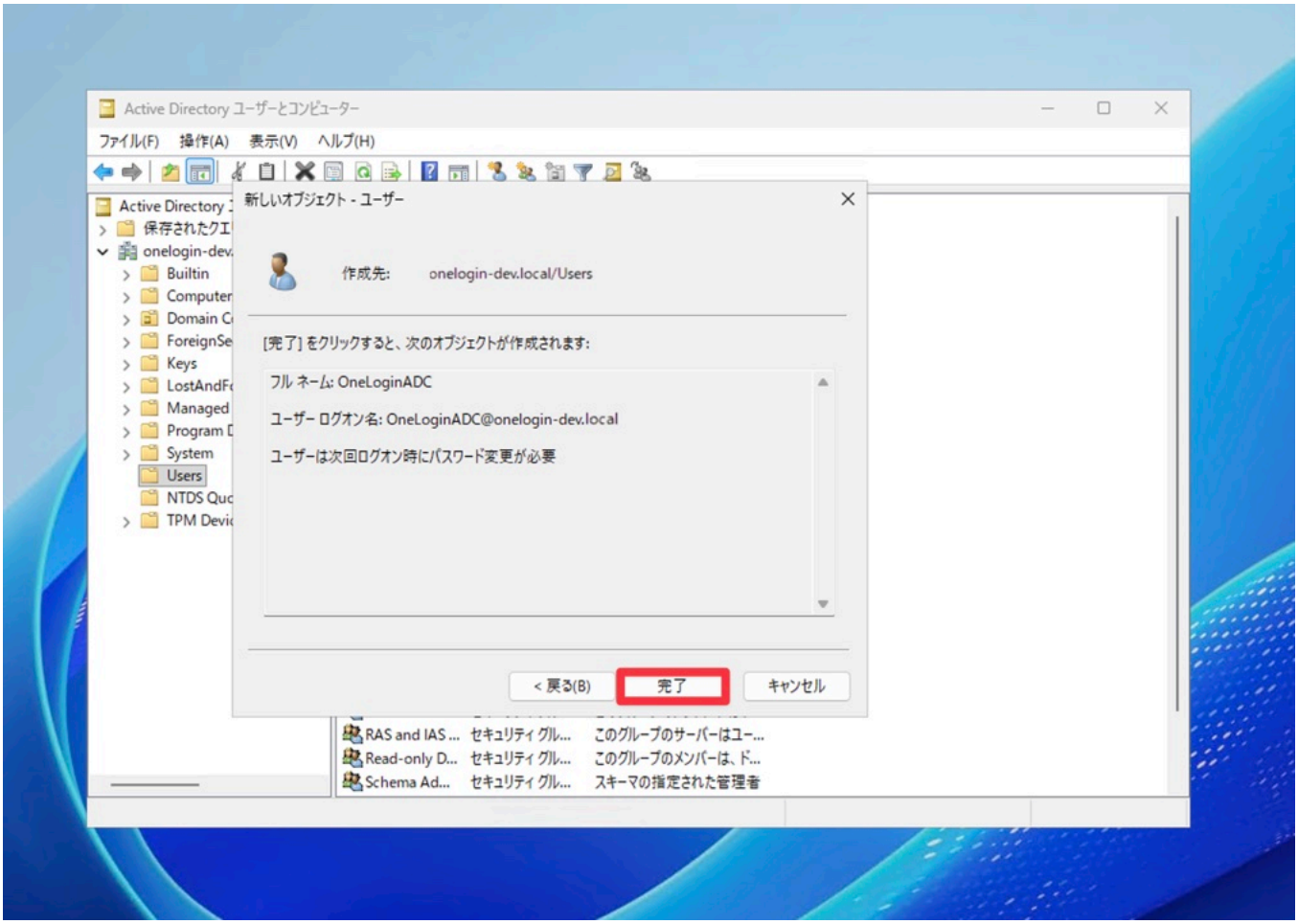
7. 作成するユーザーの任意の **パスワード** を入力します



8. **パスワードの確認入力** に、再度パスワードを入力します

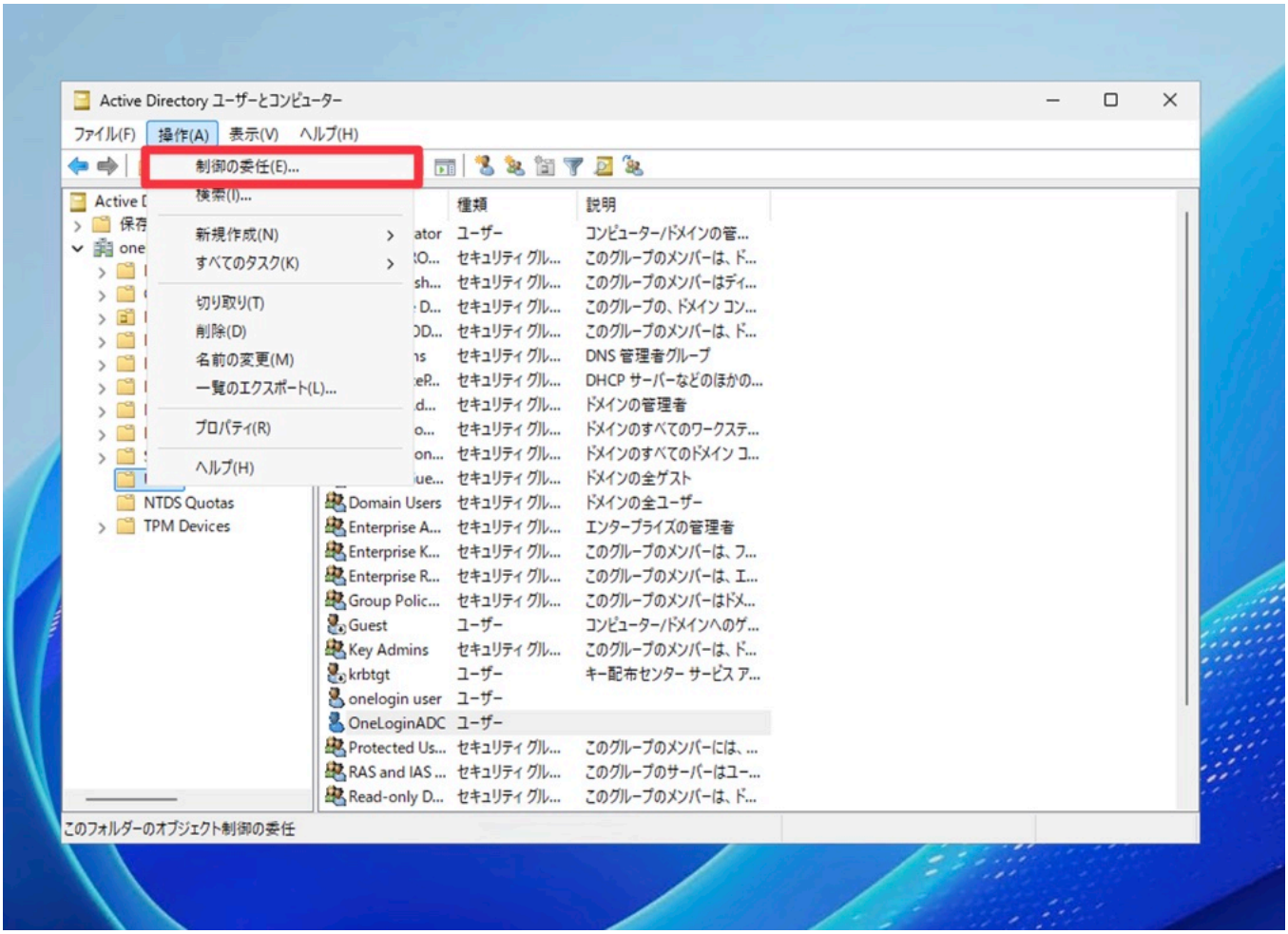


9. ［**完了**］をクリックします

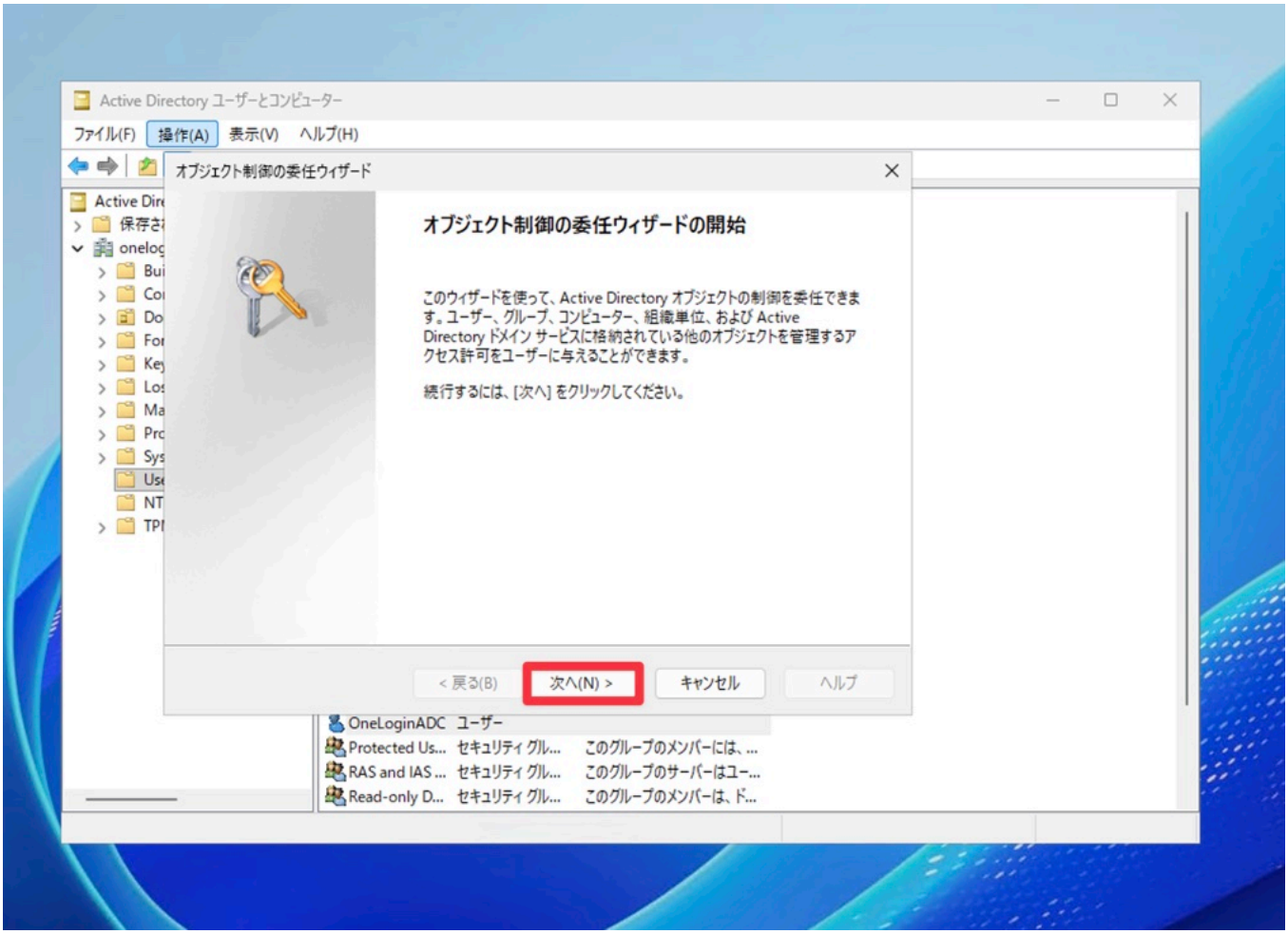


2. 作成したユーザーに権限を付与

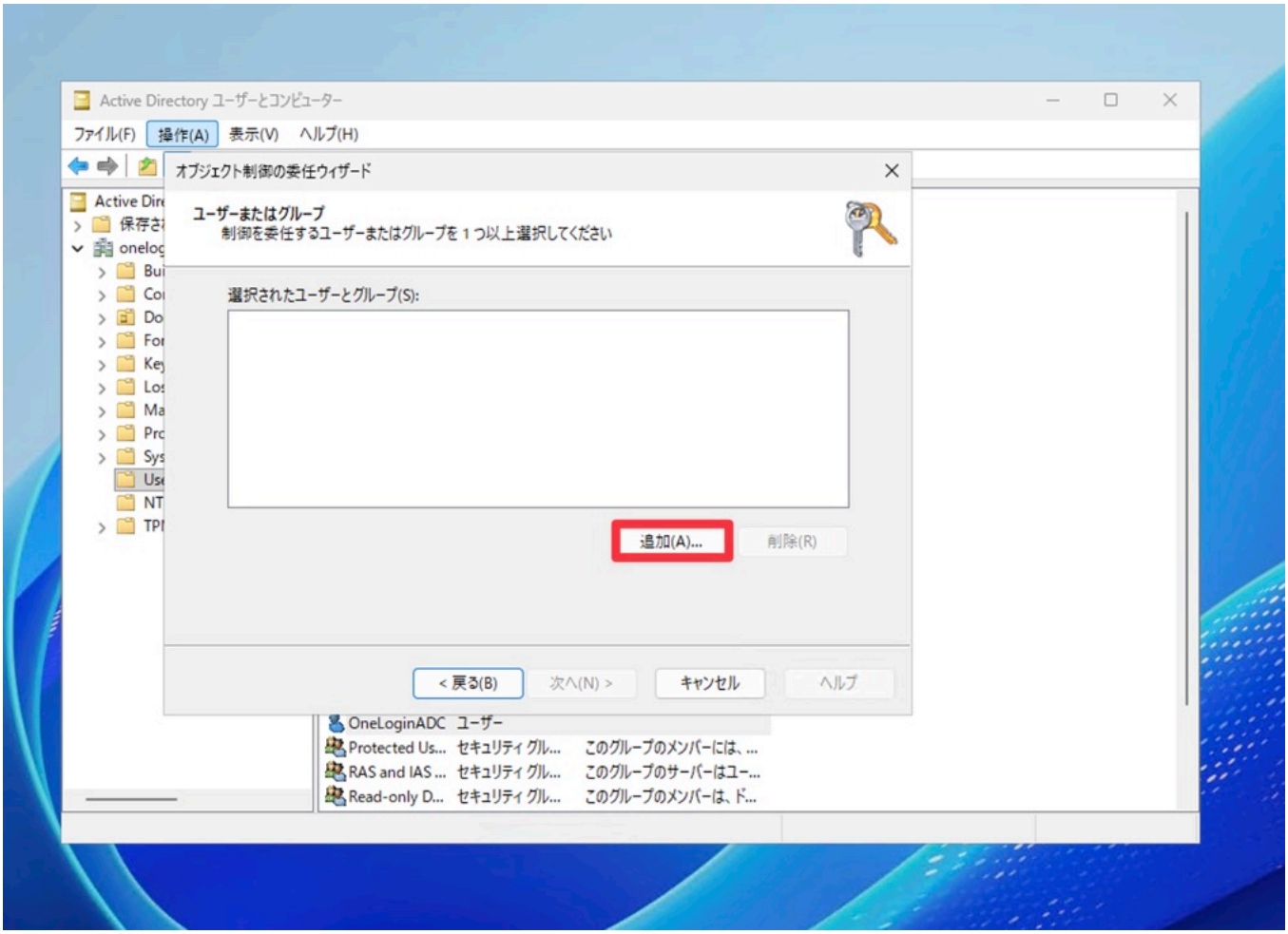
1. 操作 > [**制御の委任**] をクリックします



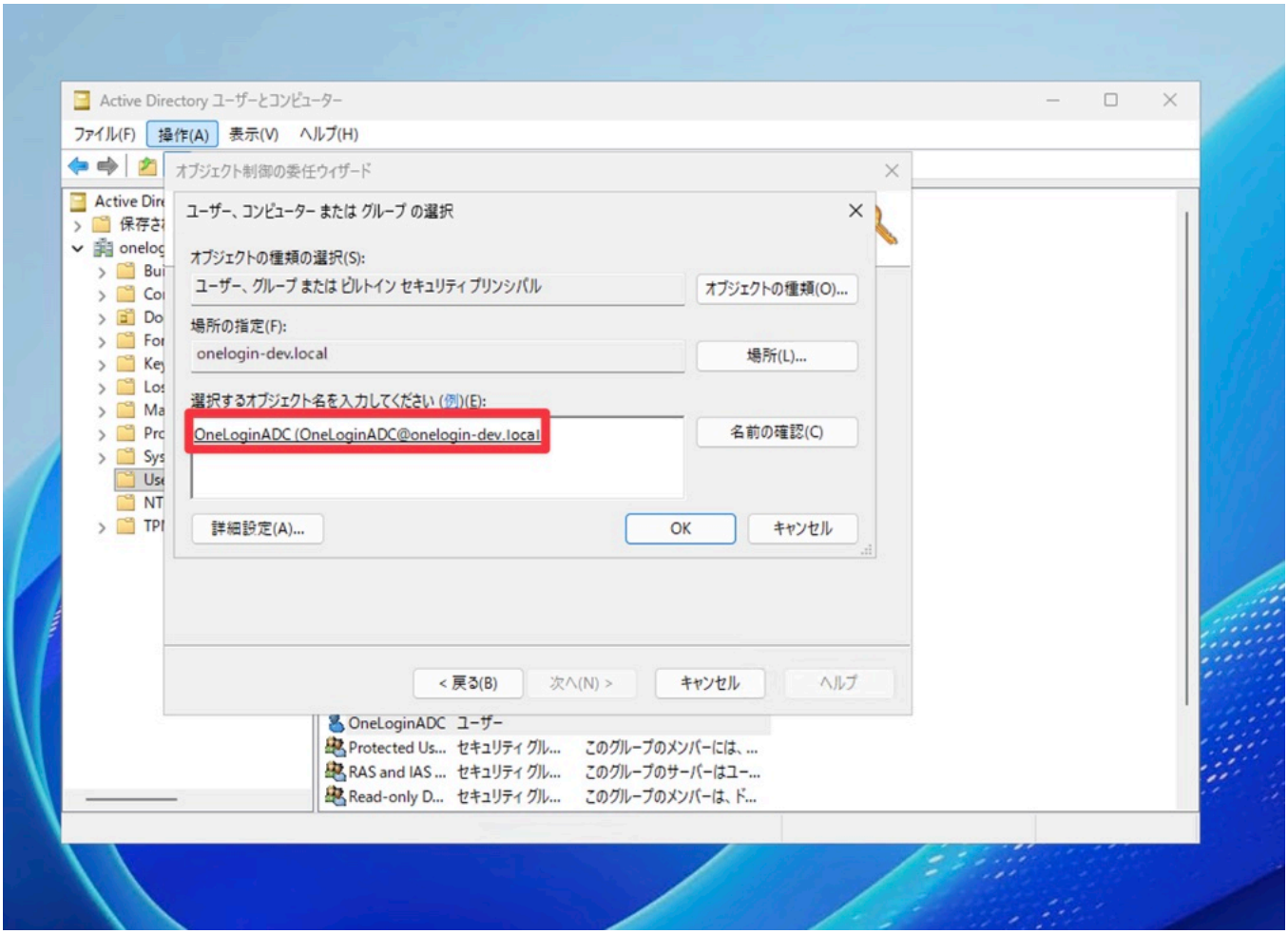
2. [**次へ**] をクリックします



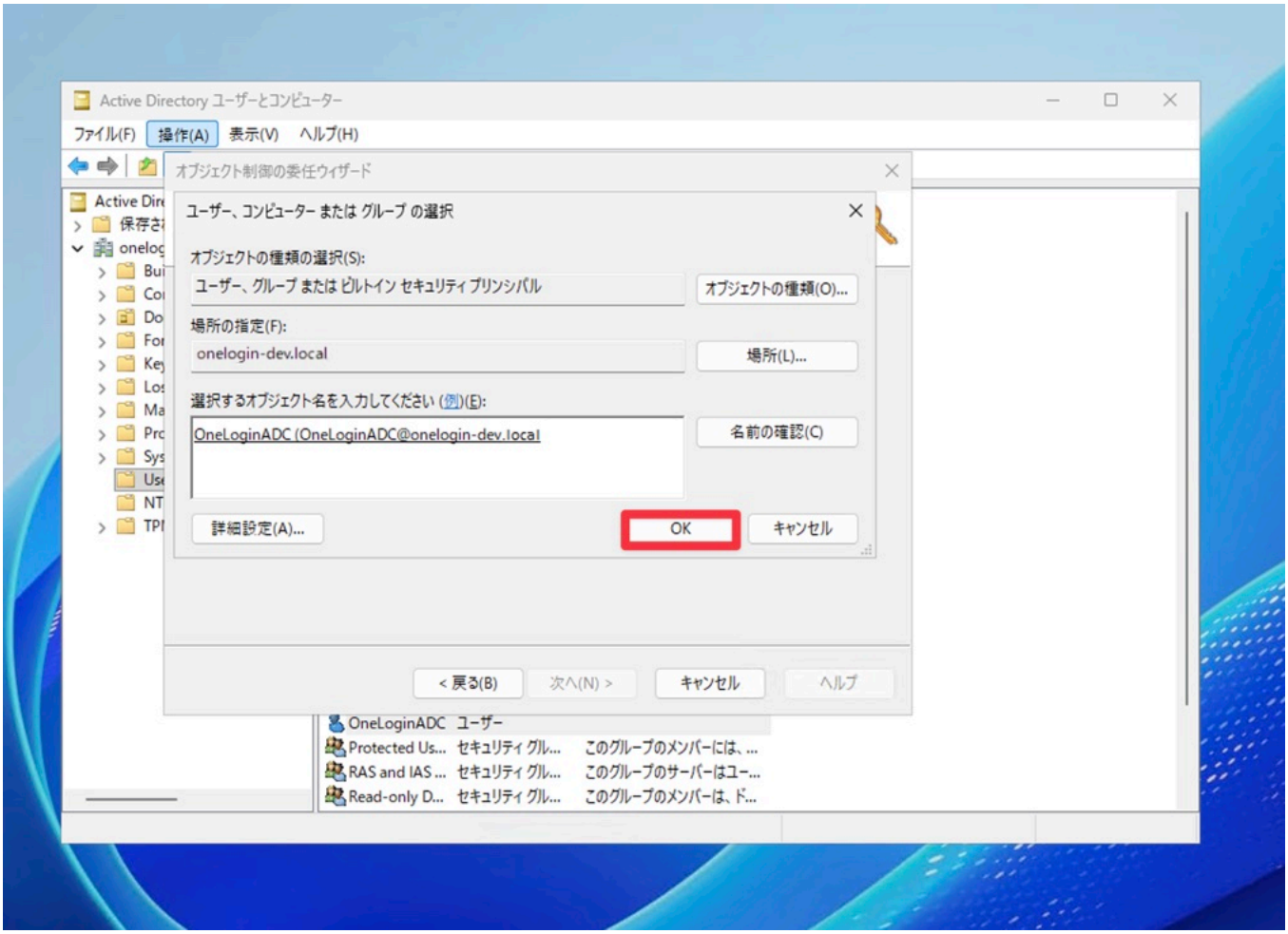
3. ［**追加**］をクリックします



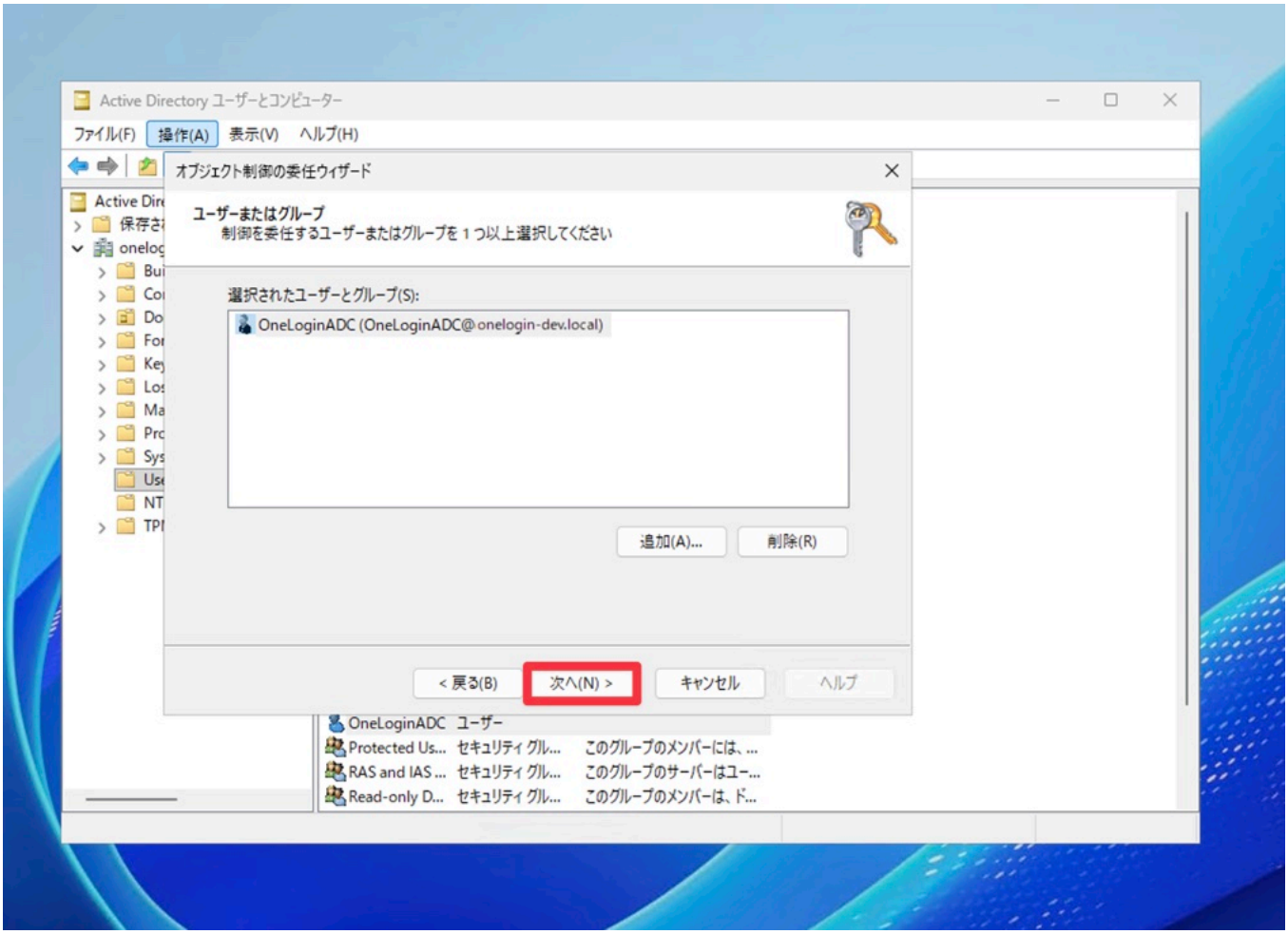
4. OneLogin ADCアカウントの設定 手順5で設定したユーザーを入力します



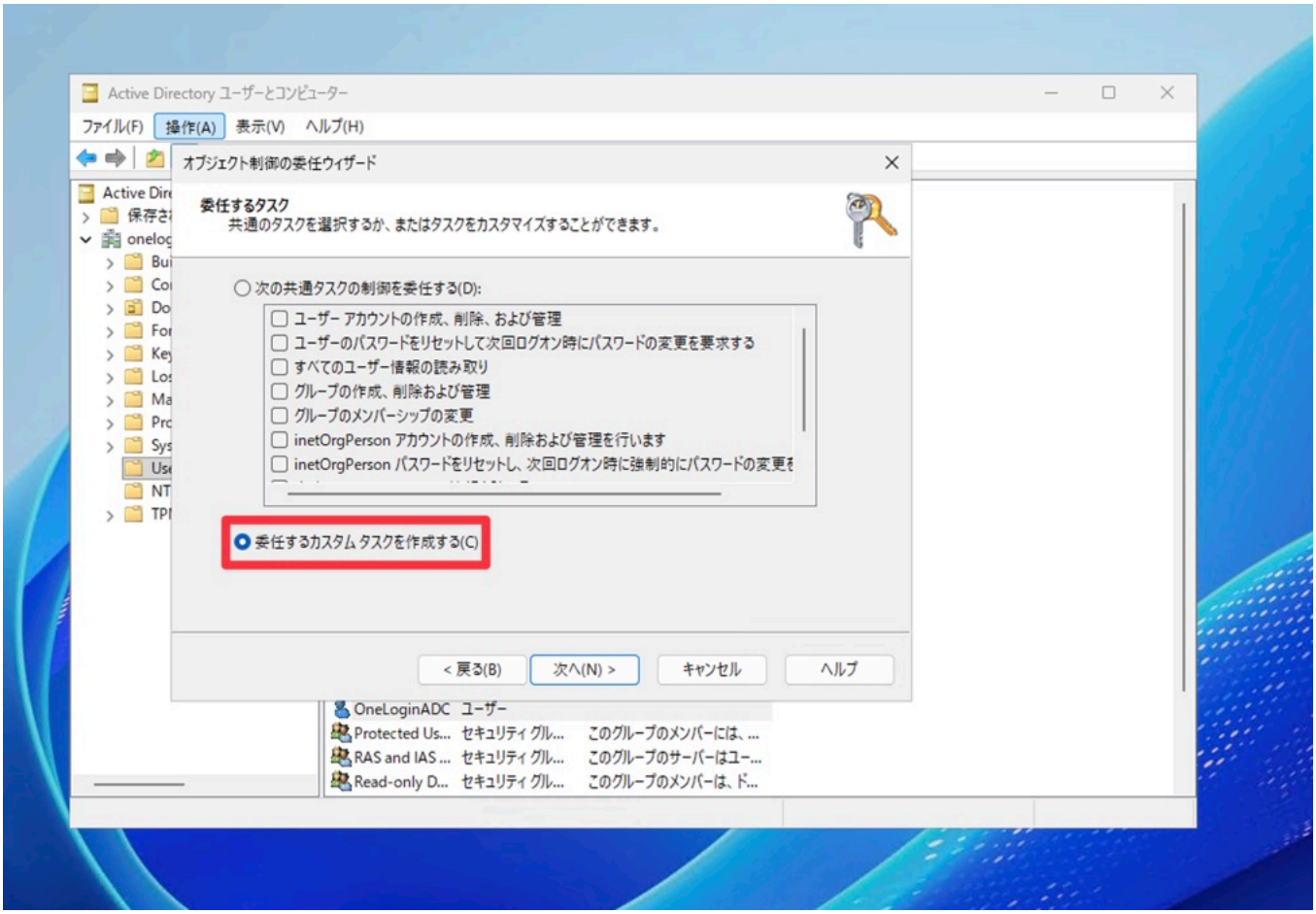
5. ［**OK**］をクリックします



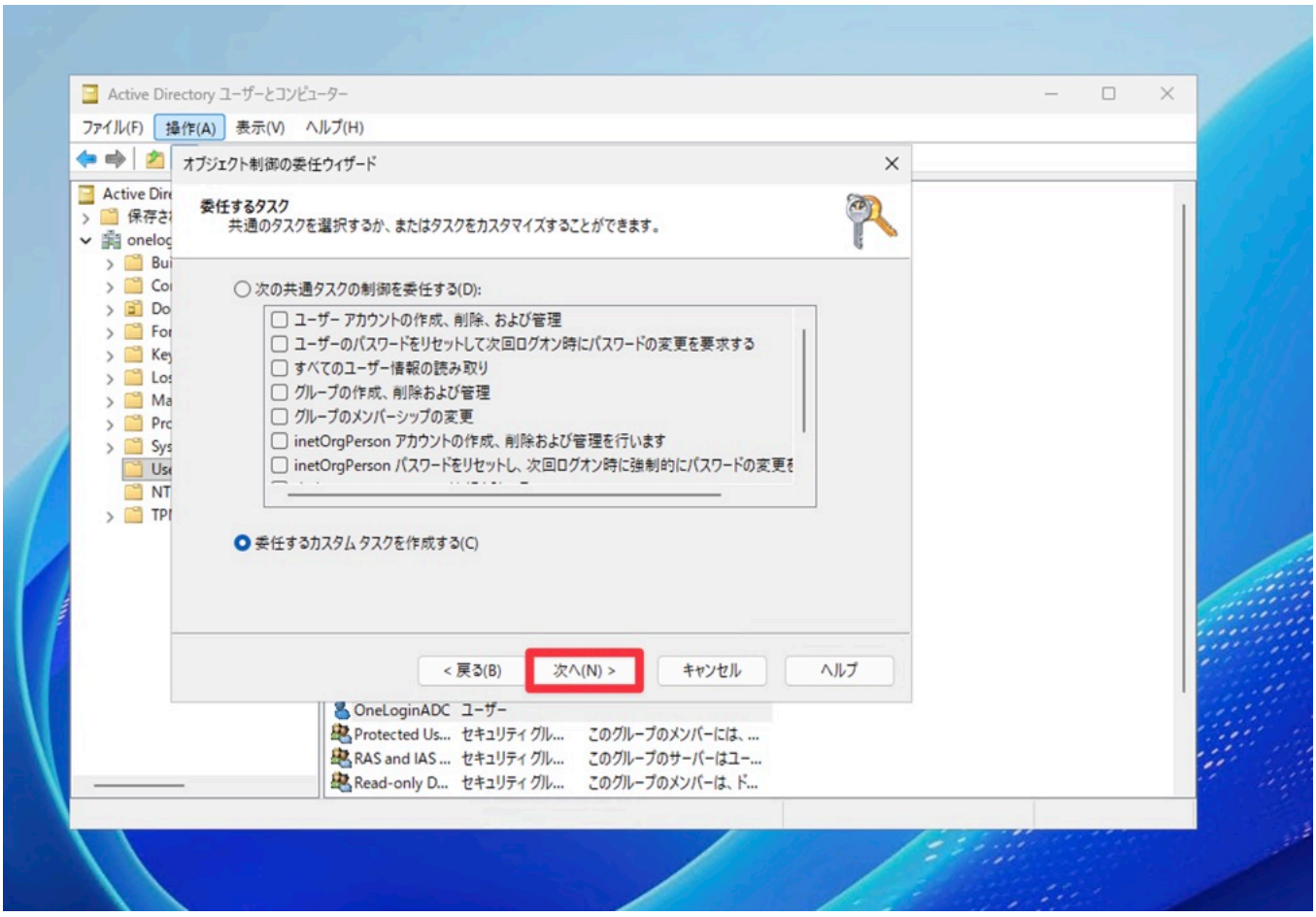
6. ［**次へ**］をクリックします



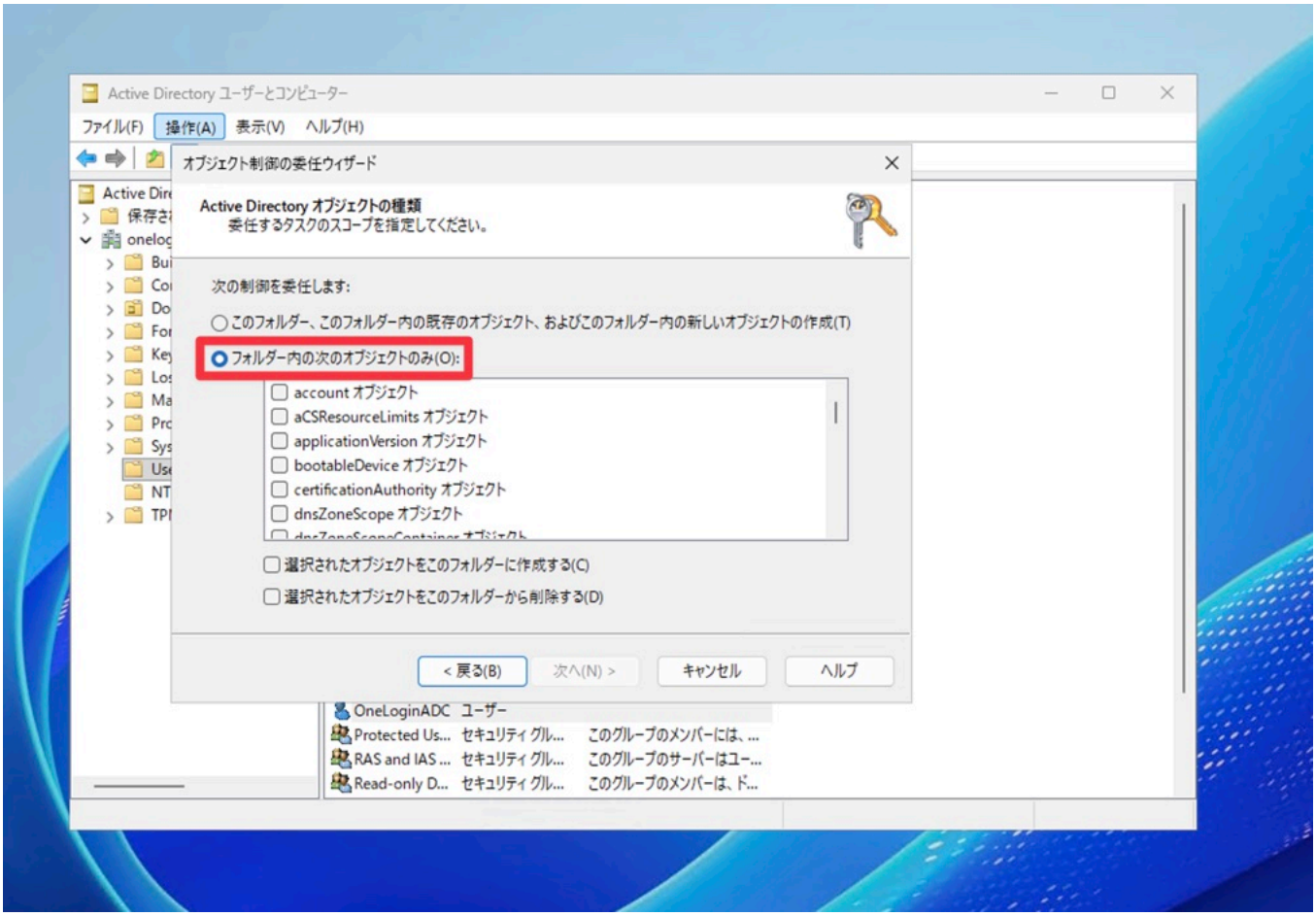
7. **委任するカスタム タスクを作成する** を選択します



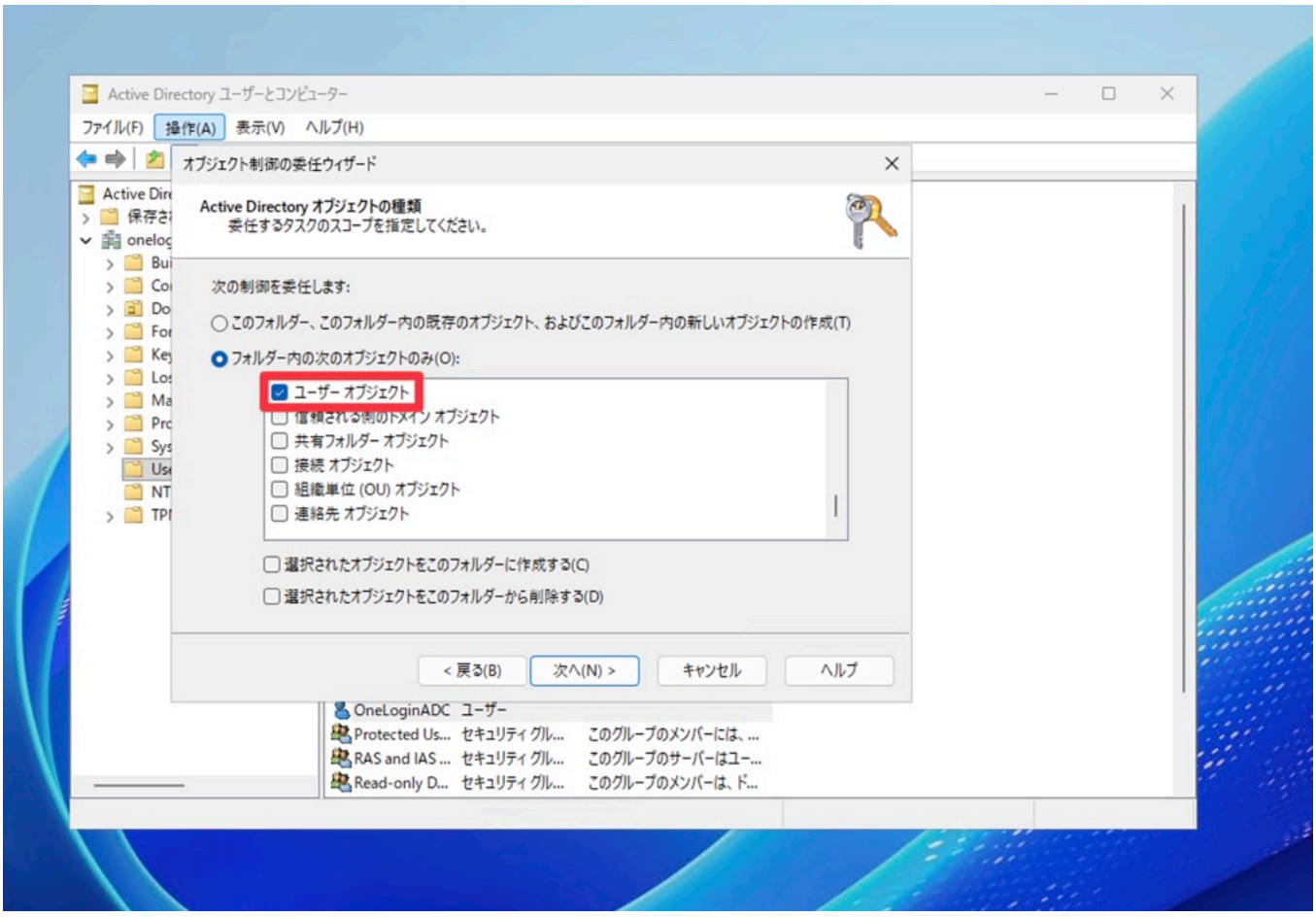
8. ［**次へ**］をクリックします



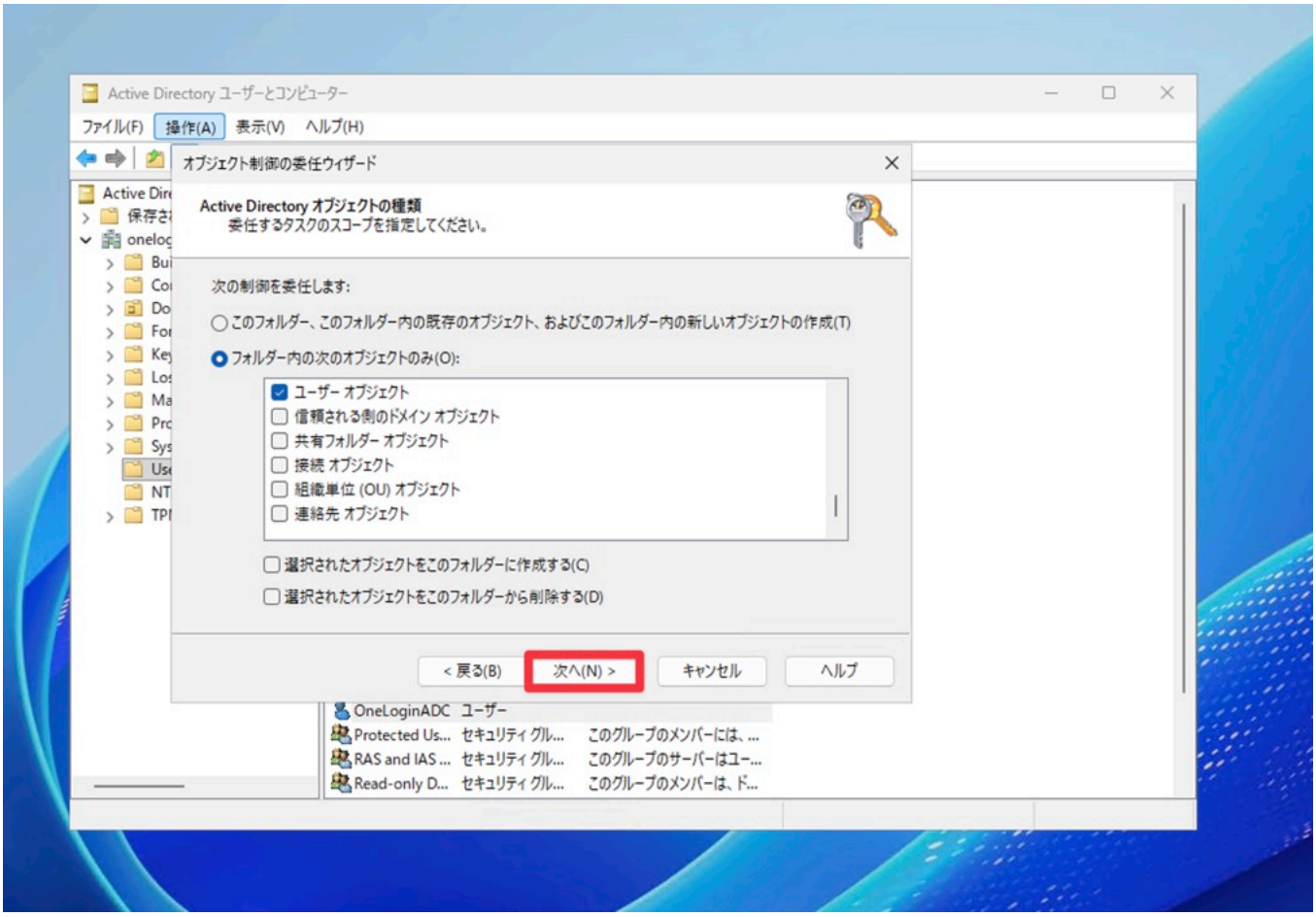
9. **フォルダー内の次のオブジェクトのみ** を選択します



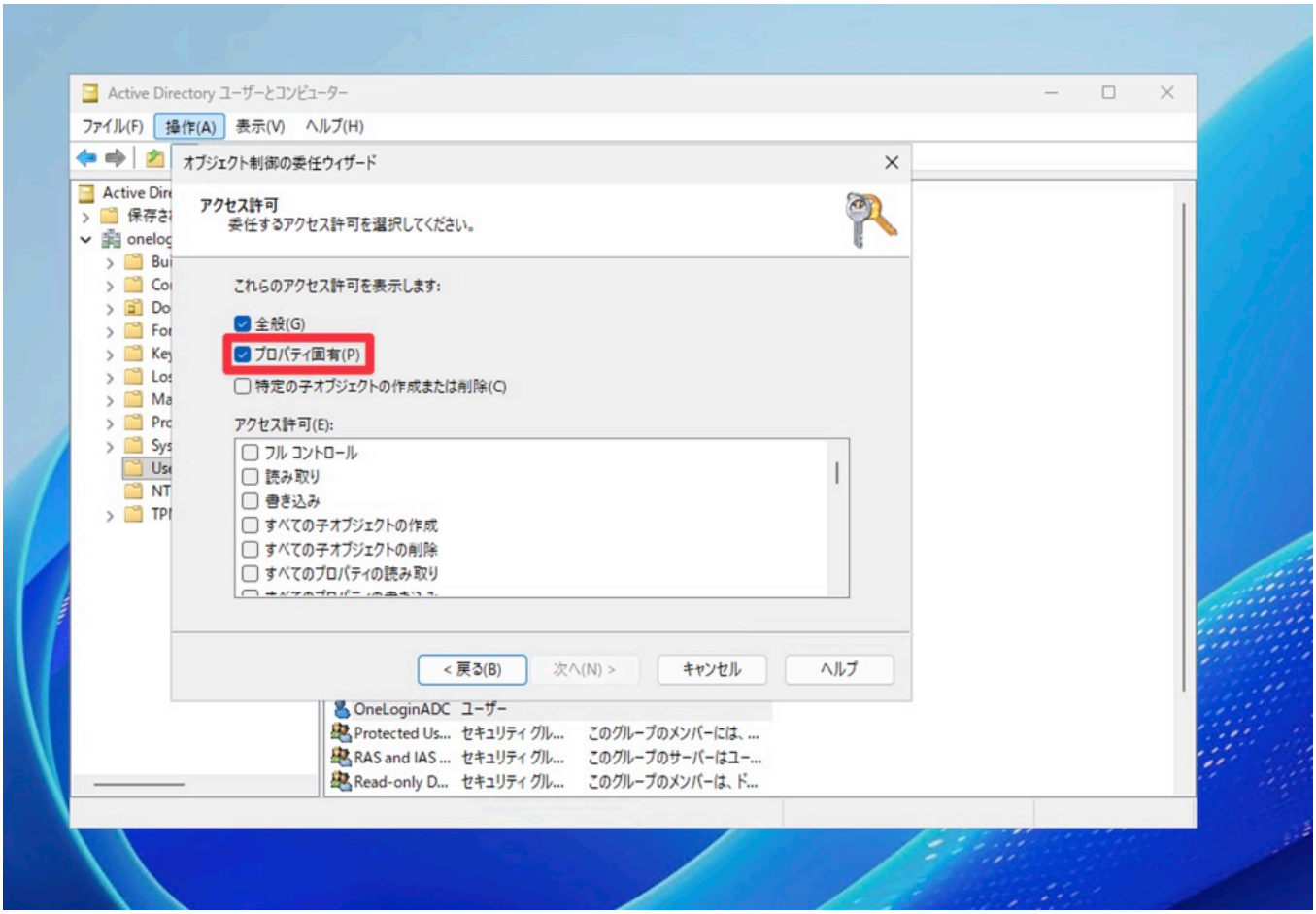
10. **ユーザー オブジェクト** を選択します



11. ［**次へ**］をクリックします



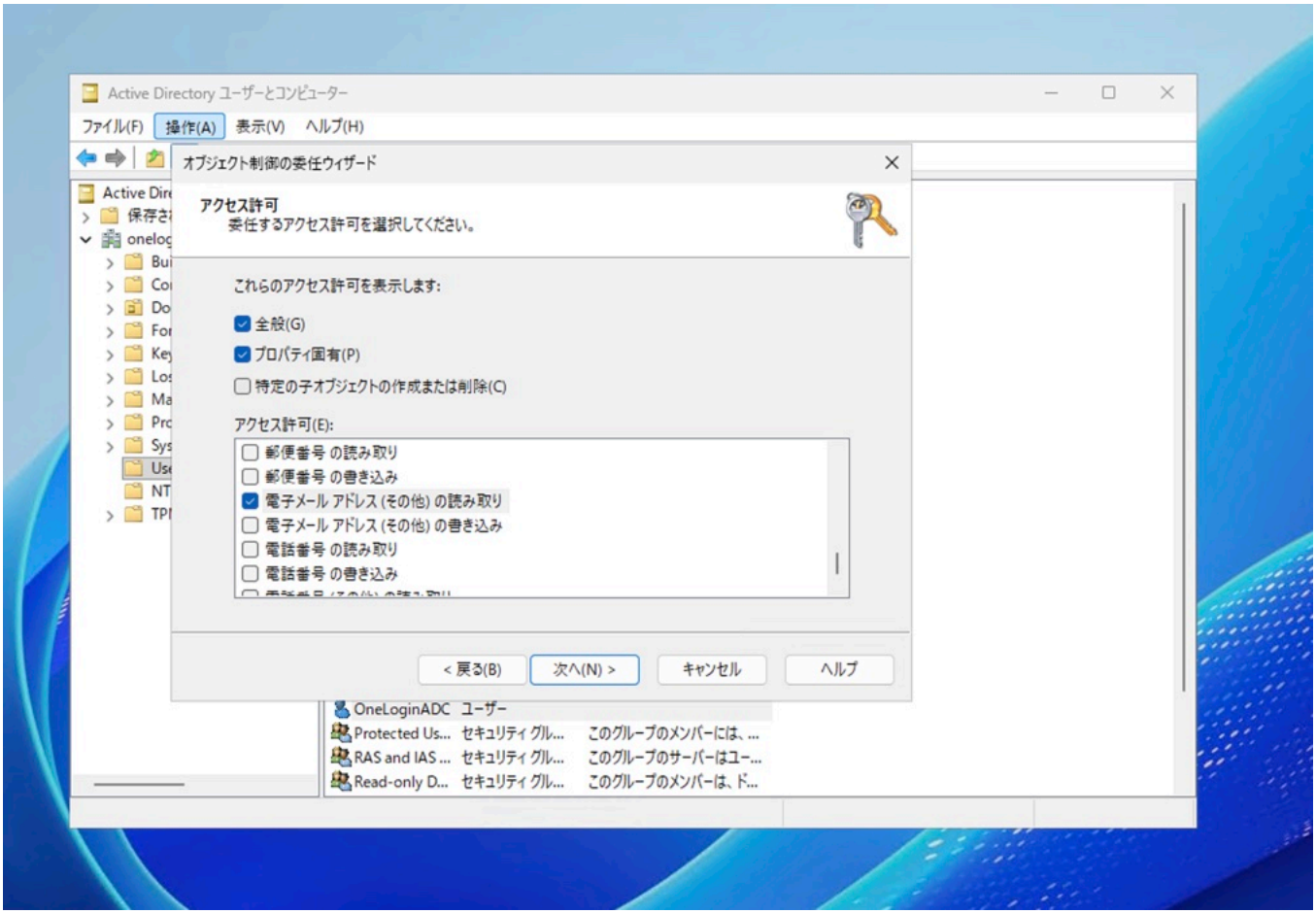
12. **プロパティ固有** のチェックボックスにチェックを入れます



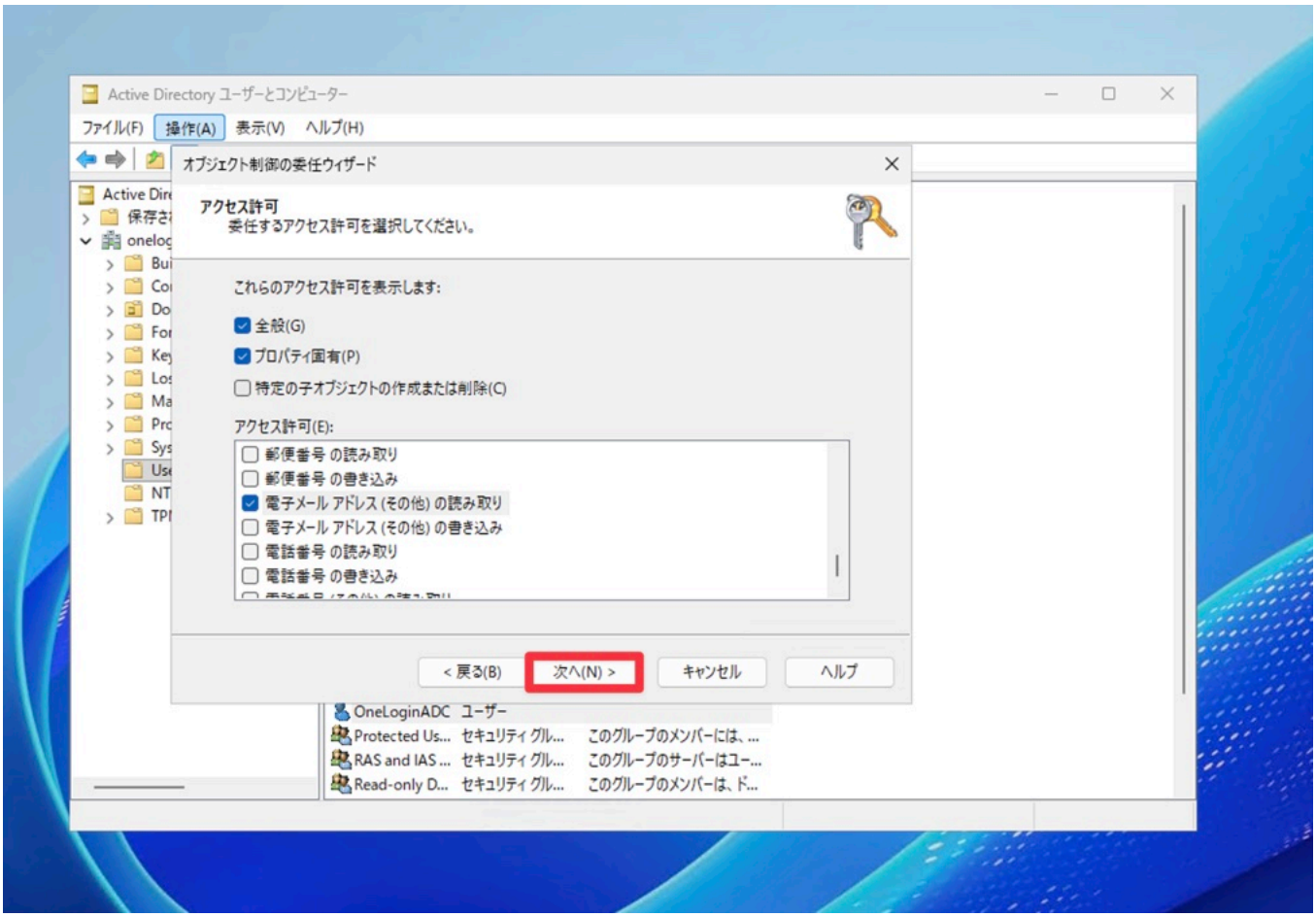
13. **アクセス許可** のチェックリストにおいて少なくとも以下の項目にチェックを入れます

- パスワードの変更
- パスワードのリセット
- lockoutTimeの読み取り
- lockoutTimeの書き込み
- objectSidの読み取り
- userAccountControlの読み取り
- userAccountControlの書き込み
- ミドルネームの読み取り
- ログオン名の読み取り
- ログオン名（Windows 2000より前）の読み取り
- 名前の読み取り
- 所属するグループの読み取り
- 表示名の読み取り
- 電子メールアドレス（その他）の読み取り

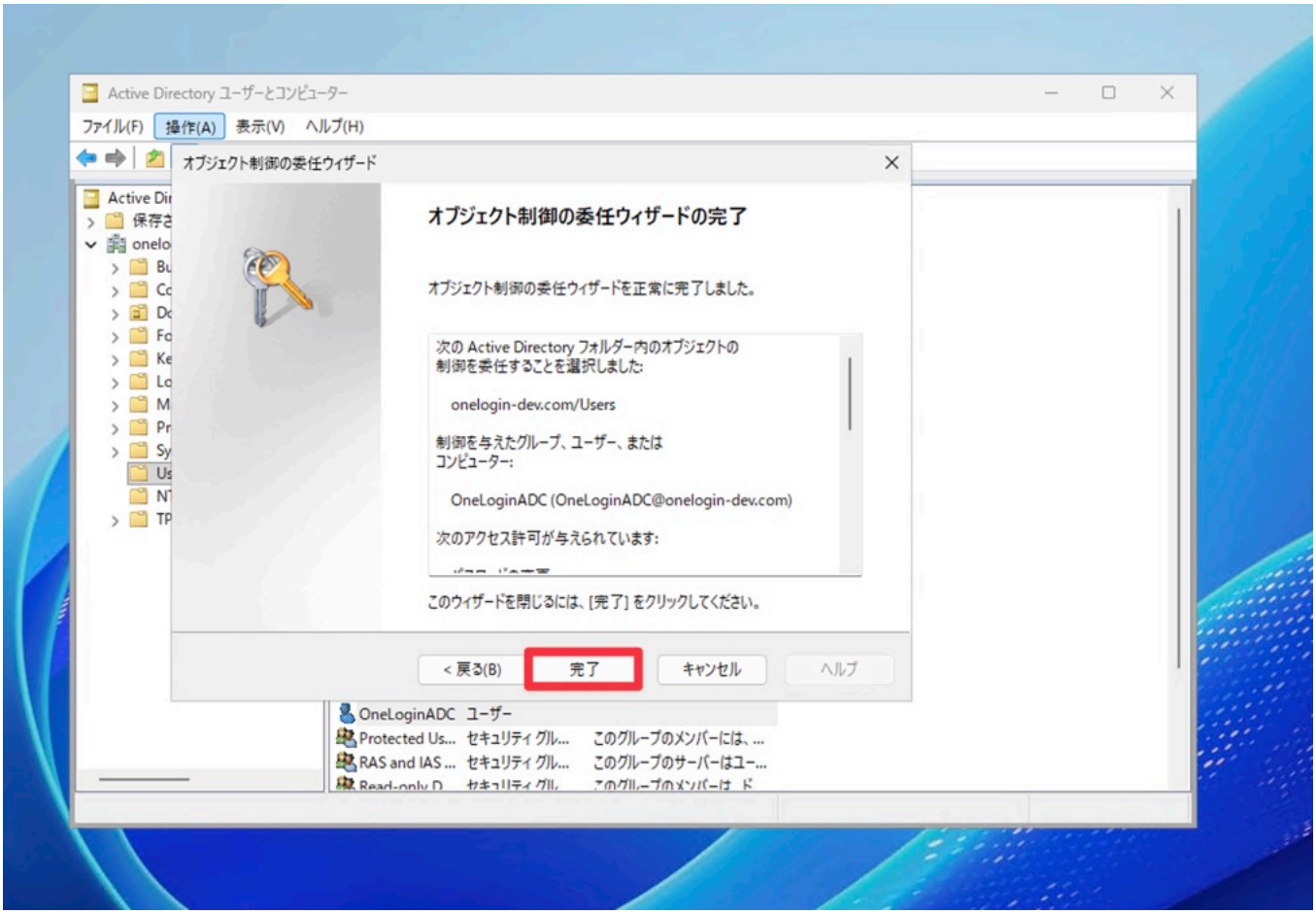
標準同期項目以外も同期を行っている場合は、該当する項目へもアクセスを許可してください



14. ［**次へ**］をクリックします



15. ［**完了**］をクリックします

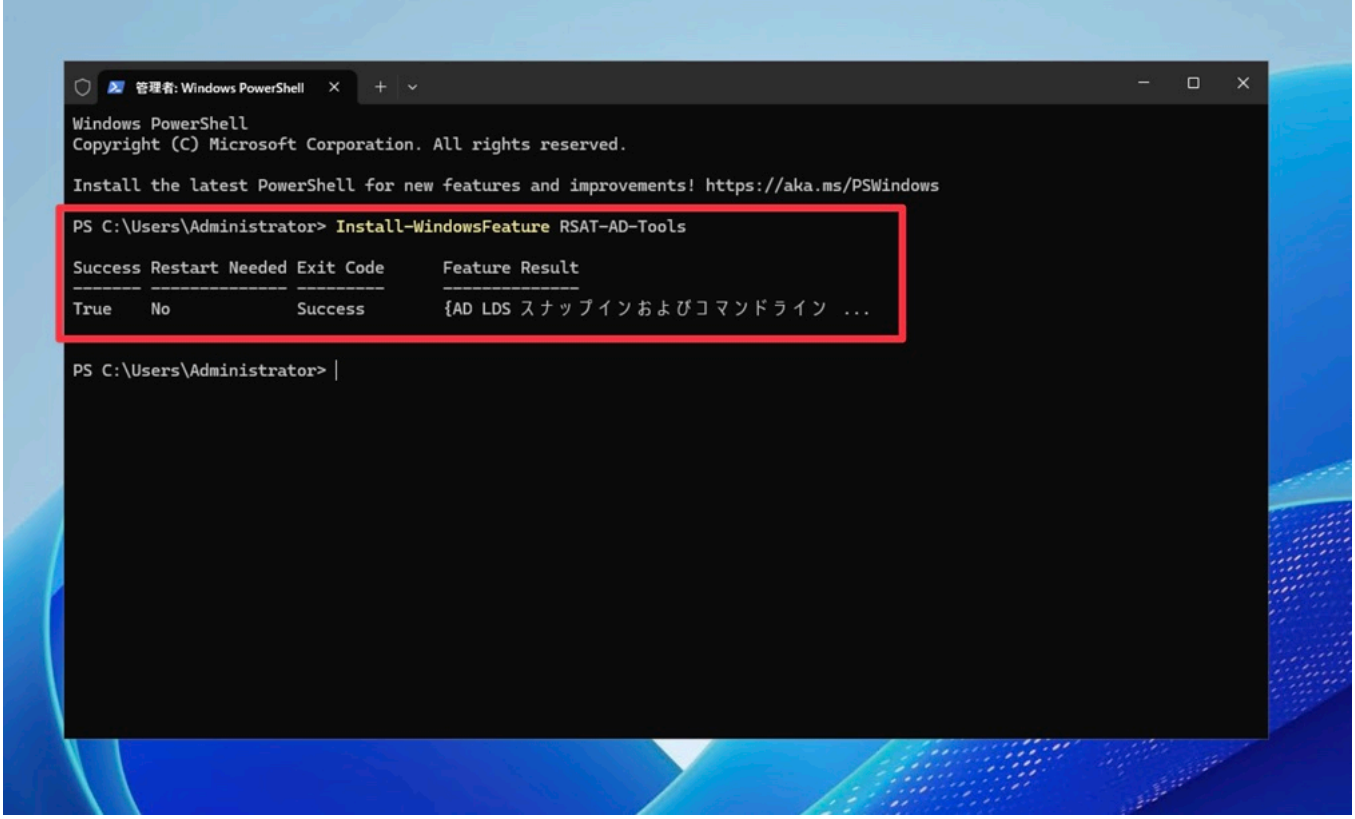


OneLogin Active Directory Connectorをメンバーサーバーにインストールする場合

OneLogin ADCをメンバーサーバーにインストールする場合、2. OneLogin Active Directory ConnectorをWindows Serverにインストールする 手順16のコマンドを実行するために別途 **Remote Server Administration Tools** のインストールが必要となります。

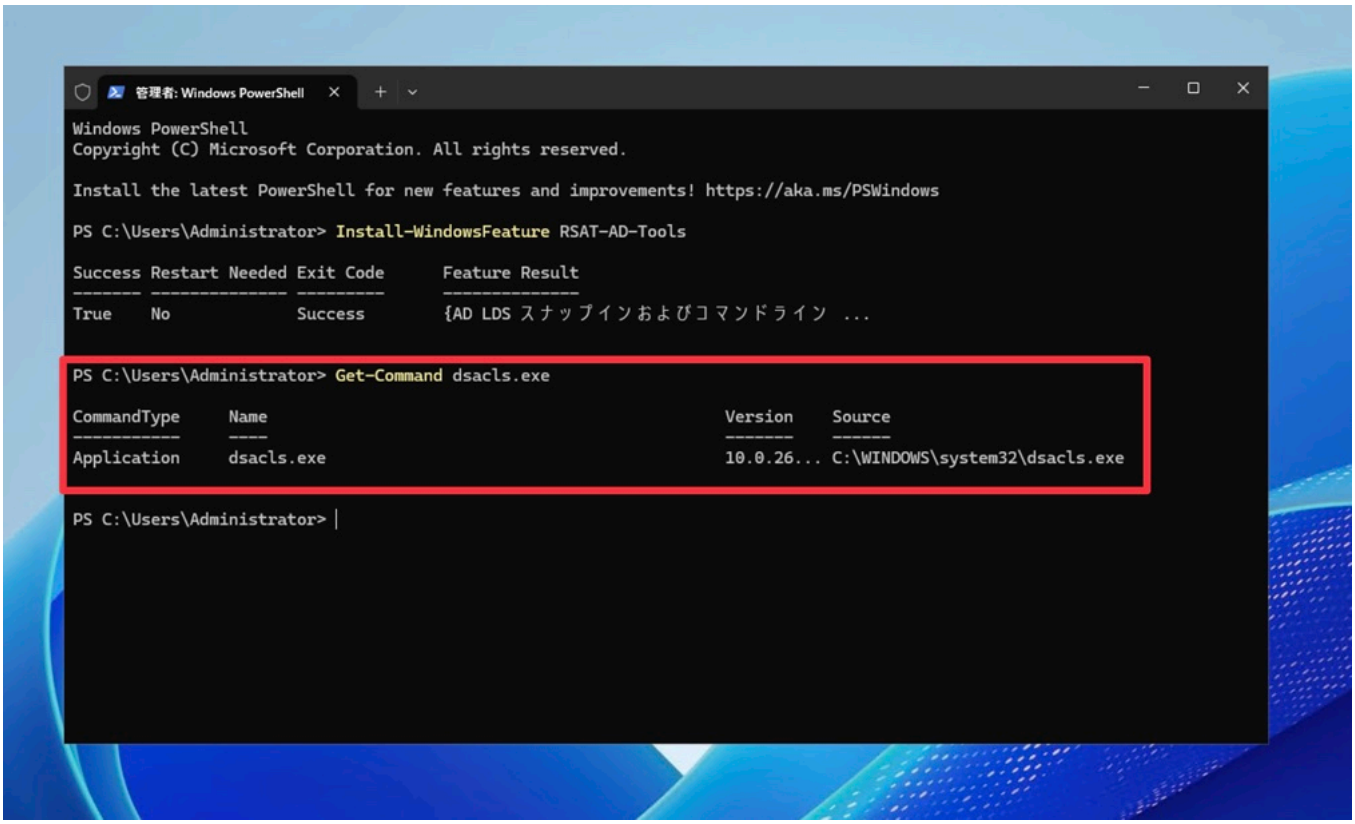
1. 以下のコマンドを実行し、インストールを行います。

```
Install-WindowsFeature RSAT-AD-Tools
```



2. インストールが完了後、以下のコマンドを実行し、dsacls.exeが実行できることを確認します。

```
Get-Command dsacls.exe
```

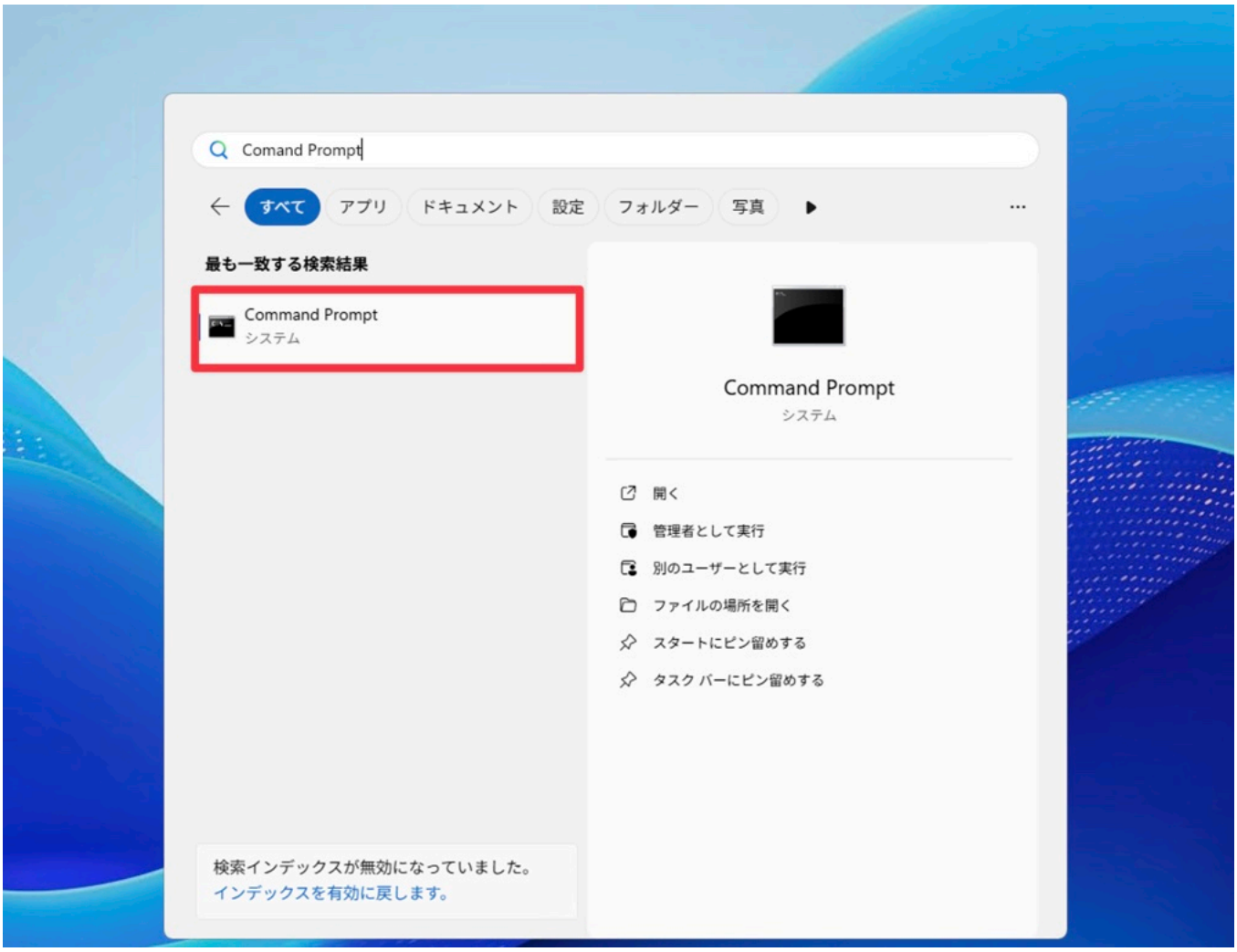


バージョン情報等が正しく表示されますと、インストールは完了です。

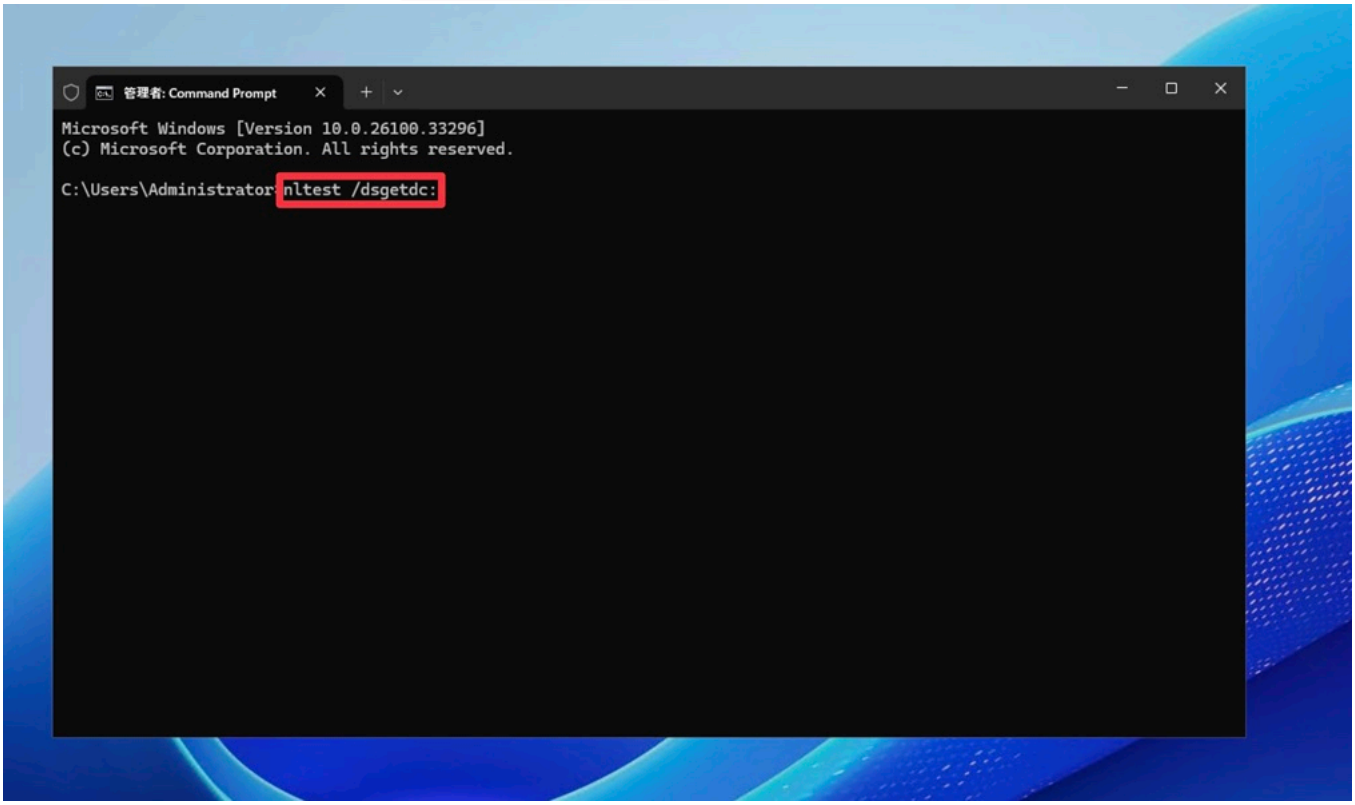
ドメイン名とドメイン識別名の確認

ここでは 2. OneLogin Active Directory ConnectorをWindows Serverにインストールする 手順19、手順21 で用いるドメイン名とドメイン識別名の確認方法を解説いたします。

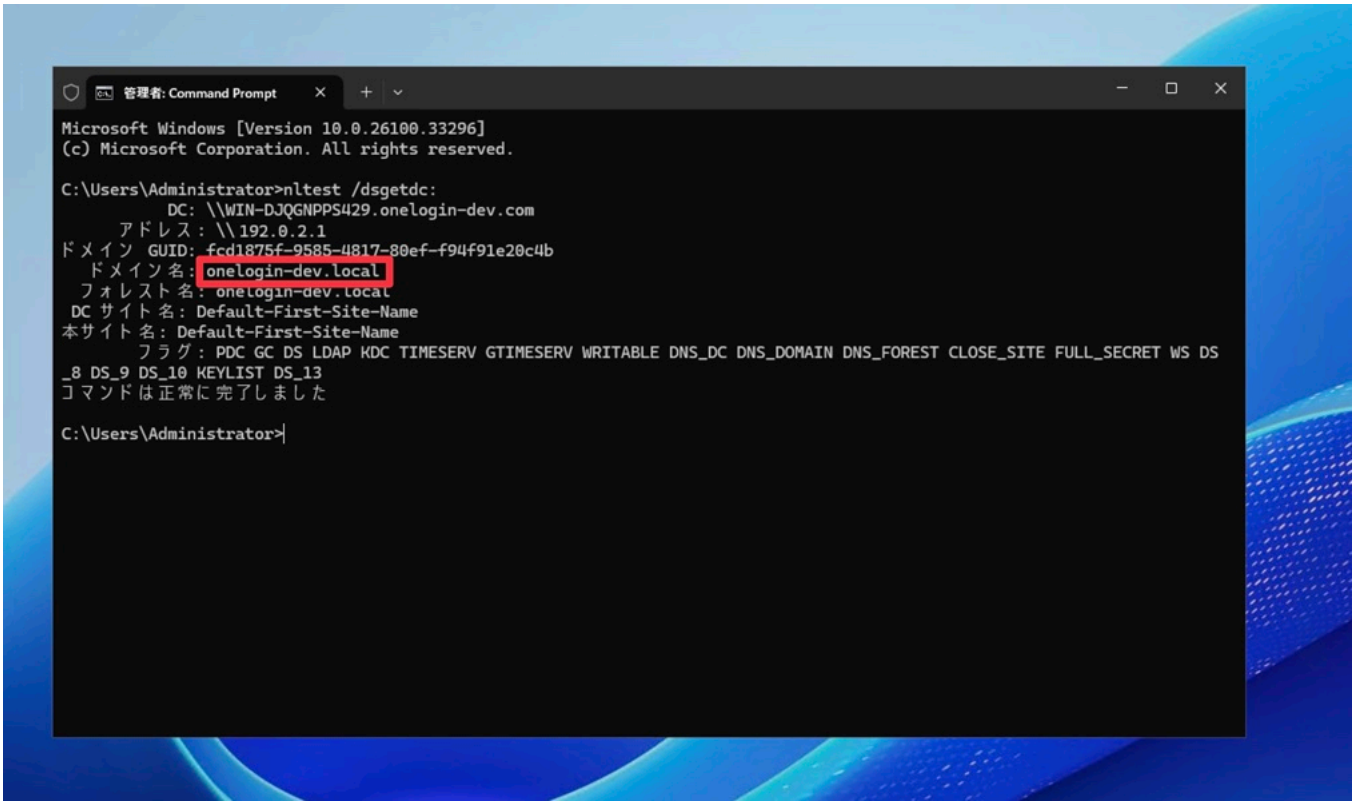
1. OneLogin ADCをインストールするサーバーへ接続し、コマンドプロンプトを実行します



2. 開いたコマンドプロンプトに `nltest /dsgetdc:` と入力します



3. **ドメイン名** に記載されている値がご利用いただいている環境のドメイン名となります
   ドメイン識別名 は確認したドメイン名の各要素の先頭に **DC=** を付け、それぞれを , で結合した形式の値となります
   例）ドメイン名が **onelogin-dev.local** の場合、ドメイン識別名は **DC=onelogin-dev,DC=local** となります



トラブルシュート

1. インストールにおけるトラブル

OneLogin ADCのインストールにおけるトラブルの多くはActive DirectoryとOneLoginが疎通しないことによるものです。その原因は主に以下の3つが考えられます。

- プロキシ認証
  プロキシサーバーを使用して出口対策をしている場合、通信の内容やOneLogin ADCシステム要件のネットワークレンジへの通信が許可されていないことにより、疎通していない可能性がありますので、設定の再確認をお願いいたします
- ファイアウォール
  OneLogin ADCシステム要件のネットワークレンジへの通信が許可されていない場合がありますので、設定の再確認をお願いいたします
- アカウントの権限
  OneLogin ADCのサービス実行用アカウントを手動で作成した場合、付与した権限が不足している可能性があります。OneLogin ADCアカウントの設定 手順13に記載されている権限が付与されているかのご確認をお願いいたします

2. ユーザー同期に関するトラブル

- 必須属性の入力漏れ
  Active Directory上でユーザーを作成してもOneLoginに同期されない場合、OneLoginへの同期に必須となる属性が不足している場合があります。必須属性である「電子メール」「姓」「名」が全て入力されているかの確認をお願いいたします
- 同期処理のタイムアウト
  ユーザーの属性を変更しても同期が正しく行われない場合、所属している全ユーザーを同期する時間よりも、システムに設定された同期の間隔が短いことに起因している可能性があります。概ねユーザー数1,000名に対して同期に10分以上かかることが確認されております。デフォルトの同期間隔は15分で設定されているため、大規模なユーザー数を同期する場合はこのトラブルが発生しかねませんので、ユーザー同期間隔の変更をご参考に同期間隔の調整をお願いいたします

その他、詳細なトラブルシュートはActive Directory ディレクトリ連携のよくあるトラブルシューティングも合わせてご確認ください。

CONFIDENTIAL

当ウェブサイトに掲載されている情報は一般公開されているコンテンツを除き、当社の承諾なくご契約者様以外への開示・転送・転載することはできません