

WowTalk

Active Directory 連携ガイド

Ver. 2.0

つながる実感。社内コミュニケーションアプリ

 WowTalk

3つの機能で社内のコミュニケーションを活性化！

- 社内チャット
- タイムライン
- 無料通話

パソコン・スマートフォン対応



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.....	5
2.	システム要件.....	5
3.	AD FS との認証連携の設定	6
3.1.	WowTalk 管理サイトでメタデータダウンロード	6
3.2.	ADFS で信頼できる証明書利用者として WowTalk を登録する	7
3.3.	要求規則の設定	11
3.4.	トークン署名の証明書を発行	14
3.5.	WowTalk 管理サイトで AD 連携用の設定をする	18
4.	ユーザー登録.....	19
5.	ログイン方法.....	20
5.1.	iOS 版からログインする	20
5.2.	Android 版からログインする	21
5.3.	ユーザー向け Web 画面からログインする	22

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 ヘ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 Directory 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

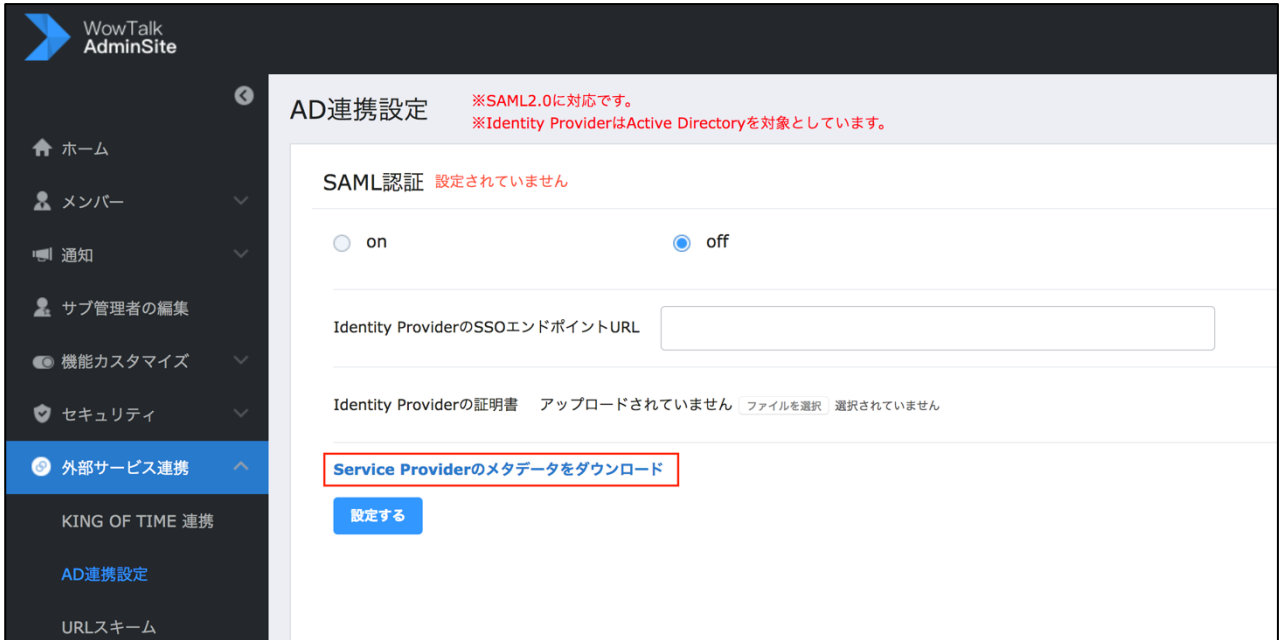
サーバー証明書を作成する場合には以下のアプリケーションをインストールします

- 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



WowTalk AdminSite

AD連携設定 ※SAML2.0に対応です。
※Identity ProviderはActive Directoryを対象としています。

SAML認証 設定されていません

☐ on ☒ off

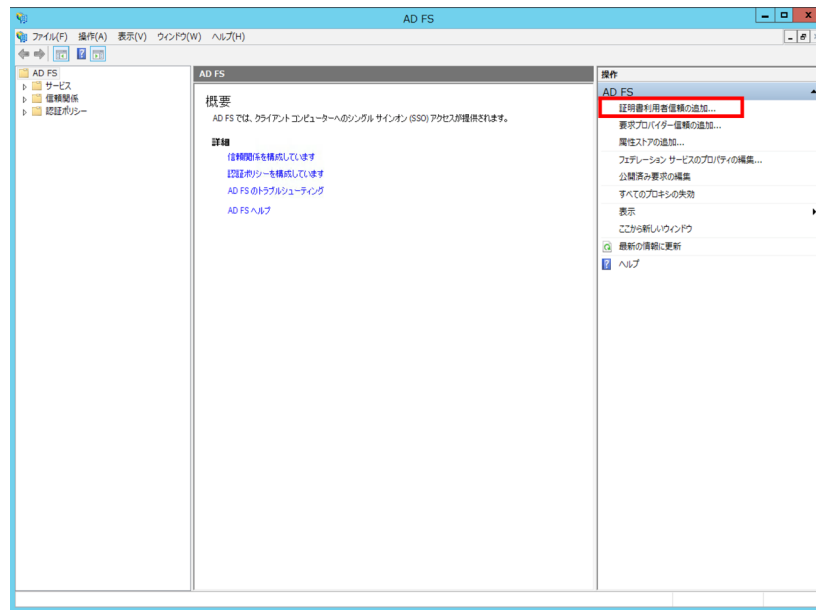
Identity ProviderのSSOエンドポイントURL

Identity Providerの証明書 アップロードされていません 選択されていません

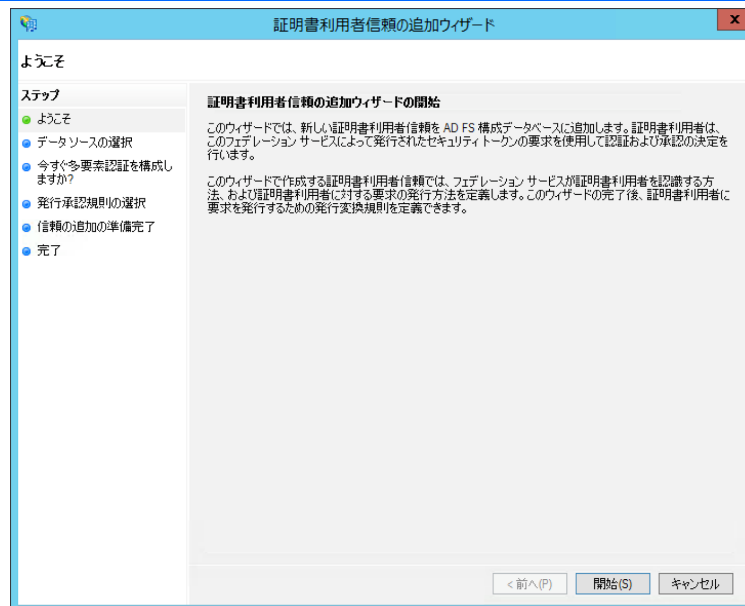
Service Providerのメタデータをダウンロード

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。

証明書利用者信頼の追加ウィザード

データソースの選択

ステップ

- ようこそ
- データソースの選択
- 今すぐ多要素認証を構成しますか?
- 発行承認規則の選択
- 信頼の追加の準備完了
- 完了

この証明書利用者についてのデータを取得するために使用するオプションを選択してください:

☐ オンラインまたはローカル ネットワークで公開されている証明書利用者についてのデータをインポートする(M)
このオプションを使用すると、フェデレーション メタデータをオンラインまたはローカル ネットワークで公開している証明書利用者組織から必要なデータおよび証明書をインポートできます。

フェデレーション メタデータのアドレス (ホスト名または URL)(F):
例: fs.contoso.com または https://www.contoso.com/app

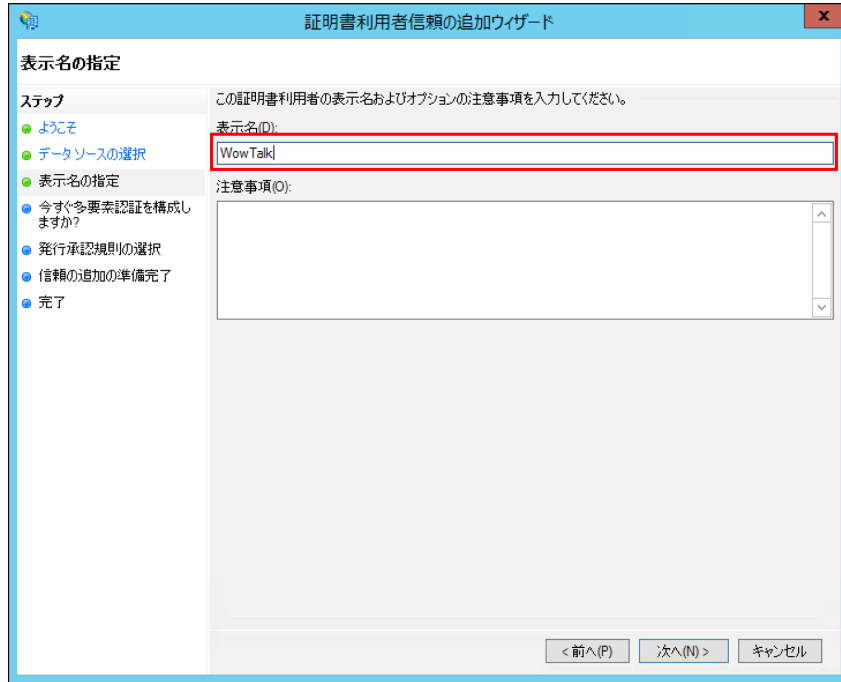
☒ 証明書利用者についてのデータをファイルからインポートする(O)
このオプションを使用すると、ファイルにエクスポートされた証明書利用者組織のフェデレーション メタデータから必要なデータおよび証明書をインポートできます。このファイルが信頼された発行元からのものであることを確認してください。このウィザードでは、ファイルの発行元の検証は行いません。

フェデレーション メタデータ ファイルの場所(F):
 参照(B)...

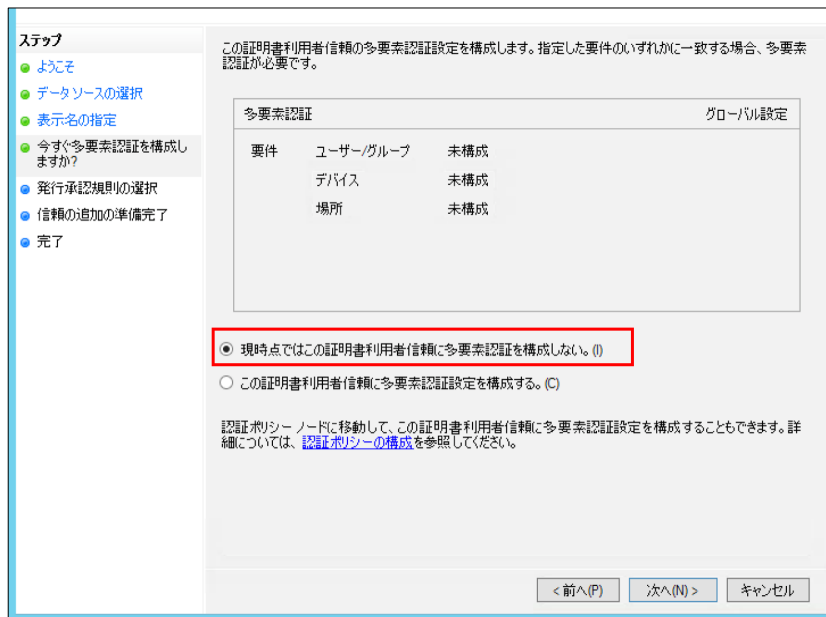
☐ 証明書利用者についてのデータを手動で入力する(I)
このオプションを使用すると、この証明書利用者組織についての必要なデータを手動で入力できます。

< 前へ(P) 次へ(N) > キャンセル

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。

ステップ

- ようこそ
- データソースの選択
- 表示名の指定
- 今すぐ多要素認証を構成しますか?
- 発行承認規則の選択
- 信頼の追加の準備完了
- 完了

発行承認規則によって、証明書利用者の要求の受信をユーザーが許可されるかどうかが決まります。この証明書利用者の発行承認規則の初期動作として、次のいずれかのオプションを選択してください。

☒ 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(A)
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が許可されるように発行承認規則が構成されます。証明書利用者サービスまたはアプリケーションは、ユーザーアクセスを拒否することもできます。

☐ 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拒否する(D)
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拒否するように証明書承認規則が構成されます。ユーザーがこの証明書利用者にアクセスできるようにするには、後で発行承認規則を追加する必要があります。

この証明書利用者の発行承認規則を変更するには、証明書利用者情報を選択し、操作ウィンドウで [要求規則の編集] をクリックしてください。

< 前へ(P) 次へ(N) > キャンセル

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。

証明書利用者信頼の追加ウィザード

信頼の追加の準備完了

ステップ

- ようこそ
- データソースの選択
- 表示名の指定
- 今すぐ多要素認証を構成しますか?
- 発行承認規則の選択
- 信頼の追加の準備完了
- 完了

証明書利用者信頼が構成されました。次の設定を確認し、[次へ] をクリックして、AD FS 構成データベースに証明書利用者信頼を追加してください。

この証明書利用者信頼の監視設定を指定してください。

証明書利用者のフェデレーション メタデータの URL(R):

☐ 証明書利用者を監視する(M)

☐ 証明書利用者を自動的に更新する(U)

この証明書利用者のフェデレーション メタデータのデータの最終確認日:

<なし>

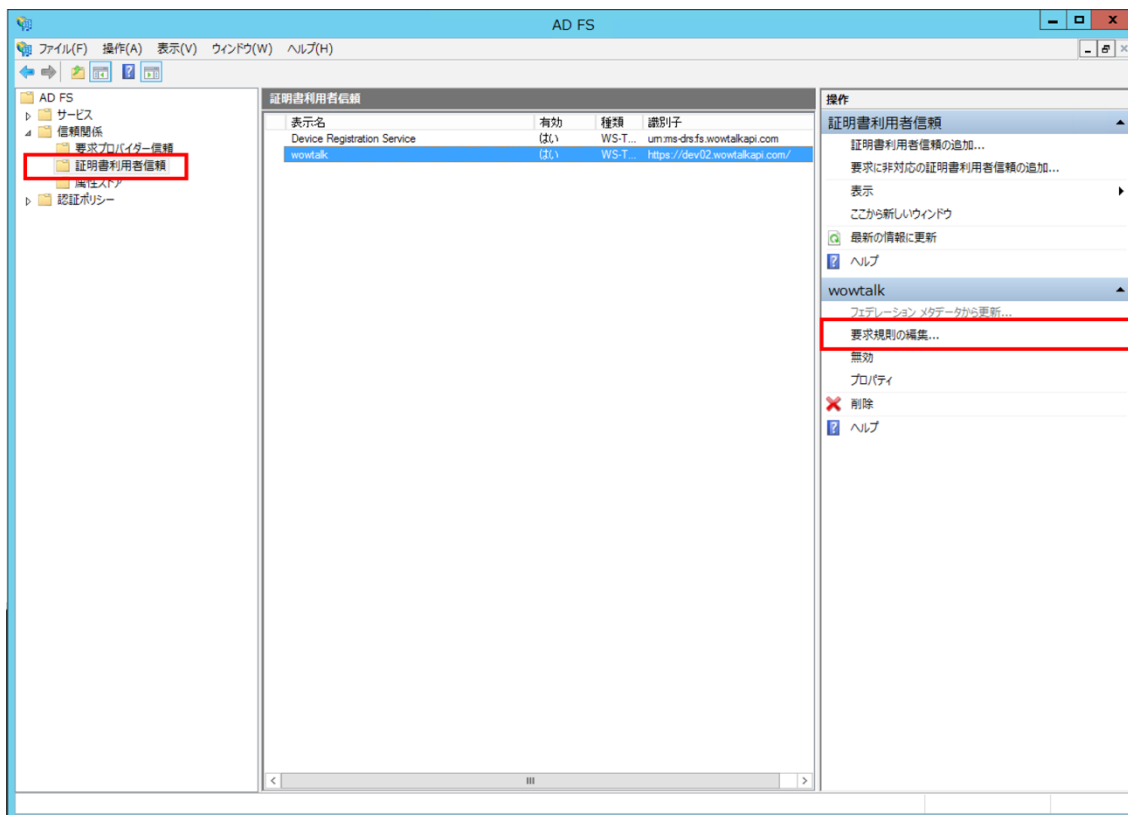
この証明書利用者のフェデレーション メタデータからの最終更新日:

<なし>

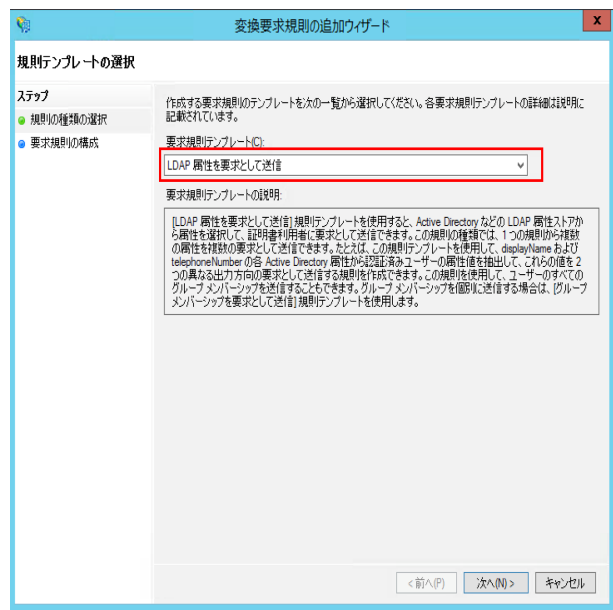
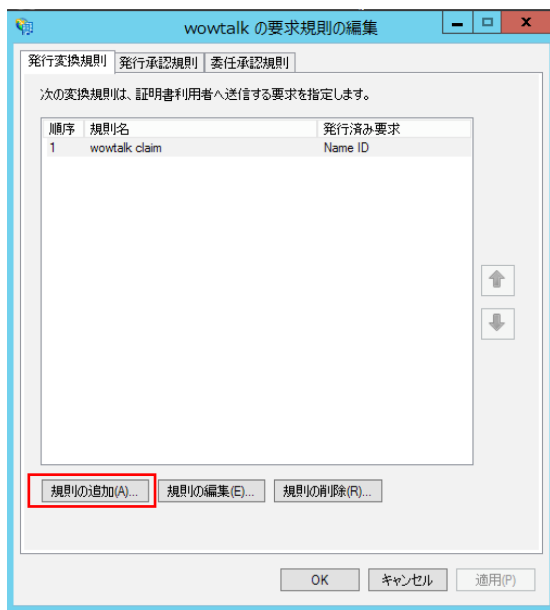
< 前へ(P) 次へ(N) > キャンセル

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。

変換要求規則の追加ウィザード

規則の構成

ステップ

- 規則の種類を選択
- 要求規則の構成

この規則を構成することにより、LDAP 属性の値を要求として送信できます。まず、LDAP 属性の抽出元となる属性ストアを選択します。次に、規則から発行する出力方向の要求の種類に属性を関連付ける方法を指定します。

要求規則名(C):
WowTalk

規則テンプレート: LDAP 属性を要求として送信

属性ストア(S):
Active Directory

LDAP 属性の出力方向の要求の種類への関連付け(M):

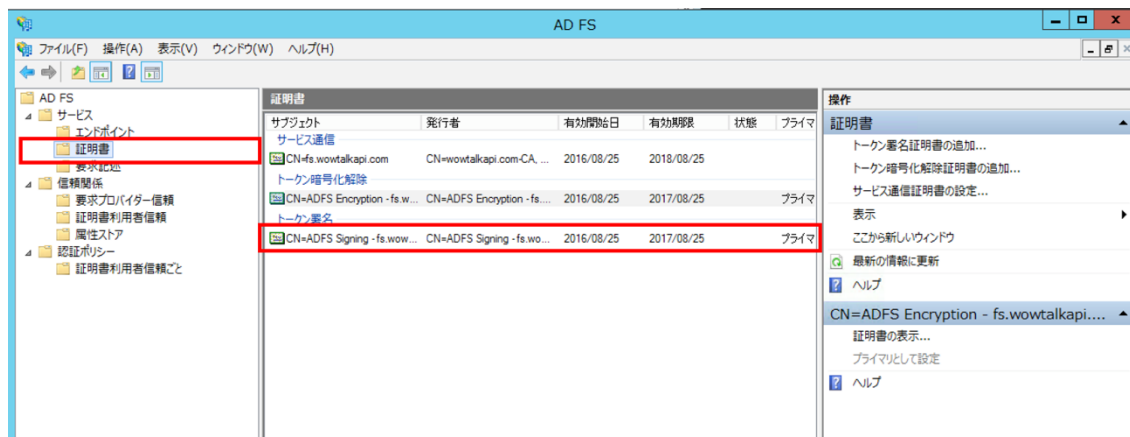
LDAP 属性 (さらに追加する場合は選択または入力してください)	出力方向の要求の種類 (さらに追加する場合は選択または入力してください)
▶ SAM-Account-Name	NameID
*	

< 前へ(P) 完了 キャンセル

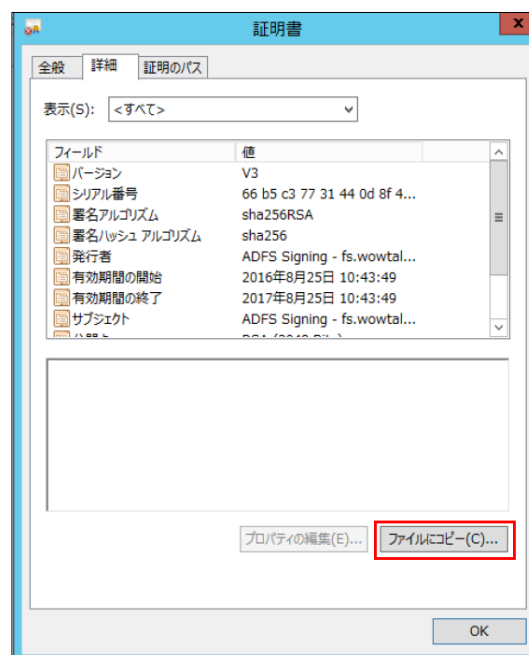
1. 要求規則名(どんなものでも構いません)を設定します。
2. 属性ストアを「Active Directory」に設定します。
3. LDAP 属性を「SAM-Account-Name」に設定します。
4. 出力方向の要求の種類を「Name ID」と設定します。
5. 「完了」ボタンをクリックします。

3.4. トークン署名の証明書を発行

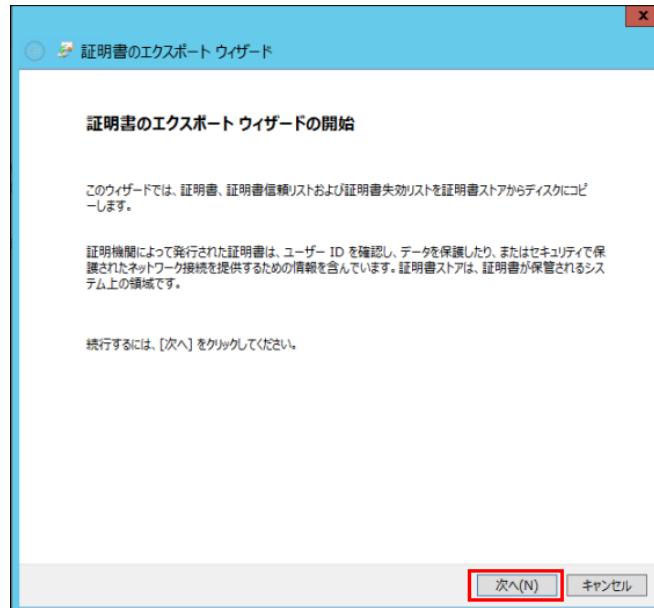
AD FS の管理で[AD FS]>[サービス]>[証明書]を選択します。



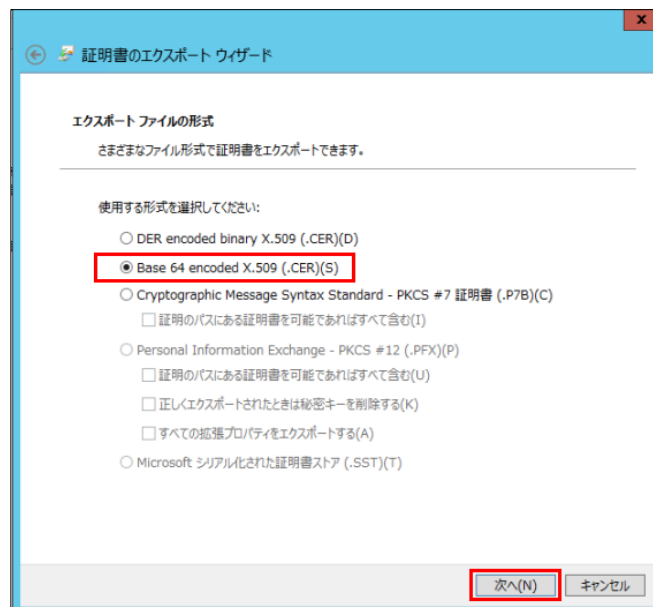
1. AD FS の管理画面で[AD FS]>[サービス]>[証明書]を選択します。



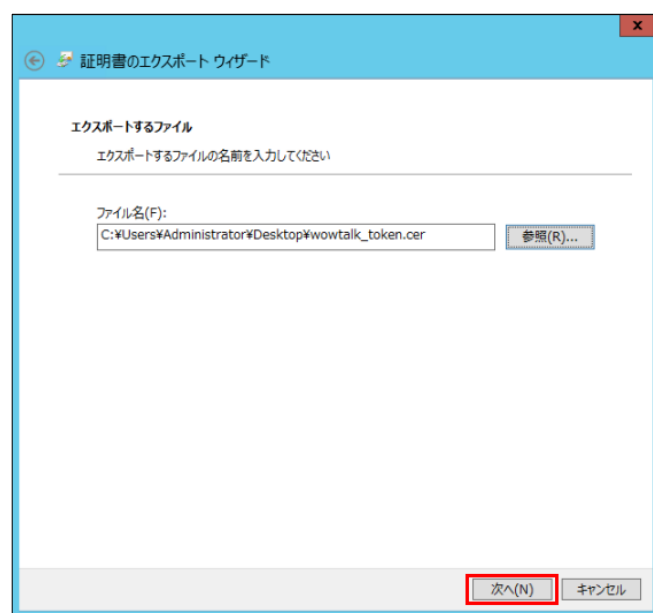
1. 証明書のウィンドウが現れます。
2. 「詳細」タブをクリックします。
3. 「ファイルにコピー」ボタンをクリックします。



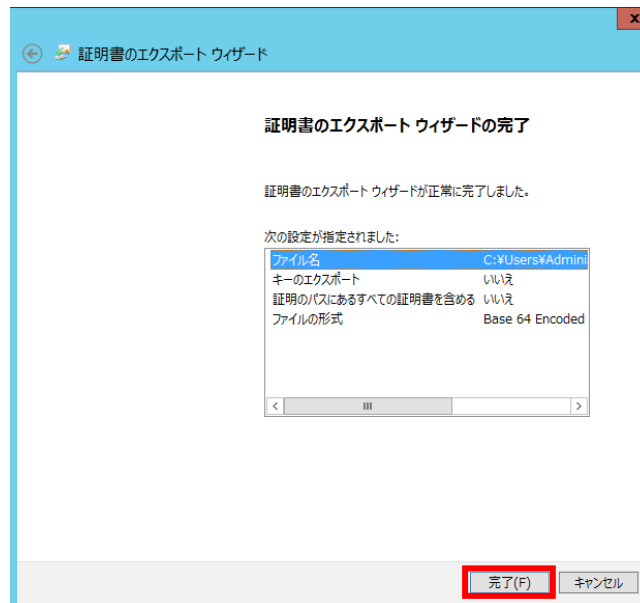
1. 証明書のエクスポートウィザードが表示されます。
2. 「次へ」ボタンをクリックします。



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。

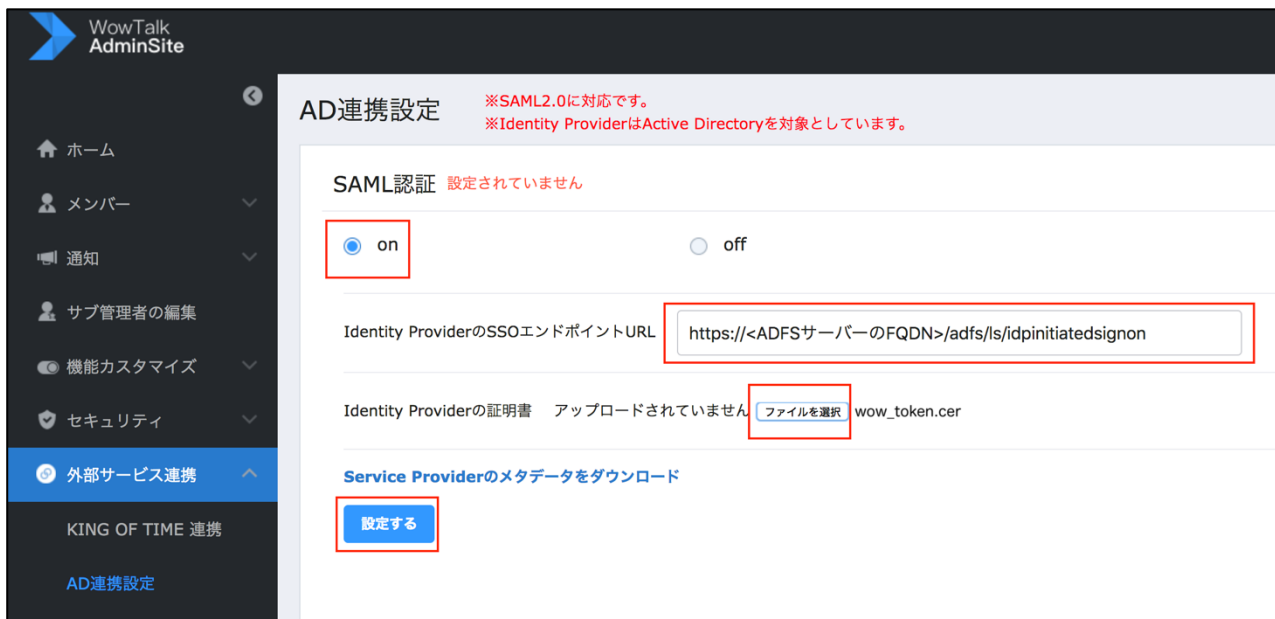


1. エクスポートする証明書のファイル名を指定します。
2. 「次へ」ボタンをクリックします。



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



WowTalk AdminSite

AD連携設定 ※SAML2.0に対応です。
※Identity ProviderはActive Directoryを対象としています。

SAML認証 設定されていません

☒ on ☐ off

Identity ProviderのSSOエンドポイントURL

Identity Providerの証明書 アップロードされていません wow_token.cer

Service Providerのメタデータをダウンロード

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。



WowTalk AdminSite

AD連携設定 ※SAML2.0に対応です。
※Identity ProviderはActive Directoryを対象としています。

SAML認証 設定済み

☒ on ☐ off

Identity ProviderのSSOエンドポイントURL

Identity Providerの証明書 アップロード済みです 選択されていません

Service Providerのメタデータをダウンロード

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

金宮 太郎

アカウント(A) アカウント

組織(O) フリガナ(姓): カネミヤ

所属するグループ(F) 姓: 金宮

パスワードの設定(S) フリガナ(名): タロウ

プロファイル(P) 名: 太郎

ポリシー フルネーム: 金宮 太郎

サイロ ユーザー UPN ログイン: @

拡張(E) ユーザー SAM アカウント: wowtalkapi

アカウントの期限: ☒ なし ☐ 有効期限

パスワードのオプション: ☐ ユーザーは次回ログイン時にパスワード変更が必要 ☒ その他のパスワード オプション

☐ 対話型ログインにはスマート カードが必要 ☒ パスワードを無期限にする ☐ ユーザーはパスワードを変更できない

番号化のオプション: ☐ その他のオプション: ☐

組織

フリガナ(表示名): カネミヤ タロウ

表示名: 金宮 太郎

事業所:

電子メール:

Web ページ:

役職:

フリガナ(部署):

部署:

フリガナ(会社):

会社:

上司:

直属の部下:

電話番号:

メイン:

詳細情報

OK キャンセル

■ WowTalk 管理サイト ユーザー登録画面

WowTalk AdminSite

About WowTalk Inc.

メンバー 新しいメンバー

部門

WowTalk Inc.

製品開発部

品質保証部

OS部

情報システム部

経理部

事業部

WT_JP

削除用部門

ID kingutaro

ID ▲ 名前 ▲

kingutar 金宮太郎

ID* kingutaro

名前* 金宮太郎

アバター

内線電話 0931648499

携帯電話

勤務先住所 福岡県北九州市若松区浜町7-13-3

メール itugattaguti@aitai.ne.jp

部門 第01製品開発課

役職 部長

社員番号 1

フリガナ キングウタロウ

端末ホワイトリスト

PCのホワイトリスト

PCのIPホワイトリスト

誕生日 1974-05-15

編集 キャンセル

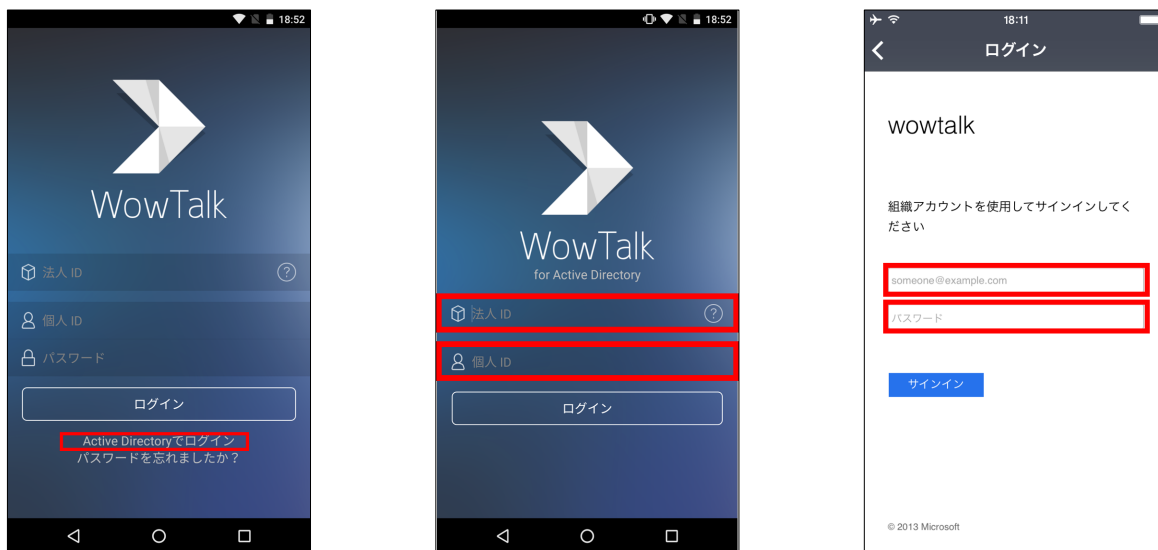
5. ログイン方法

5.1. iOS 版からログインする

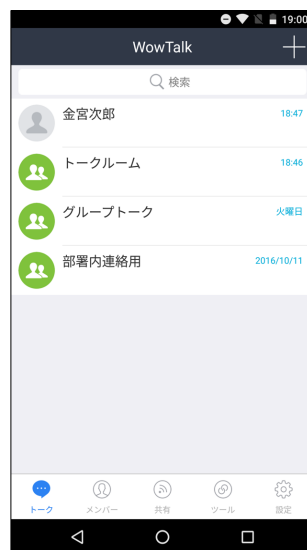


1. 「Active Directoryでログイン」をタップします。ログイン画面が表示されます。
2. 「法人 ID」と「個人 ID」を入力し、「ログイン」ボタンをタップします。
3. ActiveDirectory のログイン画面が表示されます。
4. 「法人 ID」と「個人 ID」を入力し「サインイン」ボタンをタップします。
5. トーク一覧画面が表示されます。

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。

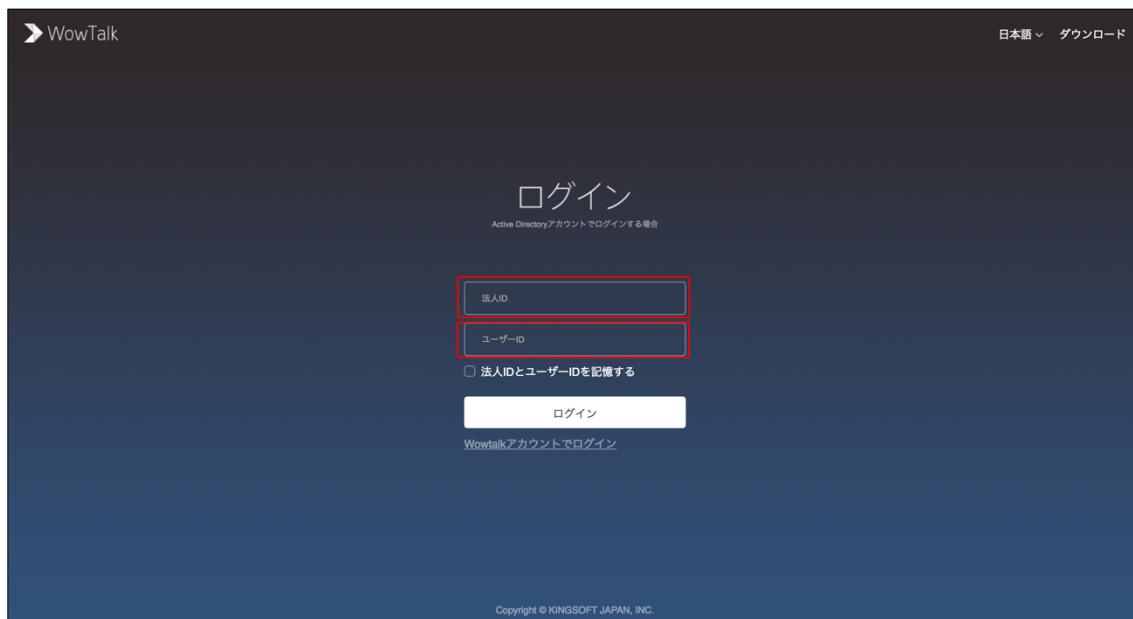


1. トーク一覧画面が表示されます。

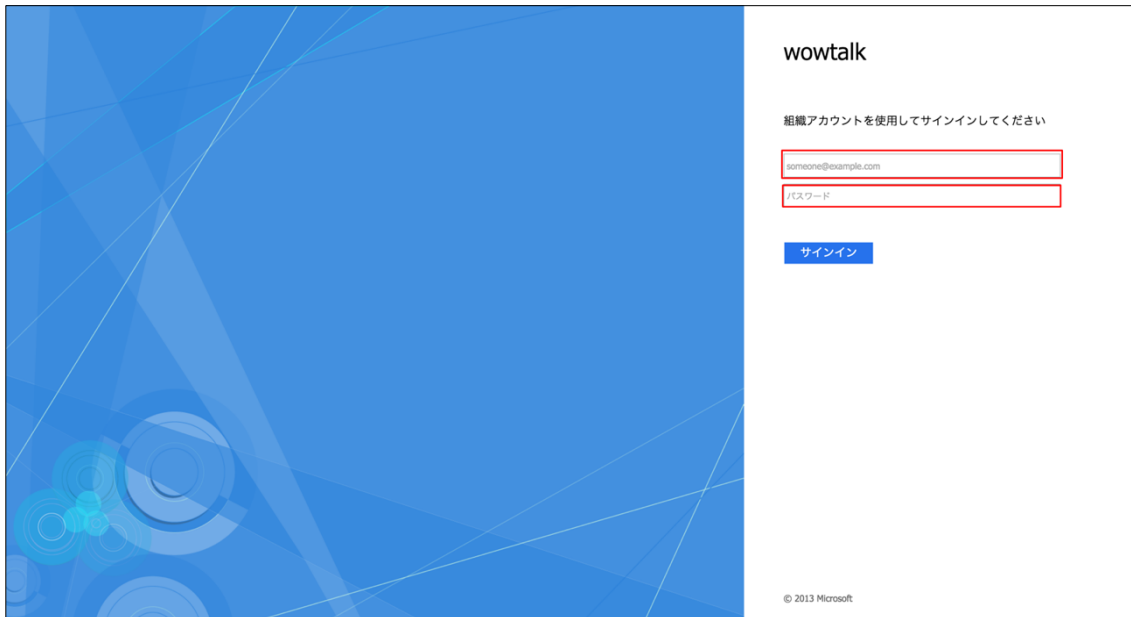
5.3. ユーザー向け Web 画面からログインする



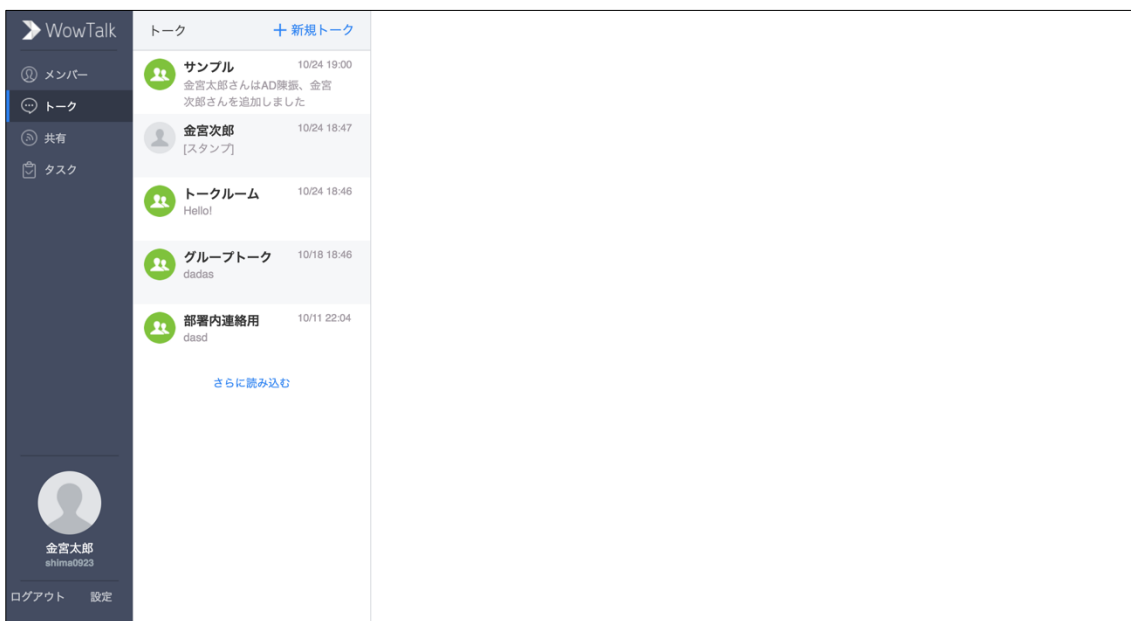
1. 「Active Directory アカウントでログイン」をクリックします。



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。