2018年6月14日 Ver2.0

WowTalk

Active Directory 連携ガイド

Ver.2.0

注意事項

1. 本書の著作権は「ワウテック株式会社(以下、当社という)」に帰属します。

２. 本書のいかなる部分においても、当社に事前の書面による許可なく、電子的、機械的を含むいかなる手段や形式によってもその複製、改変、頒布、ならびにそれらに類似する行為を禁止します。

３. 本仕様書は貴社と当社との間で締結した契約において秘密情報として規定される情報です。本仕様書の取扱いは契約の規定に従ってください。

４. 本書の内容は、予告なく随時更新されます。

５. 本書の内容について万全を期しておりますが、万一記載もれ等お気づきの点がございましたら、当社までご連絡下さい。

更新履歴

バージョン	更新日時	内容
1.0	2016年11月11日	新規作成
2.0	2018年6月14日	一部画面キャプチャの差し替え

目次

1. 概要

Active Directory フェデレーションサービス（以下 AD FS）での認証情報と連携し、WowTalk へシングルサインオンを行うための設定方法について説明します。

2. システム要件

Windows Server 環境上に以下の3つのアプリケーションが必要です。

- Active Direcotry ドメインサービス
- DNS
- AD FS

外部ネットワークから接続する場合には、プロキシサーバーを構築し以下のアプリケーションをインストールして AD 環境と連携します。

- Web Application Proxy　もしくは　ADFS Proxy

サーバー証明書を作成する場合には以下のアプリケーションをインストールします

- Active Directory 証明書サービス

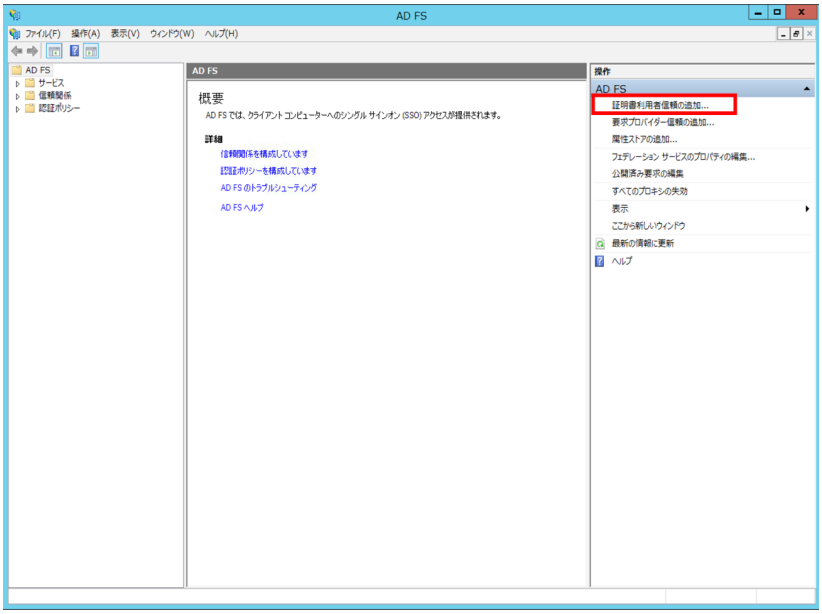
3. AD FS との認証連携の設定

WowTalk が AD FS での認証を有効化するには WowTalk と信頼関係を結ぶ必要があります。

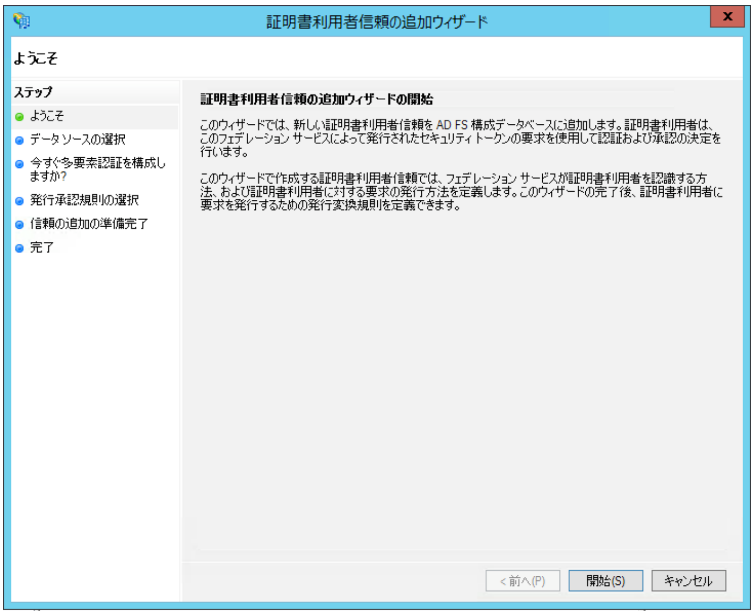
3.1. WowTalk 管理サイトでメタデータダウンロード

1. WowTalk 管理者サイトで［外部サービス連携］>［AD 連携設定］を選択します。
2. 「Service Provider のメタデータをダウンロード」をクリックします。
3. 「wowtalk_sp_metadata.xml」というメタデータファイルがダウンロードされます。

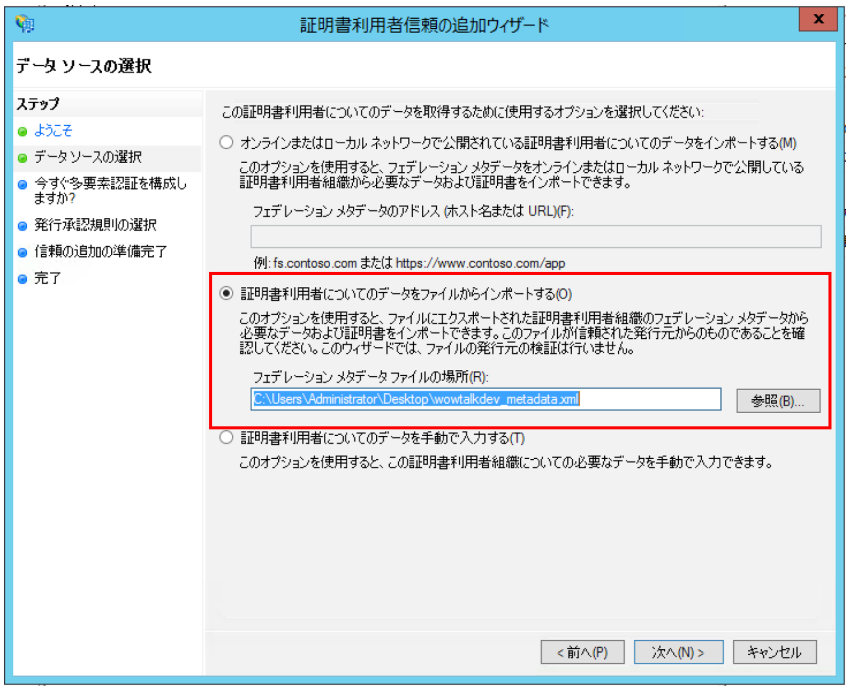
3.2. ADFS で信頼できる証明書利用者として WowTalk を登録する



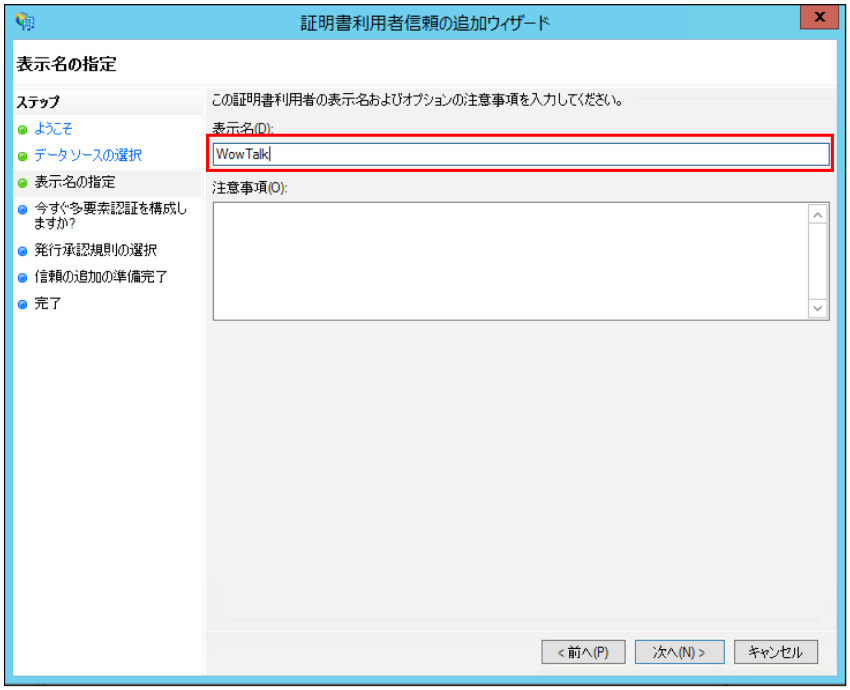
1. Windows Server で「ADFS の管理」を起動します。
2. 「証明書利用者信頼の追加」を選択します。



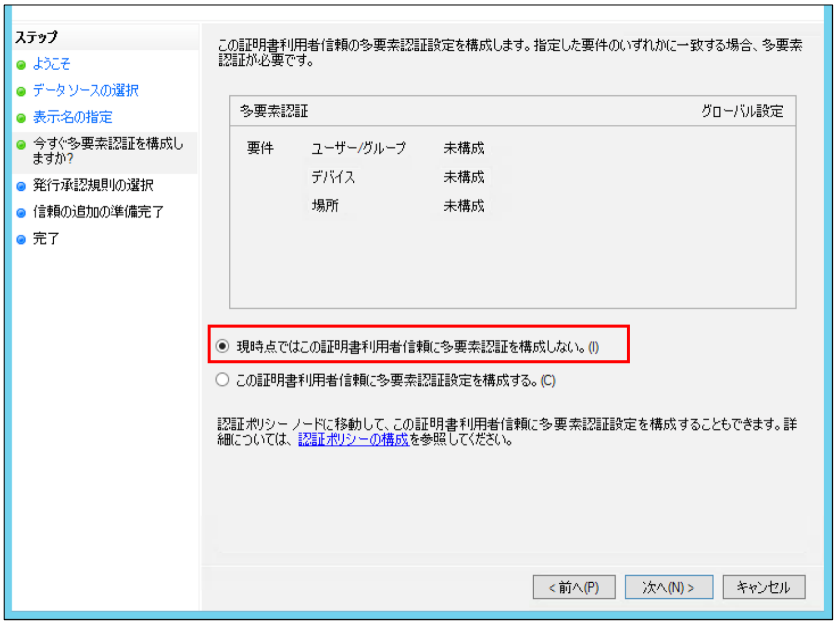
1. 「開始」ボタンをクリックします。



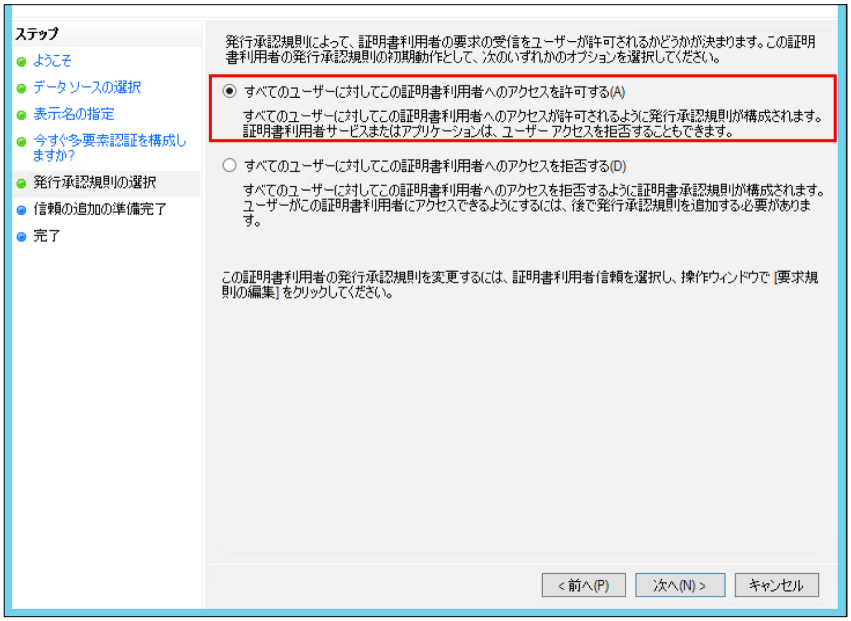
1. 「証明書利用者についてのデータをファイルからインポートする」を選択し、
2. 「手順3.1」でダウンロードしたメタデータファイルを登録します。
3. 「次へ」を選択します。



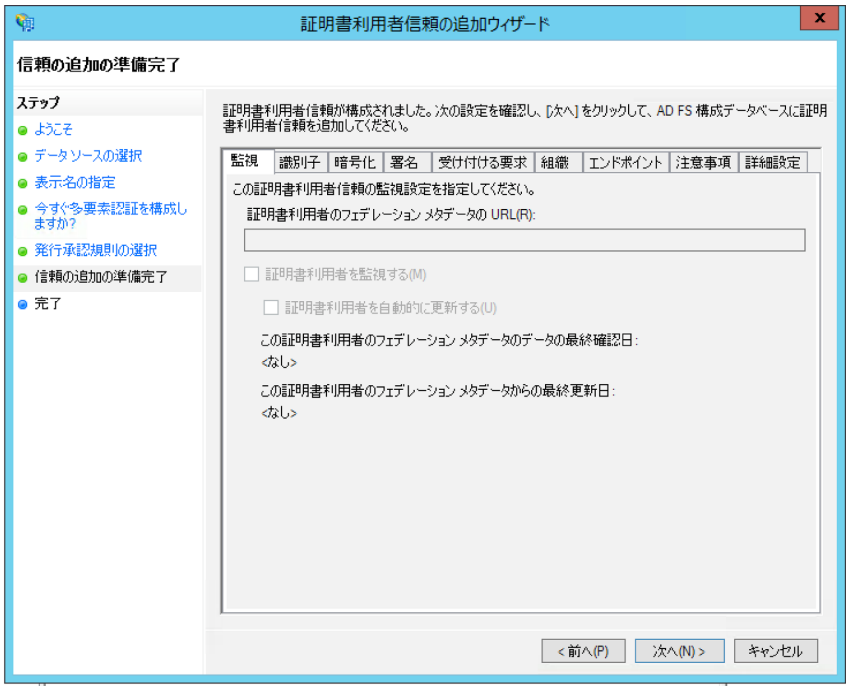
1. 表示名（どんなものでも構いません）を登録します。
2. 「次へ」ボタンをクリックします。



1. 「現時点ではこの証明書利用者信頼に多要素認証は構成しない」を選択します。
2. 「次へ」ボタンをクリックします。

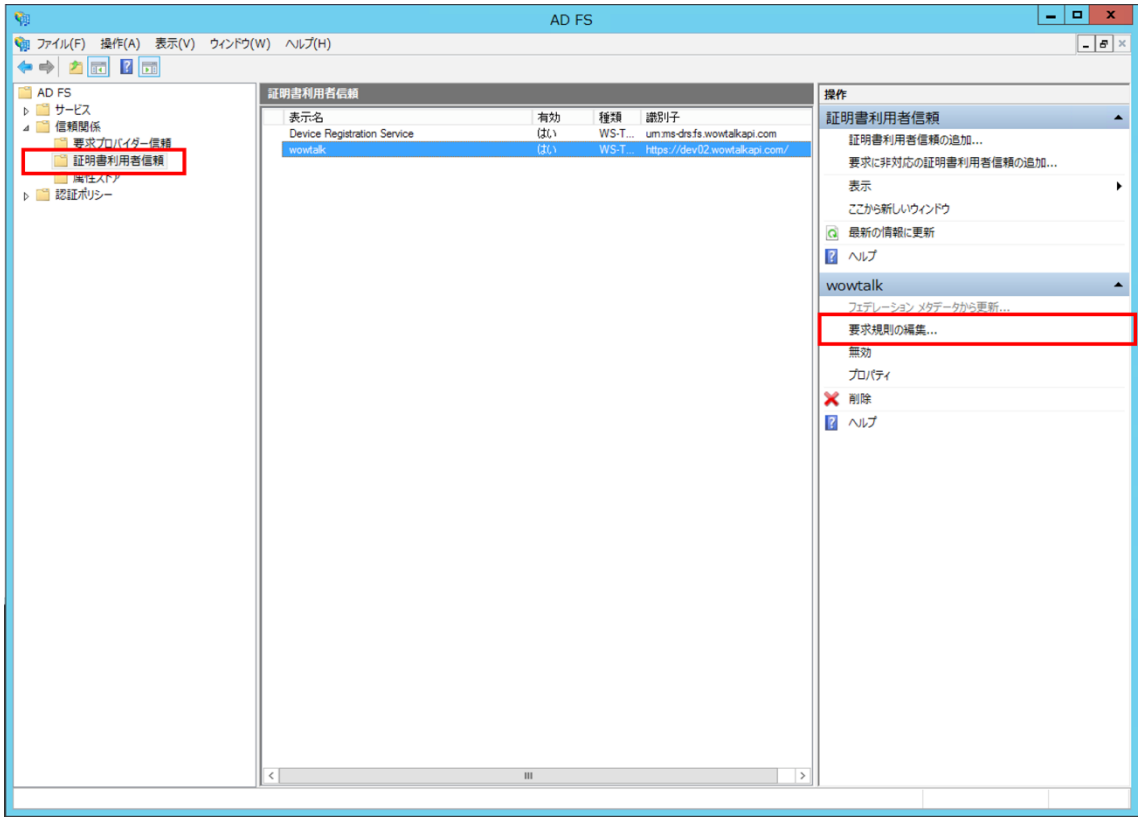


1. 「すべてのユーザーに対してこの証明書利用者へのアクセスを許可する」を選択します。
2. 「次へ」ボタンをクリックします。

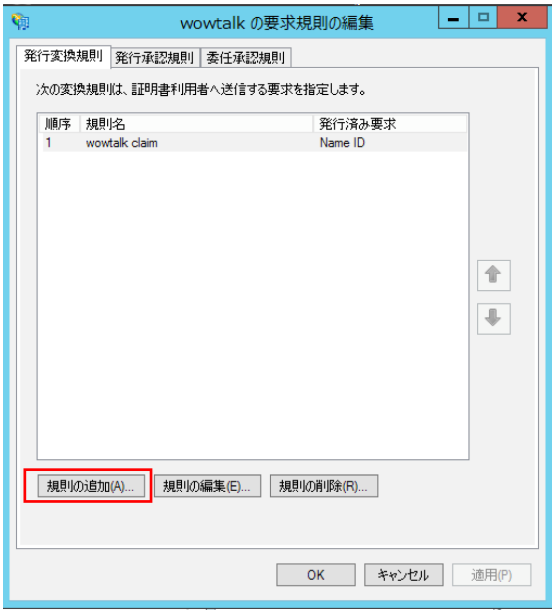


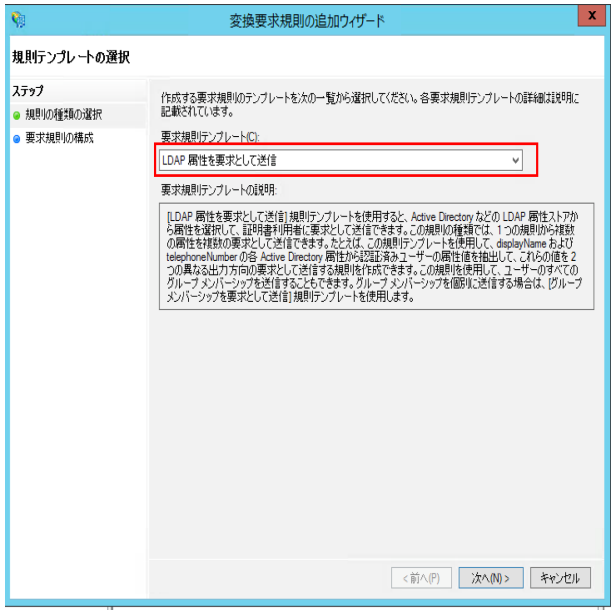
1. 「次へ」ボタンをクリックします。

3.3. 要求規則の設定

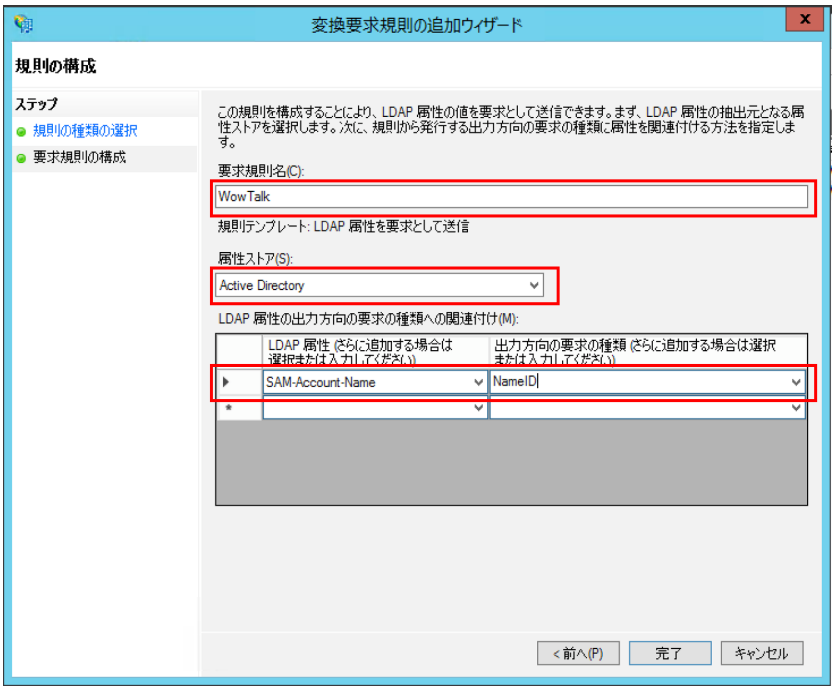


1. 「ADFS の管理」の左カラムで[ADFS]>[信頼関係]>[証明書利用者信頼]をクリックします。
2. 証明書利用者信頼の表示名が3.2で設定した表示名の項目をクリックします。
3. 右カラムで[<表示名>] > [要求規則の編集]をクリックします。





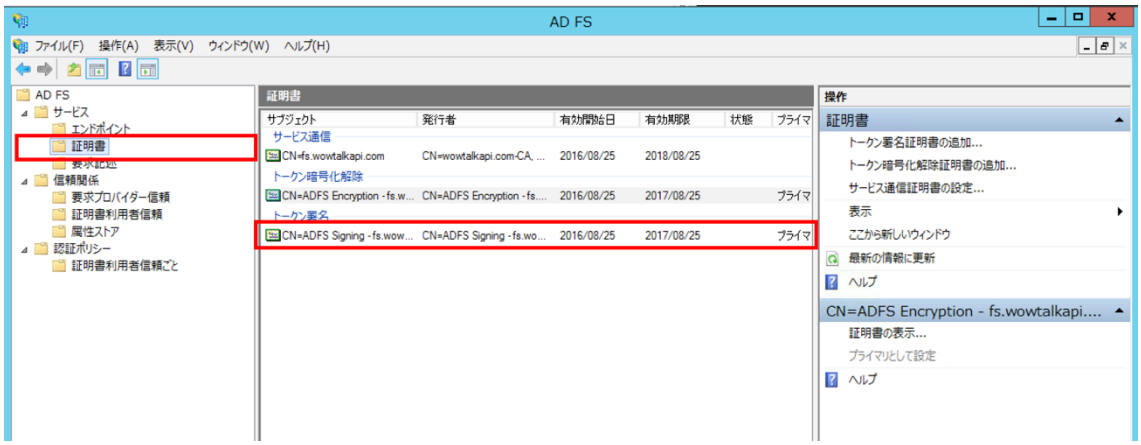
1. 「規則の追加」をクリックします。
2. 要求規則テンプレートを「LDAP 属性として送信」設定します。
3. 「次へ」をクリックします。



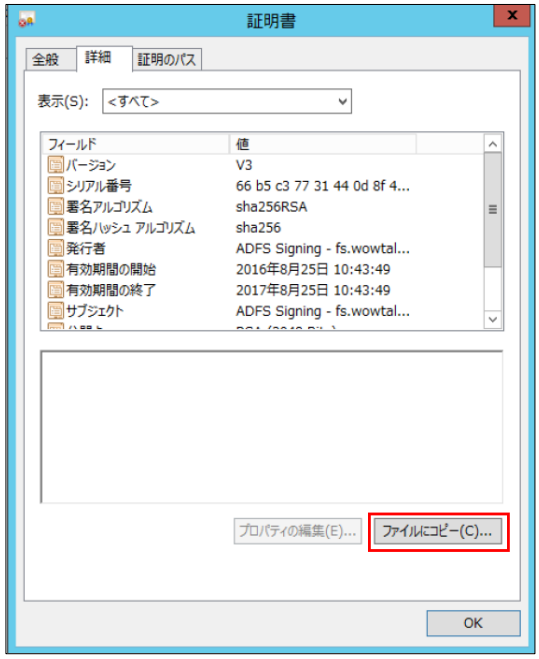
1. 要求規則名(どんなものでも構いません)を設定します。
2. 属性ストアを「Active Directory」に設定します。
3. LDAP 属性を「SAM-Account-Name」に設定します。
4. 出力方向の要求の種類を「Name ID」と設定ます。
5. 「完了」ボタンをクリックします。

3.4. トークン署名の証明書を発行

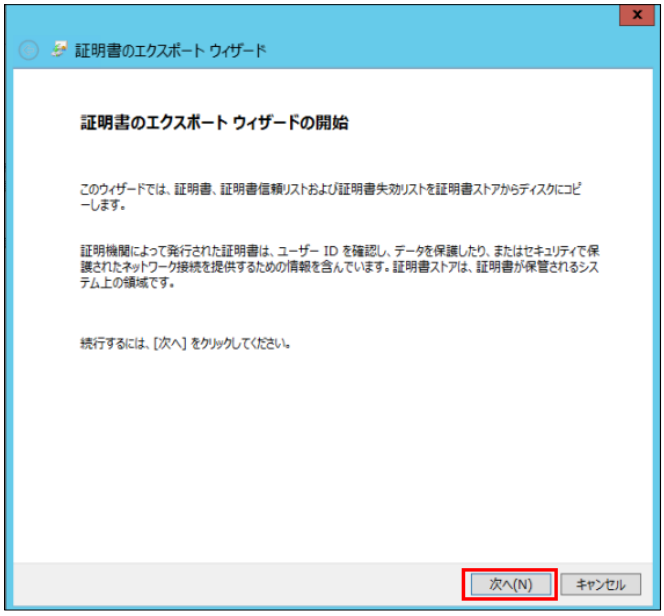
AD FS の管理で[AD FS]>[サービス]>[証明書]を選択します。



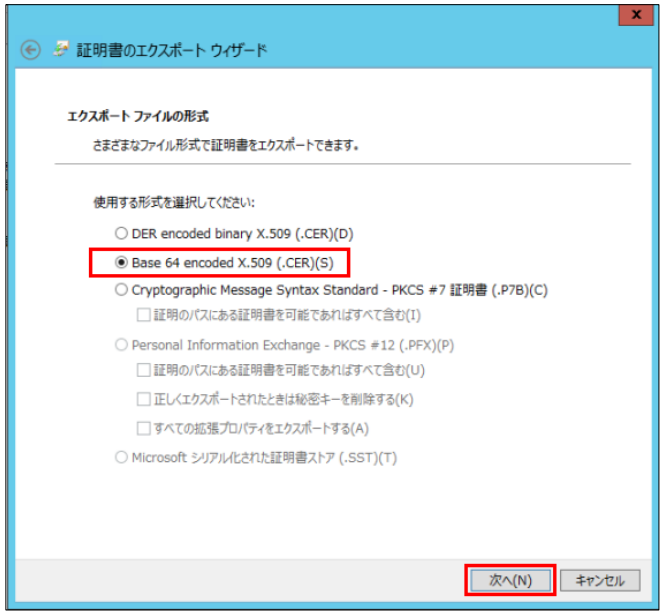
1. AD FS の管理画面で[AD FS]>[サービス]>[証明書]を選択します。



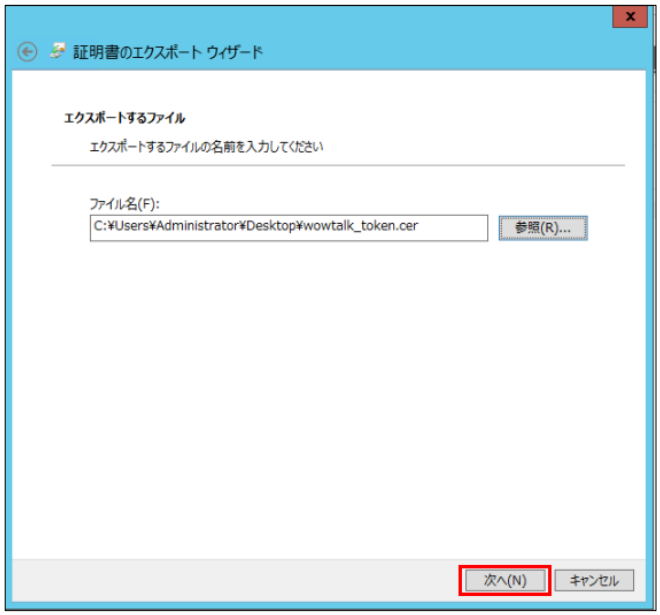
1. 証明書のウィンドウが現れます。
2. 「詳細」タブをクリックします。
3. 「ファイルにコピー」ボタンをクリックします。



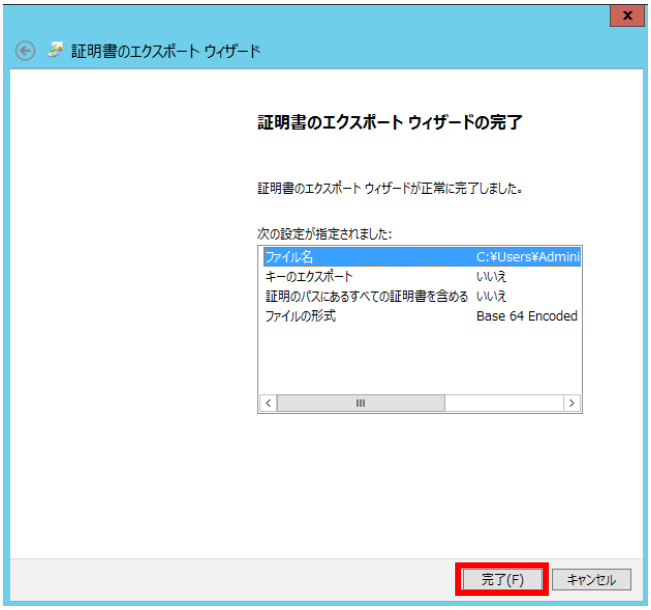
1. 証明書のエクスポートウィザードが表示されます。
2. 「次へ」ボタンをクリックします。



1. 「Base 64 encoded X.509 (.CER)」を指定します。
2. 「次へ」ボタンをクリックします。



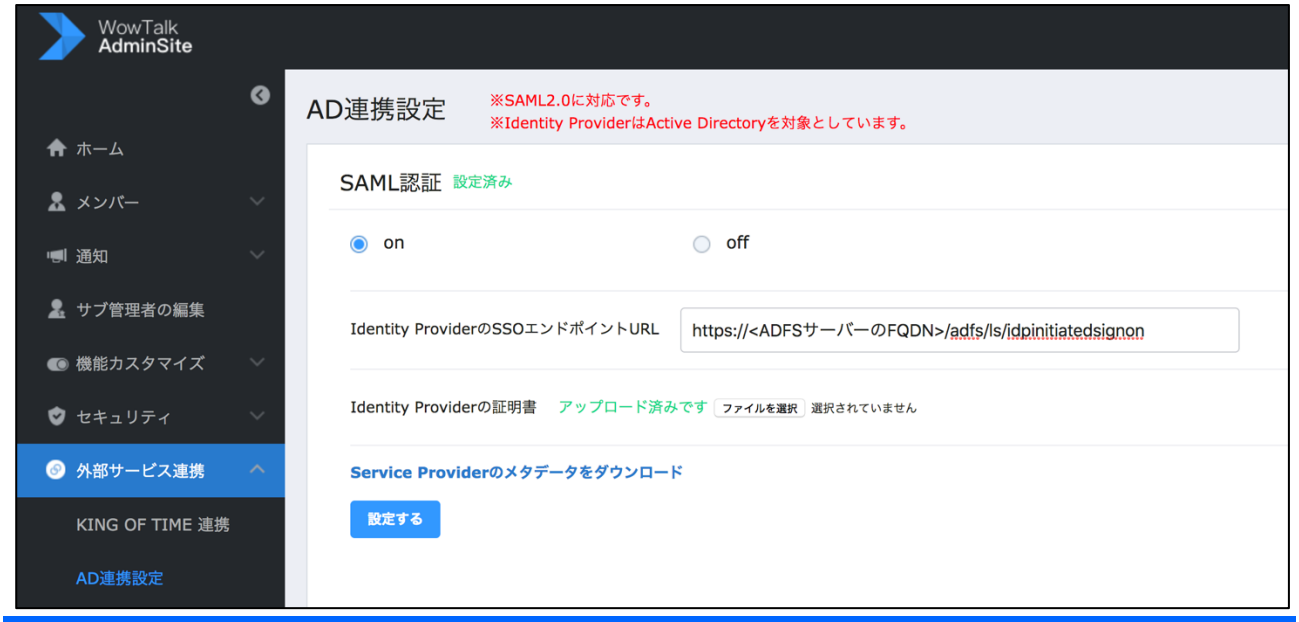
1. エクスポートする証明書のファイル名を指定します。
2. 「次へ」ボタンをクリックします。



1. 「完了」ボタンをクリックします。
2. 指定した場所に証明書ファイルがエクスポートされます。

3.5. WowTalk 管理サイトで AD 連携用の設定をする

1. [外部サービス連携]>[AD 連携設定]の順にクリックします。
2. AD 連携設定画面が表示されます。
3. 「on」に設定します。
4. 「Identity Provider の SSO エンドポイント URL」を
   「https://<ADFS サーバーの FQDN>/adfs/ls/idpinitiatedsignon」に設定します。
5. 「Identity Provider の証明書」の「ファイルを選択」をクリックし、[3.4]で発行した証明書をアップロードします。「設定する」ボタンをクリックします。



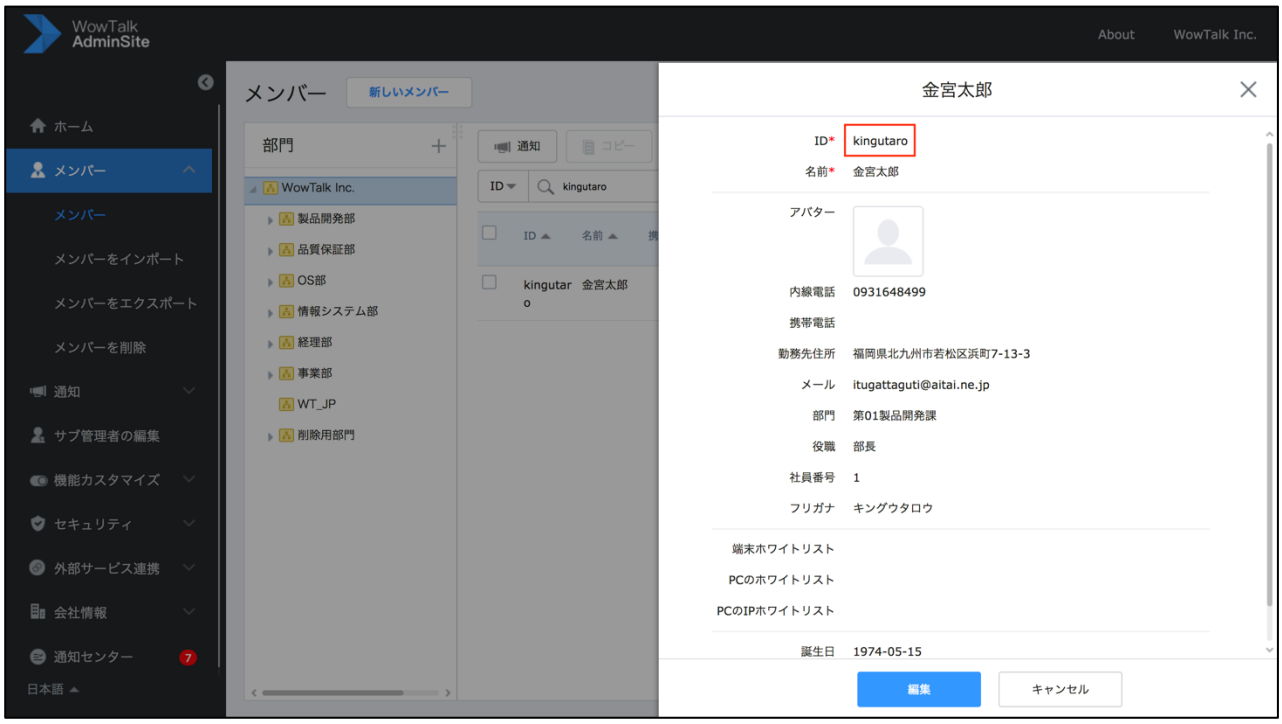
1. 入力した項目が反映され、設定情報が表示されます。

4. ユーザー登録

ActiveDirectory のアカウントで WowTalk にログインするためには、ActiveDirectory の SAM アカウントと個人 ID を同一のものにする必要があります。

■ ActiveDirectory 管理センター　ユーザー詳細情報画面

■ WowTalk 管理サイト ユーザー登録画面



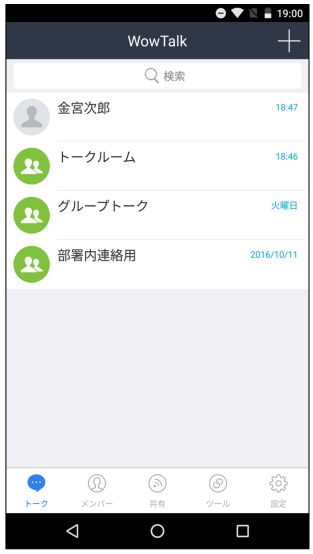
5. ログイン方法

5.1. iOS 版からログインする

1. 「Active Directory でログイン」をタップします。ログイン画面が表示されます。
2. 「法人 ID」と「個人 ID」を入力し、「ログイン」ボタンをタップします。
3. ActiveDirectory のログイン画面が表示されます。
4. 「法人 ID」と「個人 ID」を入力し「サインイン」ボタンをタップします。
5. トーク一覧画面が表示されます。

5.2. Android 版からログインする

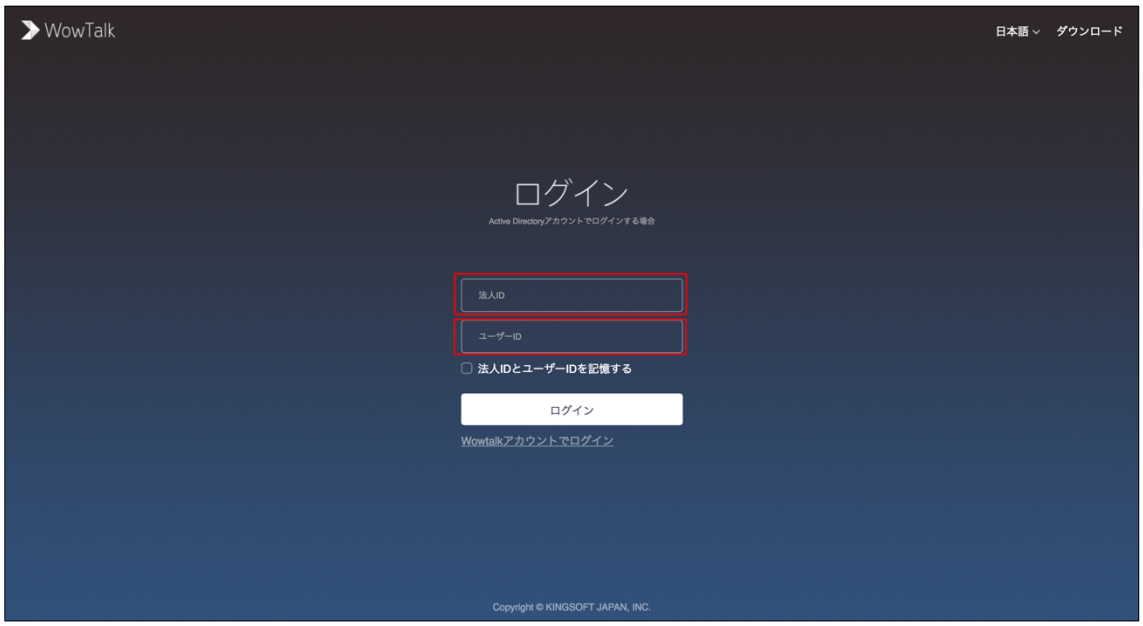
1. 「Active Directory でログイン」をタップします。
2. ActiveDirectory アカウントでのログイン画面が表示されます。
3. 「法人 ID」と「個人 ID」を入力します。ActiveDirectory のログイン画面が表示されます。
4. 「SAM アカウント」と「パスワード」を入力して「サインイン」をタップします。



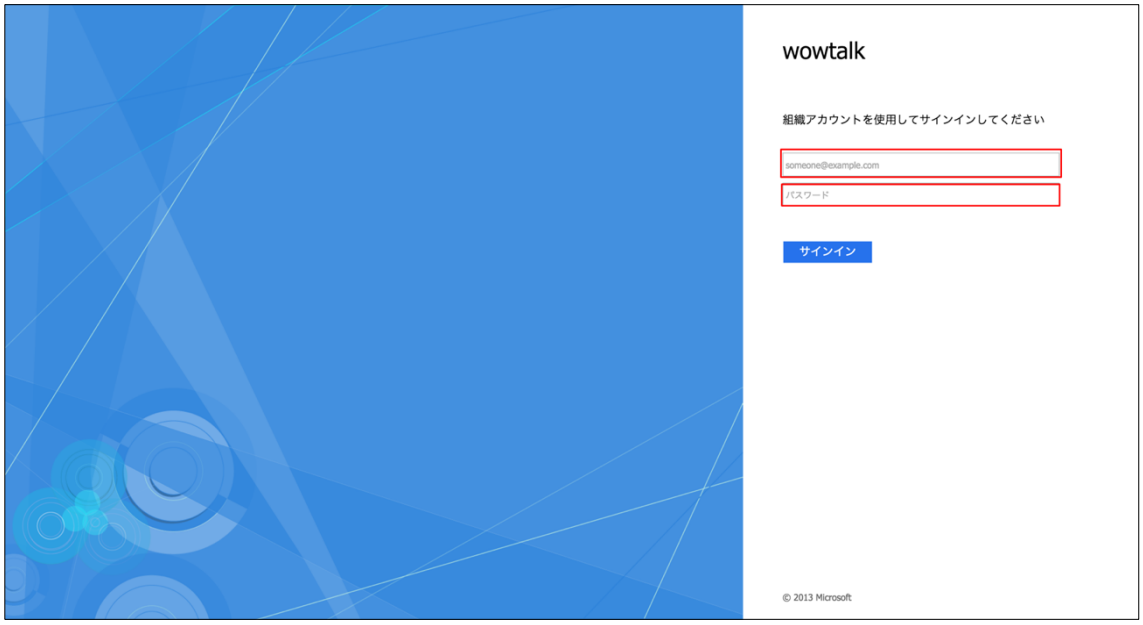
1. トーク一覧画面が表示されます。

5.3. ユーザー向け Web 画面からログインする

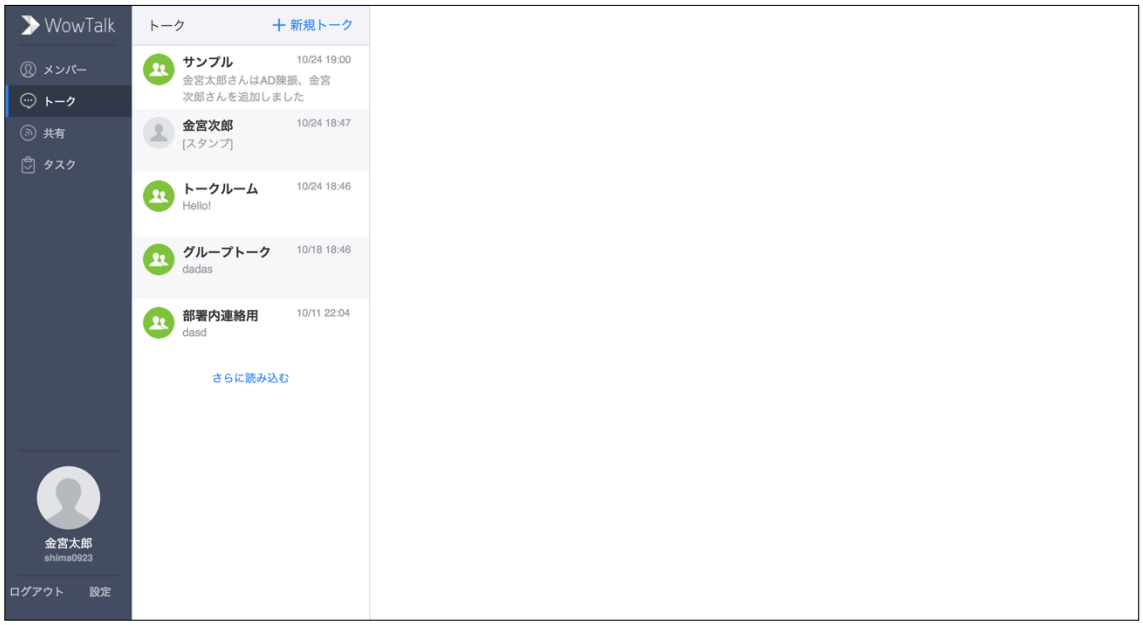
1. 「Active Directory アカウントでログイン」をクリックします。



1. ActiveDirectory でのログイン画面が表示されます。
2. 「法人 ID」と「個人 ID」を入力して「ログイン」ボタンをクリックします。
3. Active Directory のログイン画面へ遷移します。



1. 「ログイン ID」と「パスワード」を入力します。
2. 「サインイン」をクリックします。



1. ログインが完了しトーク一覧画面が表示されます。
2. 利用を開始することができます。