インストール・アップデートガイド

オープンソース・ソリューション・テクノロジ(株)

作成日: 2010 年 12 月 18 日
更新日: 2015 年 12 月 1 日
リビジョン: 3.2

目次

1.　はじめに

本ドキュメントは、弊社提供の Unicorn ID Manager を導入するための手順書です。

Unicorn ID Manager のインストールの際に、必ず本ドキュメントの内容を確認してから、作業を実施してください。

本ドキュメントに関する記載内容について、疑問点等がある場合には、弊社サポート窓口までお問い合わせください。

2. Unicorn ID Manager パッケージ

2.1 システム要件

2.1.1 ソフトウェア要件

以下のいずれかの OS 環境が必要です。

- Red Hat Enterprise Linux 7.0 以降
- Red Hat Enterprise Linux 6.2 (x86-64)以降
- CentOS 7.0 以降
- CentOS 6.2 (x86-64)以降

注: Unicorn ID Manager は、SE Linux に対応していません。

2.1.2 ハードウェア要件

ソフトウェア要件に記載の OS が動作する以下のハードウェア環境が必要です。

- CPU: Intel Xeon 2.0GHz 以上あるいは互換 CPU
- メモリ: 2GB 以上
- ディスク: ソフトウェア: /opt/osstech 512MB 以上
  データ、ログ: /var/opt/osstech 1GB 以上(推奨)

2.2 パッケージ構成

弊社が提供する Unicorn ID Manager は以下のパッケージにより構成されています。

- OSSTech ソフトウェア製品基本パッケージ
  - osstech-base
  - osstech-support
- Unicorn ID Manager パッケージ
  - osstech-unicornIDM
  - osstech-python27
  - osstech-python27-django
  - osstech-python27-google-directory-api-wrapper
  - osstech-python27-ldap

- osstech-python27-m2crypto
- osstech-python27-mod_wsgi
- osstech-python27-ntlm
- osstech-python27-ymailutils
- osstech-winexe

3. Unicorn ID Manager のインストール

3.1 パッケージインストール

3.1.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、最初に su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力 (画面には表示されません)
```

次に弊社から提供されたパッケージ一式をインストール先ホストの任意のディレクトリに展開します。下記の例では/srv/osstech/software/RPMS に展開したことを前提として記述します。

3.1.2 パッケージのインストール

弊社提供の Unicorn ID Manager パッケージは、/opt/osstech ディレクトリに新規インストールされます。

まず、Unicorn ID Manager が依存するパッケージをインストールします。

```
# yum install ksh perl gnutls httpd
```

RHEL6.1/CentOS6.1 までのバージョンを利用している場合、OS 標準の openldap パッケージに問題があるため、openldap パッケージのアップデートを行います。RHEL6.2/CentOS6.2 に含まれている openldap-2.4.23-19 以降にアップデートすれば問題ありません。

```
# yum update openldap
```

続いて、Unicorn ID Manager パッケージ一式をインストールします。

```
# cd /srv/osstech/software/RPMS
# rpm -ivh *.rpm
```

以下のようなメッセージが出力される場合、該当のパッケージはすでにインストール済みですので /srv/osstech/software/RPMS から移動してください。以下の場合、osstech-base パッケージはすでにインストール済みですので osstech-base-*.noarch.rpm を別のディレクトリに移動してください。

```
# /bin/rpm -Uhv *.rpm
準備中...                ########################################### [100%]
        パッケージ osstech-base-xxx は既にインストールされています。
```

以上で、Unicorn ID Manager パッケージのインストールは完了です。

3.2 Unicorn ID Manager の起動

3.2.1 SE Linux の無効化

root でログイン後、getenforce コマンドで SELinux が無効になっていることを確認します。

```
# getenforce
Disabled    (もしくは Permissive)
```

SELinux が有効(Enforcing)となっている場合は、/etc/sysconfig/selinux の SELINUX パラメーターを「disabled」に変更してから、マシンを再起動してください。

```
SELINUX=disabled
```

3.2.2 Unicorn ID Manager の初期化

続いて、Unicorn ID Manager の初期化を行ないます。

最初に su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力 (画面には表示されません)
```

Unicorn ID Manager の初期セットアップコマンドを実行します。

途中で、Unicorn ID Manager にログインする際の管理者ユーザーの登録を促されますので、管理者名とメールアドレス、パスワードを入力してください。

なお、現在の Unicorn ID Manager では、ここで登録した管理者のメールアドレスへのメール送信は行なっていません。

```
# /opt/osstech/sbin/unicornidm-setup
....
Would you like to create one now? (yes/no): yes  ← yes を入力して管理者を作成します
Username (Leave blank to use 'root'): admin ← 管理者ユーザー名
E-mail address: admin@example.com ← 管理者のメールアドレス
Password: ********
Password (again): ********
Superuser created successfully.
```

セットアップコマンドが完了したら、Apache を起動します。

```
# /sbin/service httpd start
```

なお、マシン起動時に自動的に Unicorn ID Manager が起動するようにするため、次のコマンドで Apache の自動起動を有効にしておきます。

```
# /sbin/chkconfig httpd on
```

Apache の起動が完了したら、Unicorn ID Manager の管理画面にアクセスして、初期設定を行ってください。

http://<サーバー>/unicornIDM/admin/


管理者メニュー
Unicorn ID Manager
ユニコーンIDマネージャー
ユーザー名
admin
パスワード
ログイン

4. Unicorn ID Manager のアップデート

4.1 パッケージのアップデート

4.1.1 前提

Unicorn ID Manager のアップデートは既存の Unicorn ID Manager のバージョンが 2.0 以降の場合に実施可能です。

4.1.2 準備

パッケージのアップデートは、root ユーザーのみに許可されていますので、最初に su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力 (画面には表示されません)
```

次に弊社から提供されたパッケージ一式をインストールアップデート先ホストの任意のディレクトリに展開します。下記の例では/srv/osstech/software/RPMS に展開したことを前提として記述します。

4.1.3 パッケージのアップデート

次のコマンドでアップデートを実行します。

```
# /bin/rpm -Uhv *.rpm
```

既に最新のパッケージがインストール済みの場合、次のようなエラーが表示されアップデートは完了しません。この場合はインストール済みのパッケージと同じバージョン、もしくは古いバージョンを利用してアップデートしようとしていますので、アップデートパッケージをディレクトリから除いておき、再度アップデートを試みます。

```
# /bin/rpm -Uhv *.rpm
準備中...                ########################################### [100%]
        パッケージ osstech-base-xxx は既にインストールされています。
        パッケージ osstech-support-xxx は既にインストールされています。
```

続いて、設定情報が格納されたデータベースを更新します。次のコマンドを実行してください。

```
# /opt/osstech/sbin/unicornidm-updatedb
```

このコマンドにより、バックアップとして/opt/osstech/var/lib/unicornIDM/unicornIDM.db.<日時>というファイルが生成され、/opt/osstech/var/lib/unicornIDM/unicornIDM.db が更新されます。なお、この更新はデータ自体の修正は実施しません。データベースの構造を更新します(たとえば、テーブルにカラムを追加する、などです)。

データベースの更新後、Apache を再起動してアップデートは終了です。

```
# /sbin/service httpd restart
```

4.1.4 バージョン 2.3 以降のパスワード変更画面

バージョン 2.3 から、一般ユーザー向けのパスワード変更画面のデザインが次のように変わり、新しいパスワード文字列の強度を判定します。

4.2 Google バックエンドのアップデート

2015 年 4 月にて、これまでの UnicornIDM で利用していた「Provisioning API」が廃止されます。それに伴いまして、UnicornIDM はバージョン 2.3 より Google が提供する新しい API、「Admin SDK's Directory API」を利用するように改修いたしました。

これまで、Google バックエンドを利用していたお客様は 5.4.1Google Apps API 利用のための事前準備に示す手順で「Admin SDK's Directory API」を利用するための設定を行ってください。

5. Unicorn ID Manager の設定

Unicorn ID Manager の設定画面にログインすると、次の画面が表示されます。

Unicorn ID Manager の基本的な設定は、

1. 「対象組織」
2. 「バックエンド」

の設定を行うことで完了します。

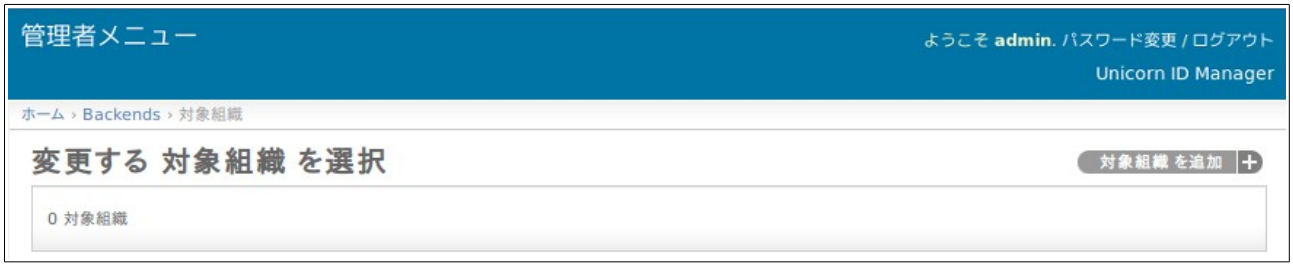
Unicorn ID Manager の設定が完了したら、「Unicorn ID Manager 管理者ガイド」を参考に利用を開始してください。

5.1 対象組織の設定

Unicorn ID Managerでは、バックエンドのサーバー群に対する一連の動作の動作単位を「対象組織」として設定します。

対象組織に対して、管理するLDAP、Active Directory、Google Appsをバックエンドとして追加します。

「対象組織」の設定は、管理画面で「対象組織」を選択します。



画面右端上部の「対象組織を追加」のボタンを選択します。

「対象組織」に設定可能なパラメーターの設定画面が表示されます。

各項目の意味を説明します。

5.1.1 基本設定

項目名	設定内容
対象組織の識別子	組織を特定するための一意な名称です。
対象組織名	対象組織を画面上で表示する際の名称です。日本語を含めて設定可能です。

5.1.2 ログ設定

項目名	設定内容
ログレベル	Unicorn ID Manager のデバッグログの出力レベルです。0～10 の値で指定します。通常の運用時は 1 を指定してください。大きい数字にすると、詳細なログが出力されます。
ログファイルの最大サイズ	デバッグログの 1 ファイルの最大サイズです。
ログローテート数	デバッグログのログファイルを最大いくつまでローテーションするか指定します。
ログファイルのディレクトリ	デバッグログの出力先です。通常は変更不要です。
syslog 機能を有効	設定を有効にすると、Unicorn IDM 経由のユーザーアカウントの操作履歴が、syslog に出力されます。(出力される内容はデバッグログではありません。)
Syslog の Facility 設定	syslog 機能を有効にしているときに、syslog の出力先となる Facility を選択します。

5.1.3 表示設定

項目名	設定内容
CSV ファイルのエンコーディング	管理者が CSV ファイルを一括操作のためにアップロードする時の、CSV ファイルのエンコーディングです。「選択」を指定した場合は、アップロード時に「UTF-8」か「シフト JIS」を選択することができます。
プレビュー時に表示されるエントリ数	CSV ファイルのアップロード時に、CSV の内容をプレビューします。このときに、先頭からいくつのエントリ数をプレビューするか指定します。
サマリに表示されるエントリ数	CSV の一括操作の操作結果を、直近のものからいくつ表示するか指定します。
一覧画面での最大表示件数	ユーザー一覧、グループ一覧の画面で、1 画面に表示するエントリ数を指定します。

5.1.4 パスワードの長さ

項目名	設定内容
ユーザーのパスワードの最大文字数	パスワード変更画面でパスワードとして設定可能な最大文字数を指定します。
ユーザーのパスワードの最小文字数	パスワード変更画面でパスワードとして設定可能な最小文字数を指定します。
自動生成パスワードの文字数	ユーザー登録画面やパスワード変更画面でランダムパスワードを指定した際に、生成されるパスワードの文字数を指定します。

5.1.5 パスワードの複雑性

項目名	設定内容
パスワードの複雑性をチェック	この設定を有効にすると、一般ユーザーがパスワード変更画面でパスワードを設定する際に、パスワードの複雑性がチェックされます。 管理者ページでパスワードを変更する場合には、複雑性のチェックは行われません。 パスワードの複雑性は次の条件を組み合わせて設定します。
パスワードに含めなければならない英字(大文字、小文字)の数	アルファベットの大文字・小文字が、この項目に設定した数以上含まれているパスワードのみ許可されます。
パスワードに含めなければならない英字(大文字)の数	アルファベットの大文字が、この項目に設定した数以上含まれているパスワードのみ許可されます。
パスワードに含めなければならない英字(小文字)の数	アルファベットの小文字が、この項目に設定した数以上含まれているパスワードのみ許可されます。
パスワードに含めなければならない数字の数	数字が、この項目に設定した数以上含まれているパスワードのみ許可されます。
パスワードに含めなければならない記号の数	記号が、この項目に設定した数以上含まれているパスワードのみ許可されます。
パスワードに含めなければならない文字の種類の数	「英大文字」「英小文字」「数字」「記号」のうち、何種類の文字を含んだパスワードを許可するか指定します。

5.1.6 パスワード入力禁止文字

項目名	設定内容
パスワードの入力禁止文字列	ユーザー登録やパスワード変更の際に、この欄に記載された文字がパスワードに含まれていると、エラーになります。
自動生成パスワードの入力禁止文字列	この欄に記載した文字は、自動生成したパスワードには含まれなくなります。
現在のパスワードを新しいパスワードとして設定可能	チェックすると、現在のパスワードを新しいパスワードとして設定可能となります 。
ユーザー名を含むパスワードの設定を禁止する	チェックすると、ユーザーがユーザー名を含むパスワードに更新することを禁止します。

5.1.7 パスワード変更時のメッセージ

項目名	設定内容
パスワード変更時のユーザー向けの注意書き	この欄に記載したテキストが、パスワード変更画面に注意書きとして表示されます。 HTML 形式で記述することができます。
パスワード変更後のユーザー向けの注意書き	この欄に記載したテキストが、パスワード変更完了画面に注意書きとして表示されます。 HTML 形式で記述することができます。
パスワード印刷時の	この欄に記載したテキストが、パスワード印刷ページに注意書きとして表示されます。

ユーザー向けの注意書き	HTML 形式で記述することができます。ただし、シングルクォーテーション「'」はダブルクォーテーション「""」に変換されます。また、<pre>タグ内であっても改行は適用されません。

5.1.8 システム設定

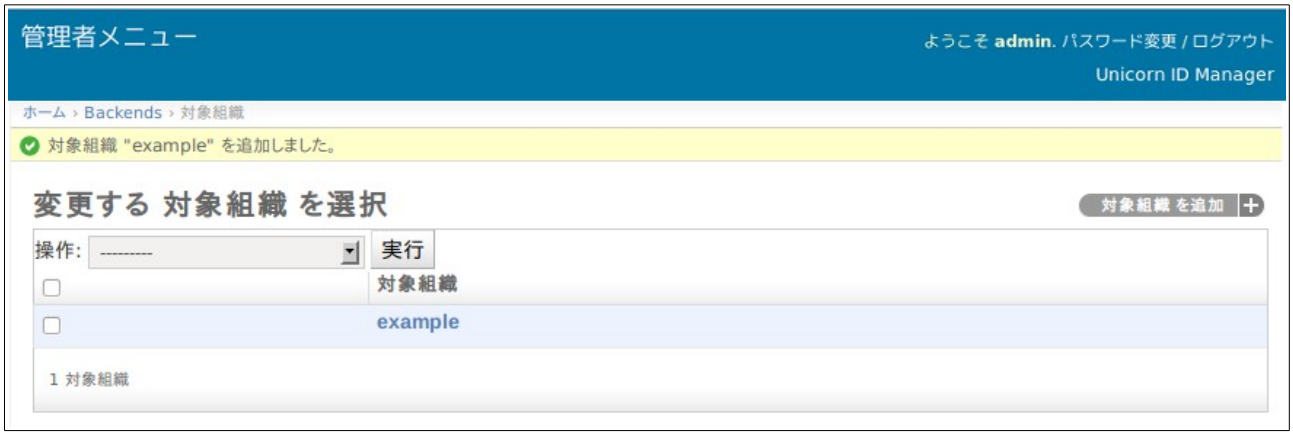
項目名	設定内容
操作完了後にアップロードしたファイルを削除	CSV ファイルの一括処理時に、アップロードした CSV ファイルを削除する場合は、この設定を有効にしてください。
属性を削除するための値	CSV ファイルの一括操作時に、設定済みの属性を削除したいときに、CSV ファイルのエントリに記載する文字列を設定します。デフォルトは「Null」です。

5.1.9 シングルサインオン設定

項目名	設定内容
認証された ID を取得する方法	シングルサインオン環境を構築した場合における、認証済みの ID の取得先を指定します。シングルサインオン製品(OpenAM など)は、認証された ID を HTTP リクエストのヘッダーやパラメーターに設定できます。これを取得することで Unicorn IDM へシングルサインオンできるようになります。
キー名	認証された ID を取得するためのキー名を指定します。
SSO を許可する IP セグメントのリスト	SSO を許可する IP セグメントのリストをカンマ区切りで指定します。 次の形式で指定してください。 127.0.0.1,10.0.0.0/8 上記設定の場合、ローカルホストと、10.0.0.0～10.255.255.255 が許可されます。

対象組織の内容として、以上の項目の入力を完了したら、画面最下段の「保存」をクリックします。

入力した値に問題が無ければ、「対象組織」として、入力した組織が登録されます。



続いて、バックエンドの設定を行いますので、左上のリンクの「ホーム」をクリックします。

5.2 バックエンド(LDAP サーバー)の設定

あらかじめ、対象となる LDAP サーバーのホスト名から、IP アドレスが名前解決できることを確認してください。

LDAP サーバーのアカウント管理を行う場合、「バックエンド(LDAP サーバー)」を選択します。

画面右上の「バックエンド(LDAP サーバー)を追加」のボタンをクリックします。

LDAP サーバー設定画面の各項目の意味を説明します。

5.2.1 基本設定

項目名	設定内容
Org	この LDAP サーバーを、どの「対象組織」の管理下に置くか選択します。
サーバーの識別子	この LDAP サーバーを特定できる名称を指定します。 Unicorn ID Manager の表示等で利用されます。
プライオリティ	対象組織内で、この LDAP サーバーに対して何番目に処理を行うか1以上の数値で指定します。
バックグラウンドでの CSV 一括処理	CSV ファイルを一括処理する際に、LDAP サーバーに対してバックグラウンドで処理を行う場合は、この設定を有効にします。 この設定が無効な場合は、LDAP サーバーへの一括処理が完了してから、ブラウザに応答が返ります。
IP アドレス	LDAP サーバーの IP アドレスを指定します。
ホスト名	LDAP サーバーのホスト名を指定します。
プロトコル	LDAP サーバーに接続するときのプロトコルとして、LDAP か LDAPS を指定します。
LDAP 管理者の DN	LDAP のエントリの更新権を持つユーザーの DN を指定します。
LDAP 管理者のパス	LDAP に接続する DN のパスワードを指定します。

ワード	
LDAP のベース Suffix	LDAP サーバーのベース Suffix を指定します。
ユーザーエントリの Suffix	ユーザーが格納されているツリーの DN を指定します。Unicorn ID Manager は、ここで指定した DN のサブツリーをユーザーの検索対象とします。
ユーザーを識別する属性	ユーザーが登録されている DN の属性名を指定します。 dn: uid=user1,dc=example,dc=com として、ユーザーが登録される場合は、「uid」を指定します。
ユーザーエントリのフィルタ	管理するユーザーを LDAP の検索フィルタで絞り込みたい場合は、検索フィルタを指定します。
グループエントリの Suffix	グループが格納されているツリーの DN を指定します。Unicorn ID Manager は、ここで指定した DN のサブツリーをグループの検索対象とします。
グループエントリのフィルタ	管理するグループを LDAP の検索フィルタで絞り込みたい場合は、検索フィルタを指定します。

5.2.2 同期設定

項目名	設定内容
ユーザーのパスワード変更時にこのサーバーのパスワードを同期する	パスワード変更画面からパスワードを変更したときに、この LDAP サーバーのパスワードを変更します。
ユーザーのアカウント操作時に、このサーバーのアカウントを同期する	管理者が CSV やアカウントの操作を行なった時に、この LDAP サーバーのユーザーエントリを更新します。
グループ操作時に、このサーバーのグループを同期する	管理者がグループに関連する操作を行なった時に、この LDAP サーバーのグループエントリを更新します。
このサーバーでユーザーを認証する	パスワード変更ページでユーザーを認証するときに、この LDAP サーバーで認証が成功した場合に、パスワード変更を許可します。パスワード変更時には、「対象組織」に含まれるいずれかのバックエンドで認証が成功すれば、パスワード変更を許可します。
パスワード変更時に「ユーザーが存在しない」エラーを無視する	この LDAP サーバー上でのパスワード変更が失敗しても、パスワード更新としては成功としてみなすための設定です。 複数のサーバーでアカウントの統合管理を行うときに、一部のサーバーにユーザーが登録されない場合に利用します。 通常は無効に設定してください。

5.2.3 デフォルト値

項目名	設定内容
パスワードの暗号化方式	LDAP サーバーに格納するパスワードの暗号化方式を選択します。
UNIX のホームディレクトリのデフォルトのパス	CSV ファイルでユーザーを登録する際に、UNIX 用のホームディレクトリの値(unixHomeDirectory)を指定しなかった場合のデフォルト値です。 「%USERNAME%」の部分はユーザー名に置換されます。
デフォルトの GID	CSV ファイルでユーザーを登録する際に、UNIX 用の GID 番号(gidNumber)の値を指定しなかった場合のデフォルト値です。
ユーザーのデフォルトのログインシェル	CSV ファイルでユーザーを登録する際に、UNIX 用のログインシェル(loginShell)の値を指定しなかった場合のデフォルト値です。

Gecos フィールドを sn と givenName で設定する	CSV ファイルでユーザーを登録する際に、UNIX 用の GECOS(gecos)の値を指定しなかった場合に、「sn givenName」の設定値で gecos フィールドを設定します。 gecos フィールドには英数字以外含めることができないため、この設定を有効にした場合、「sn」「givenName」のフィールドにも英数字以外含めることができなくなります。

5.2.4 追加コマンド実行

項目名	設定内容
ユーザー登録後に追加のコマンドを実行	ユーザーアカウント登録操作の後にコマンドを実行したい場合に有効にします。 ユーザー登録後に実行するコマンドのパスを指定します。 コマンドの引数を、LDAP に登録する属性名で指定します。指定した順番で属性に設定した値がコマンドの引数に渡されます。
ユーザー更新後に追加のコマンドを実行	ユーザーアカウント更新操作の後にコマンドを実行したい場合に有効にします。 ユーザー更新後に実行するコマンドのパスを指定します。 コマンドの引数を、LDAP に登録する属性名で指定します。指定した順番で属性に設定した値がコマンドの引数に渡されます。
ユーザー削除前にコマンドを実行	ユーザーアカウントの削除操作の前にコマンドを実行したい場合に有効にします。 ユーザー削除前に実行するコマンドのパスを指定します。 コマンドの引数には、ユーザー名、ユーザーのホームディレクトリが渡されます。
ユーザー有効化後にコマンドを実行	ユーザーアカウントの有効化操作の後にコマンドを実行したい場合に有効にします。 ユーザーアカウントの有効化操作後に実行するコマンドのパスを指定します。 コマンドの引数には、ユーザー名が渡されます。
ユーザー無効化後にコマンドを実行	ユーザーアカウントの無効化操作の後にコマンドを実行したい場合に有効にします。 ユーザーアカウントの無効化操作後に実行するコマンドのパスを指定します。 コマンドの引数には、ユーザー名が渡されます。

5.2.5 UID 番号関連設定

項目名	設定内容
UID 番号を自動的に割り当て	CSV でのユーザー一括登録時に、uidNumber が指定されていないユーザーに対して、自動的に利用されていない UID 番号を割り当てます。
自動的に割り当てる UID 番号の最小値	自動的に割り当てる UID 番号の最小値です。
自動的に割り当てる UID 番号の最大値	自動的に割り当てる UID 番号の最大値です。
自動的に割り当てる次の UID 番号	次にユーザーを登録したときに割り当てられる UID 番号です。通常は変更する必要はありません。

5.2.6 パスワード設定

項目名	設定内容
平文パスワード保存を適用する	平文パスワードをユーザエントリの任意属性に保存する場合に、チェックします。
平文パスワードを保存する属性	平文パスワードを保存する属性名を指定します。
ShadowExpire 属性を更新する	ShadowExpire 属性を更新する場合に、チェックします。
パスワード無効化日数	ShadowExpire 属性を更新する場合に、パスワードが無効化される日数を指定します。

OpenLDAP サーバーのパスワードポリシーを使用する	対象の LDAP サーバーが OpenLDAP の時に、OpenLDAP サーバーのパスワードポリシー(ppolicy)を使用する場合に、チェックします。

5.2.7 ランダム文字列設定

項目名	設定内容
ランダムに生成した文字列を自動で追加	LDAP にユーザーを登録する際に、ある属性にランダムな文字列を自動的に割り当てたい場合に有効に設定します。指定した文字数で、ランダムな英数字からなる文字列が登録されます。
ランダムに生成した文字列の属性名	文字列を登録する LDAP の属性名を指定します。
ランダムに生成する文字列の文字数	生成する文字列の文字数を指定します。

5.2.8 ユーザーエントリのオブジェクトクラス

ユーザー登録時に、ユーザーのエントリの objectClass として登録するオブジェクトクラス名を選択します。

通常の場合は、次の1つを指定してください。

- posixAccount

Active Directory と連携する場合は、上記に加えて次の1つを指定してください。

- inetOrgPerson

5.2.9 グループエントリのオブジェクトクラス

グループ登録時に、グループのエントリの objectClass として登録するオブジェクトクラス名を選択します。

5.3 バックエンド(Active Directory サーバー)の設定

5.3.1 準備

Active Directory サーバーとの連携を行う場合は、あらかじめ Active Directory に証明書サービスのインストールを行い、Windows サーバーの再起動を行ってください。

証明書サービスのインストール手順は、別紙「Active Diretory 証明書サービス インストールガイド」を参照してください。

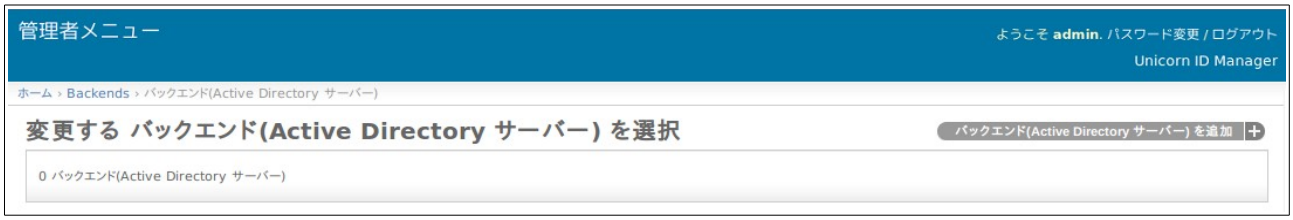
次に、/etc/openldap/ldap.conf に次の設定を追加します。

```
TLS_REQCERT    never
```

また、Active Directory サーバーのホスト名から、IP アドレスが解決できることをあらかじめ確認しておいてください。

5.3.2 Unicorn ID Manager の設定

Active Directory サーバーの管理を行う場合、「バックエンド(Active Directory サーバー)」を選択します。



画面右上の「バックエンド(Active Directory サーバー)を追加」をクリックします。

各項目の設定を完了後、最下部の「保存」ボタンをクリックして設定を保存します。

5.3.3 基本設定

項目名	設定内容
Org	この Active Directory サーバーを、どの「対象組織」の管理下に置くか選択します。
サーバーの識別子	この Active Directory サーバーを特定できる名称を指定します。 Unicorn ID Manager の表示等で利用されます。
プライオリティ	対象組織内で、この Active Directory サーバーに対して何番目に処理を行うか1以上の数値で指定します。
バックグラウンドでの CSV 一括処理	CSV ファイルを一括処理する際に、LDAP サーバーに対してバックグラウンドで処理を行う場合は、この設定を有効にします。 この設定が無効な場合は、LDAP サーバーへの一括処理が完了してから、ブラウザに応答が返ります。
IP アドレス	Active Directory サーバーの IP アドレスを指定します。
ホスト名	Active Directory サーバーのホスト名を指定します。
Active Directory のドメイン名	接続先の Active Directory のドメイン名を指定します。
Active Directory 管理者のユーザー名	Domain Admins 権限を持つ Active Directory の管理者ユーザー名を指定します。
Active Directory 管理者のパスワード	指定した Active Directory 管理者のパスワードを指定します。

5.3.4 同期設定

項目名	設定内容
ユーザーのパスワード変更時にこのサーバーのパスワードを同期する	パスワード変更画面からパスワードを変更したときに、この Active Directory サーバーに登録されているユーザーのパスワードを変更します。
ユーザーのアカウント操作時に、このサーバーのアカウントを同期する	管理者が CSV やアカウントの操作を行なった時に、この Active Directory サーバーのユーザーエントリを更新します。
グループ操作時に、このサーバーのグループを同期する	管理者がグループに関連する操作を行なった時に、この Active Directory サーバーのグループエントリを更新します。
このサーバーでユーザーを認証する	パスワード変更ページでユーザーを認証するときに、この Active Directory サーバーで認証が成功した場合に、パスワード変更を許可します。 パスワード変更時には、「対象組織」に含まれるいずれかのバックエンドで認証が成功すれば、パスワード変更を許可します。
パスワード変更時に「ユーザーが存在しない」エラーを無視する	この Active Directory サーバー上でのパスワード変更が失敗しても、パスワード更新としては成功としてみなすための設定です。 複数のサーバーでアカウントの統合管理を行うときに、一部のサーバーにユーザーが登録されない場合に利用します。 通常は無効に設定してください。

5.3.5 デフォルト値

項目名	設定内容
ユーザーのデフォルトのプライマリグループ名	ユーザー登録時に、ユーザーが所属するデフォルトのプライマリグループです。通常は「Domain Users」です。
ユーザーのデフォルトの OU	ユーザー登録時に、CSV で OU が指定されない場合のデフォルトの OU です。通常は「CN=Users」です。
グループのデフォルトの OU	グループ登録時に、CSV で OU が指定されない場合のデフォルトの OU です。通常は「CN=Users」です。
ユーザーのデフォルトのホームドライブ	ユーザー登録時に、CSV で homeDrive 属性が指定されない場合のデフォルトのドライブ名です。
ユーザーのデフォルトのホームディレクトリ	ユーザー登録時に、CSV で homeDirectory 属性が指定されない場合のデフォルトのホームドライブのパスです。パスに「%USERNAME%」を含めると、登録時にユーザー名に置換されて、登録されます。
ユーザーのデフォルトのプロファイルパス	ユーザー登録時に、CSV で profilePath 属性が指定されない場合のデフォルトのプロファイルのパス名です。パスに「%USERNAME%」が含まれると、登録時にユーザー名に置換されて、登録されます。
ユーザーのデフォルトのログオンパス	ユーザー登録時に、CSV で scriptPath 属性が指定されない場合のデフォルトのプロファイルのパス名です。
パスワードを無期限にする	ユーザー登録時に「パスワードを無期限にする」を有効にします。
スマートカードを使用したログインが必要	ユーザー登録時に「スマートカードを使用したログインが必要」を有効にします。

5.3.6 追加コマンド実行

項目名	設定内容
ユーザー登録後に追加のコマンドを実行	ユーザー登録成功後に、連携先の Active Directory サーバーで Windows のコマンドを実行したい場合に有効にします。
ユーザー登録後に実行するコマンド	実行するコマンドを指定します。
ユーザー更新後に追加のコマンドを実行	ユーザー更新成功後に、連携先の Active Directory サーバーで Windows のコマンドを実行したい場合に有効にします。
ユーザー更新後に実行するコマンド	実行するコマンドを指定します。
ユーザー削除前にコマンドを実行	ユーザー削除成功後に、連携先の Active Directory サーバーで Windows のコマンドを実行したい場合に有効にします。
ユーザー削除前に実行するコマンド	実行するコマンドを指定します。
ユーザー有効化後にコマンドを実行	ユーザー有効化後に、連携先の Active Directory サーバーで Windows のコマンドを実行したい場合に有効にします。
ユーザー有効化後に実行するコマンド	実行するコマンドを指定します。
ユーザー無効化後にコマンドを実行	ユーザー無効化後に、連携先の Active Directory サーバーで Windows のコマンドを実行したい場合に有効にします。
ユーザー無効化後に実行するコマンド	実行するコマンドを指定します。

実行できるコマンドは、接続先の Active Directory サーバー上に配置された Windows 用のバッチスクリプトに限られます。

また、実行の際には、Active Directory に接続している管理者ユーザーの権限で実行されます。

コマンドの引数には、ユーザー名を表す「%username%」の他に、Active Directory に登録する属性の属性名を%で囲んだ値も指定することができます。

たとえば、Active Directory サーバーにログオンする際に事前にホームディレクトリの操作が必要なため、homeDirectory 属性の値を引数にしてスクリプトを実行したい場合は、次のような設定を行います。

「ユーザー登録後に実行するコマンド」

```
CMD /C C:¥unicornidm¥mkhome %username% %homeDirectory%
```

また、Active Directory 上のバッチから、他のサーバーのファイル共有にアクセスする場合は、スクリプト内で、「net use」により明示的にドライブの割り当てを行ってください。

以下の二点の条件を満たしている場合、端末側 Windows によって指定したプロファイルパスに自動的にユーザプロファイルが作成されます。

- ユーザのプロファイルパスを指定している状態。
- 指定されたユーザのプロファイルパスに対して、ログオンを行うユーザが変更権限を所有している状態。(Domain Users 等)

プロファイルの自動生成を行うと、自動生成されたプロファイルに対して、SYSTEM およびログオンユーザのみが所有権を持つ状態で生成されます。そのため、自動生成されたプロファイルに対して管理者から何らかの操作を行う場合、明示的に所有権およびアクセス権を取得する必要があります。

自動生成されたプロファイルに対して Unicorn から操作を行う場合、以下のグループポリシーの設定をお願いします。

- コンピューターの構成¥ポリシー¥管理用テンプレート¥システム¥ユーザー プロファイル¥Administrators セキュリティ グループを移動ユーザー プロファイルに追加する

上記のグループポリシーを設定することによって、自動生成されたプロファイルに自動的に Administrators グループがアクセス権を所有した状態でプロファイルが生成され、明示的にアクセス権を取得することなく操作可能な状態で生成されます。

5.3.7 ユーザーエントリのオブジェクトクラス

Active Directory のユーザー登録時のオブジェクトクラスを指定します。

通常は、次の 4 つを指定してください。

- top
- person
- user
- organizationalPerson

5.3.8 グループエントリのオブジェクトクラス

Active Directory のグループ登録時のオブジェクトクラスを指定します。

通常は、次の 2 つを指定してください。

- top
- group

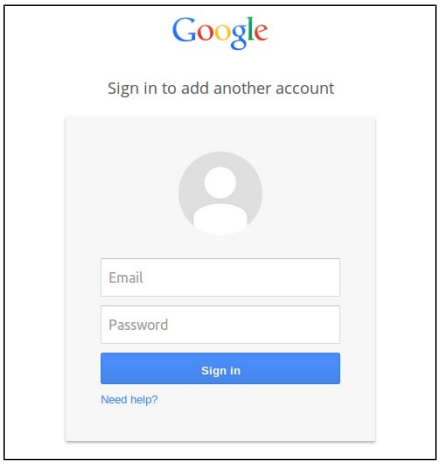
5.4 バックエンド(Google Apps)の設定

5.4.1 Google Apps API 利用のための事前準備

Google バックエンドを利用するためには以下に示す手順で「Admin SDK's Directory API」を利用するための設定を行ってください。

下記 URL にアクセスし、ドメイン管理者としてログインします。

https://code.google.com/apis/console

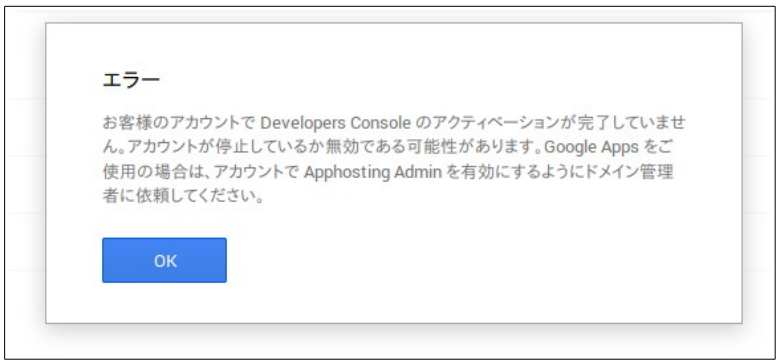


ログイン後、画面左側のサイドバーの「プロジェクト」を選択し、「プロジェクトを作成」をクリックします。

「プロジェクト名」には任意の名称を設定します。 「Google Cloud Platform 利用規約」を確認し、同意のチェックを付けてから、「作成」をクリックします。

ブラウザの画面下部に処理中を表すウィンドウが表示されますので、1 分程度でプロジェクトの作成が完了するのを待ちます。

もしプロジェクト作成時に、下記のエラー画面が出力された場合は、「Google Developers Console」サービスを有効にします。



「Google Developers Console」サービスを有効にするには、次の URL にアクセスし、Google Apps の管理コンソールにドメイン管理者としてアクセスします。

https://admin.google.com/

管理コンソールのダッシュボード画面にて、「その他の Google アプリ」を選択し、「Google Developers Console」を選択し、「オン」とします。

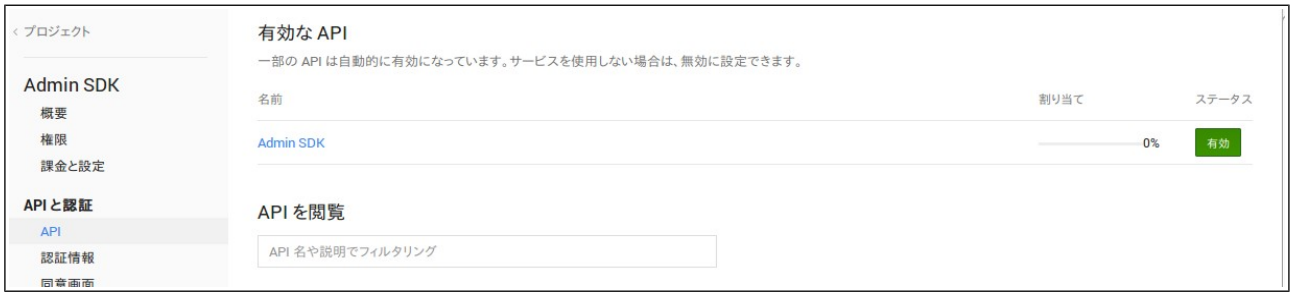
(「その他の Google アプリ」がダッシュボードにない場合には、「その他の設定」から選択が可能です。また、ドメインによっては、「アプリ」-「その他の Google アプリ」から選択しなければいけない場合もあります)。

サービス有効後、再度「プロジェクトを作成」の手順を実施します。プロジェクト一覧から、作成したプロジェクトを選択します。

画面左側にある「API と認証」を選択します。

「API と認証」のサブメニューから「API」を選択します。

API 一覧から「Admin SDK」の「無効」ボタンをクリックして、「有効」に変更します。



続いて、画面左側の「API と認証」のサブメニューの「認証情報」をクリックします。

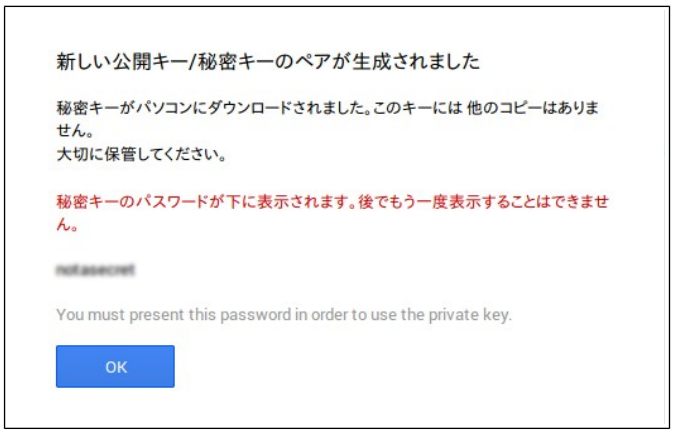
「OAuth」の項目にある「新しいクライアント ID を作成」をクリックします。

「クライアント ID を作成」の画面では、「サービスアカウント」を選択し、「クライアント ID を作成」をクリックします。

数秒程度立ってから「認証情報」の画面に戻ると、生成されたクライアント ID の情報が表示されます。

表示されている「クライアント ID」と「メールアドレス」は後ほど利用するため、記録しておきます。

秘密キーのパスワードが画面に表示されますので、書き留めておきます。



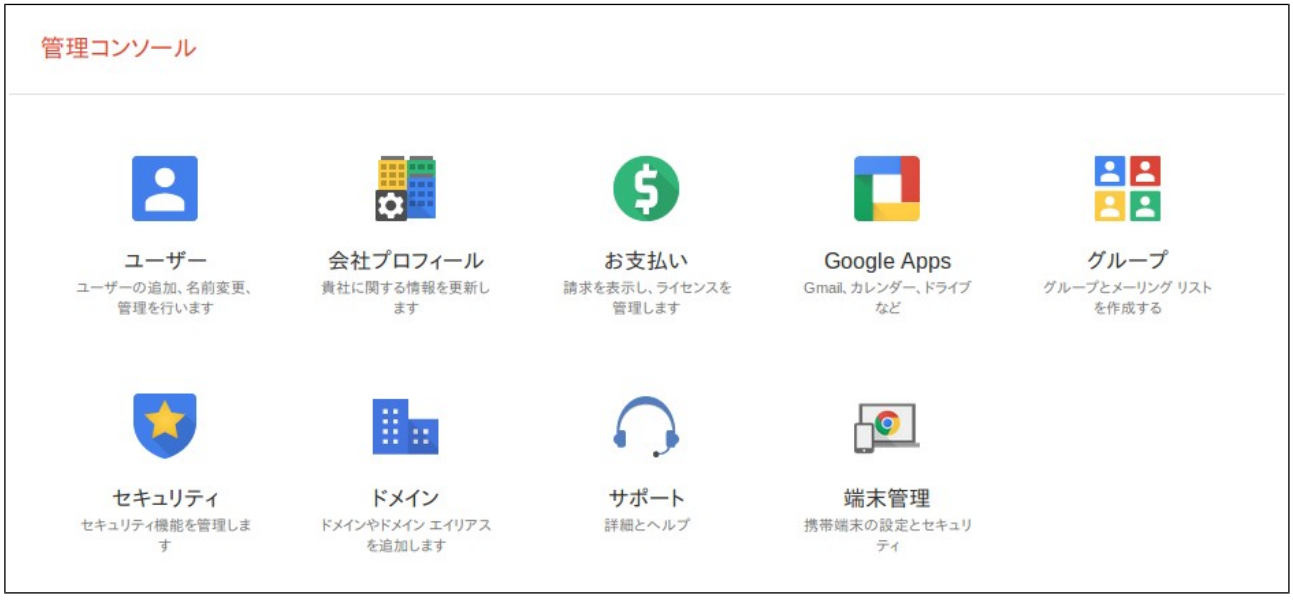
さらに Unicorn ID Manager で利用するための、P12 キーファイルのダウンロードダイアログが開きますので、ファイルを保存します。

続いて、Google Apps の設定で、API の利用を許可する設定を行います。

次の URL にアクセスし、Google Apps の管理コンソールにドメイン管理者としてアクセスします。

https://admin.google.com/

管理コンソールのダッシュボード画面にて、「セキュリティ」を選択します。



「詳細設定」の「認証」カテゴリ内の「API クライアントアクセスを管理する」をクリックします。

「クライアント名」に Admin SDK の設定時に作成された「クライアント ID」を指定します。

「1 つ以上の API の範囲」に以下の 3 つの URL を「,」(コンマ)でつなげて入力します。

```
https://www.googleapis.com/auth/admin.directory.user
https://www.googleapis.com/auth/admin.directory.group
https://www.googleapis.com/auth/admin.directory.orgunit
```

コピーする際は以下をご利用ください。

```
https://www.googleapis.com/auth/admin.directory.user,https://www.googleapis.com/auth/admin.directory.group,https://www.googleapis.com/auth/admin.directory.orgunit
```

全てを入力したら、「承認」をクリックします。

「セキュリティ」の画面に戻り、「API リファレンス」を選択します。

「API アクセスを有効にする」にチェックをつけます。

以上で Google Apps 側の設定は完了です。

続いて、Unicorn ID Manager から API を利用するために、さきほどダウンロードした「****.p12」ファイルを、Unicorn ID Manager のサーバーにインストールします。

ファイルは、/opt/osstech/var/lib/unicornIDM 直下に保存し、次のコマンドを実行してください。

```
# chown apache /opt/osstech/var/lib/unicornIDM/<プライベートキーファイル>
# chmod 0400 /opt/osstech/var/lib/unicornIDM/<プライベートキーファイル>
```

ここで用意したファイルを、Unicorn ID Manager の Google バックエンドの設定で指定します。

Google バックエンドの設定では、以下の設定を行ってください。

- 「Google API を使用するためのサービスアカウント」
  - クライアント ID 作成時に表示された「xxxx@developer.gserviceaccount.com」を指定してください。
- 「Google API を使用するための Private key ファイルのパス」
  - 前述の「xxx.p12」ファイルのパスとして、「/opt/osstech/var/lib/unicornIDM/<プライベートキーファイル>」を指定してください。

5.4.2 接続確認

Google Apps との連携を行う場合は、Unicorn ID Manager のサーバーから、Google へアクセスするために、以下の接続が可能であることを、あらかじめ確認してください。

```
https://www.googleapis.com/discovery/v1/apis/
```

HTTPS(443/TCP)でアクセスしますので、DNS の設定、および、ファイアウォールの設定を確認してください。

5.4.3 時刻設定確認

UnicornIDM は Google Apps への接続時に Google Apps に対して認証を行います。この時、認証情報とともに時刻情報も送ります。したがって、サーバー側の時刻設定が正しくないと正しく認証が行われません。

Google Apps をバックエンドに利用する際は、NTP 等でサーバーの時刻を正しく設定してください。

5.4.4 Unicorn ID Manager の設定

Google Apps の管理を行う場合、「バックエンド(Google Apps)」を選択します。

画面右上の「バックエンド(Google Apps)を追加」をクリックします。

5.4.5 基本設定

項目名	設定内容
Org	この Google Apps を、どの「対象組織」の管理下に置くか選択します。
サーバーの識別子	この Google Apps を特定できる名称を指定します。Unicorn ID Manager の表示等で利用されます。
プライオリティ	対象組織内で、この Google Apps に対して何番目に処理を行うか1以上の数値で指定します。
Google Apps のドメイン名	Google Apps のドメイン名を指定します。
Google Apps の管理者ユーザー名	Google Apps に接続するための管理者ユーザー名を指定します。
Google API を使用するためのサービスアカウント	Google Apps に接続するためのサービスアカウントを指定します。サービスアカウントは 5.4.1Google Apps API 利用のための事前準備で、クライアント ID 作成時に表示されたメールアドレス(xxxx@developer.gserviceaccount.com)のものです。
Google API を使用するための Private key ファイルのパス	Google Apps に接続するための Private key ファイルのパスを指定します。Private key ファイルは 5.4.1Google Apps API 利用のための事前準備で取得したプライベートキーファイル(xxx.p12)です。
ユーザー登録時にダミーのパスワードを割り当てる	Google Apps の認証を SSO で行う場合に、Google Apps 側のパスワードはダミーパスワードとする場合に有効にしてください。 通常は、無効にします。

5.4.6 同期設定

項目名	設定内容
ユーザーのパスワード変更時にこのサーバーのパスワードを同期する	パスワード変更画面からパスワードを変更したときに、この Google Apps に登録されているユーザーのパスワードを変更します。
ユーザーのアカウント操作時に、このサーバーのアカウントを同期する	管理者が CSV やアカウントの操作を行なった時に、この Google Apps のユーザーエントリを更新します。
グループ操作時に、このサーバーのグループを同期する	管理者がグループに関連する操作を行なった時に、この Google Apps のグループエントリを更新します。

5.4.7 ユーザーエントリのオブジェクトクラス

Google Apps 用のオブジェクトクラスとして、「basic」のみを選択してください。

5.4.8 グループエントリのオブジェクトクラス

Google Apps 用のオブジェクトクラスとして、「basic」のみを選択してください。

5.5 バックエンド(Azure AD)の設定

Unicorn ID Manager から、Office365 に連携する際、Office365 内の Azure AD に Graph API を通じて ID 連携操作を行います。

Unicorn ID Manager のサーバーから、Grapah API 経由で Azure AD へアクセスするために、以下の接続が可能であることを、あらかじめ確認してください。

```
https://graph.windows.net/
```

HTTPS(443/TCP)でアクセスしますので、DNS の設定、および、ファイアウォールの設定を確認してください。

5.5.1 Azure AD のクライアント ID とシークレットキー設定

Unicorn ID Manager から、Graph API による Azure AD へ接続するためには、Azure AD で接続用のクライアント ID とシークレットキーを発行する必要があります。

次の手順に従って、クライアント ID とシークレットキーの発行を行ってください。

1. 以下の URL をブラウザから開きます。

   https://manage.windowsazure.com/

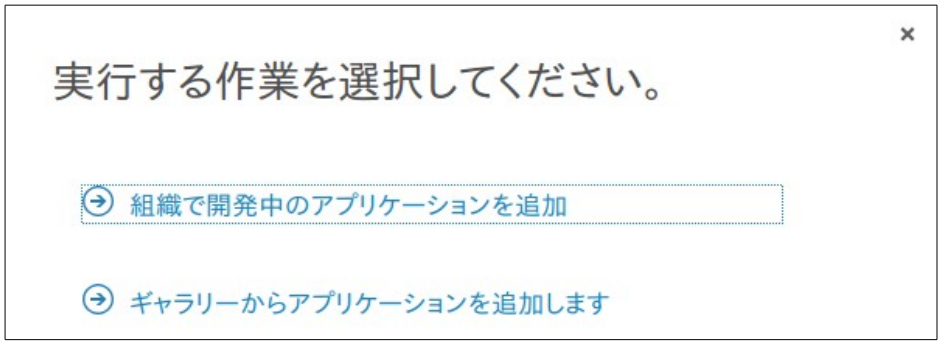
2. Microsoft Azure のログイン画面となりますので、Office365 の管理者アカウントでログインを行います。「username@xxx.onmicrosoft.com」のメールアドレスがログイン ID となります。

3. 左ペインの「ACTIVE DIRECTORY」を選択します。

4. 管理対象の「名前」の欄をクリックし、画面上部の「アプリケーション」タブをクリックします。

5. 「アプリケーション」タブの画面最下部の「追加」アイコンをクリックします。

6. 「組織で開発中のアプリケーションを追加」をクリックします。



7. 「アプリケーション情報の指定」に任意の名前を指定します。本ドキュメントでは指定例として、

「unicornidm」とします。 また、種類は「WEB アプリケーションや WEB API」を選択します。

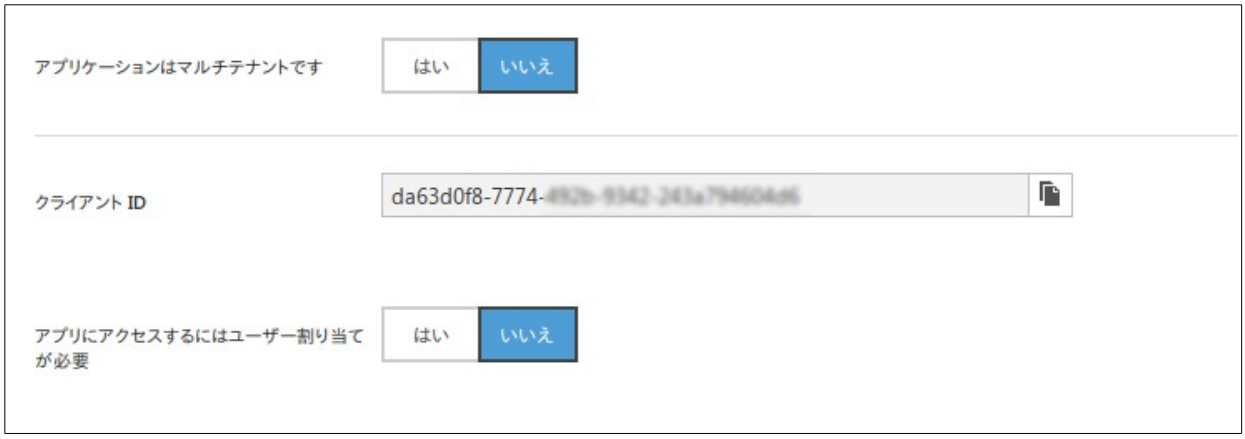
8. 「アプリケーションのプロパティ」を入力します。

    1. 「サインオン URL」には、「http://localhost」を指定します。

    2. 「アプリケーション ID/URI」は、「http://localhost/unicornidm」を指定します。アプリケーション ID は他の登録と同じ値を指定できないため、他のアプリケーションと重ならない値を指定します。Unicorn ID Manager からの連携ではここで設定した値は利用しませんので、任意の値を指定してください。

9. 入力が完了したら、右下の「チェックマーク」をクリックして、アプリケーションの登録を完了します。

10. 画面上部の「構成」をクリックし、画面中央付近にある「クライアント ID」の値を、コピーアンドペーストなどの操作で、別ファイルなどに記録しておきます。



11. 「キー」の項目で、「時間の選択」において、「2 年」を選択します。

12. 画面下部の「保存」アイコンをクリックします。

13. 「キー」の項目に、シークレットキーの値が表示されますので、テキストファイルなどにコピーアンドペーストなどで値を保存しておきます。このページ以外のページに移動すると、このキーの値を取得することはできなくなります。(値を忘れた場合などには、新しいキーを発行してください)

以上で、Office365 の Azure AD にクライアント ID とシークレットキーの登録が完了しました。

5.5.2 アプリケーションのアクセス権設定

Azure AD に登録したアプリケーションにユーザー管理に必要なロールを割り当てるため、Windows 端末にて次の操作を行います。

1. 以下の URL から PowerShell 用の Azure AD モジュールをダウンロードし、インストールします。

   http://msdn.microsoft.com/library/azure/jj151815.aspx

2. インストールして作成された PowerShell を実行します。

3. PowerShell 内で次のコマンドを実行します。

```
$APPNAME="unicornidm"　「unicornidm」の部分は、前述の操作で AzureAD に登録したアプリケーションの「名前」
Import-Module MSOnline
Connect-MsolService
Add-MsolRoleMember -RoleName "User Account Administrator" -RoleMemberType ServicePrincipal
-RoleMemberObjectId (Get-MsolServicePrincipal -SearchString $APPNAME).ObjectId
```

5.5.3 Unicorn ID Manager の設定

Unicorn ID Manager で Office365 連携を行うために、「バックエンド (Azure AD)」を選択します。

画面右上の「バックエンド(Azure AD)を追加」をクリックします。

5.5.4 基本設定

項目名	設定内容
Org	この Azure AD を、どの「対象組織」の管理下に置くか選択します。
サーバーの識別子	この Azure AD を特定できる名称を指定します。Unicorn ID Manager の表示等で利用されます。
プライオリティ	対象組織内で、この Azure AD に対して何番目に処理を行うか1以上の数値で指定します。
Office365 のドメイン名	Office365 の接続先ドメイン名を指定します。
クライアント ID	Office365 に接続するために Azure AD で割り当てられたクライアント ID を指定します。
クライアントシークレット	Office365 に接続するために、Azure AD で生成されたシークレットキーを指定します。 (シークレットキーの有効期限は最大 2 年間です。)
ユーザー登録時にダミーのパスワードを割り当てる	Office365 の認証を SSO で行う場合に、Office365 に登録するパスワードはダミーパスワードとする場合に有効にしてください。 通常は、無効にします。

5.5.5 同期設定

項目名	設定内容
ユーザーのパスワード変更時にこのサー	パスワード変更画面からパスワードを変更したときに、この Office365 に登録されているユーザーのパスワードを変更します。

バーのパスワードを同期する	
ユーザーのアカウント操作時に、このサーバーのアカウントを同期する	管理者がCSVやアカウントの操作を行なった時に、このOffice365のユーザーエントリを更新します。
グループ操作時に、このサーバーのグループを同期する	管理者がグループに関連する操作を行なった時に、このOffice365のグループエントリを更新します。
パスワード変更時に「ユーザーが存在しない」エラーを無視する	このOffice365上でのパスワード変更が失敗しても、パスワード更新としては成功としてみなすための設定です。 複数の連携先でアカウントの統合管理を行うときに、一部の連携先にユーザーが登録されない場合に利用します。 通常は無効に設定してください。

5.5.6 ユーザーエントリのオブジェクトクラス

Office365用のオブジェクトクラスとして、「basic」のみを選択してください。

5.5.7 グループエントリのオブジェクトクラス

Office365用のオブジェクトクラスとして、「basic」のみを選択してください。

6. スキーマ拡張

OpenLDAP や Active Directory でスキーマ拡張を行っている場合に、UnicornIDM から拡張した属性についてのデータ更新等を実施したい場合、Unicorn ID Manager に拡張したオブジェクトクラスや、属性を利用するための設定を行ってください。

6.1 オブジェクトクラス設定

「システム設定」から、LDAP、Active Directory に、新しく利用可能なオブジェクトクラスを登録します。

6.2 属性設定

「システム設定」から、[LDAP オブジェクトクラス」、「Active Directory オブジェクトクラス」、「Google オブジェクトクラス」のぞれぞれに関して、CSV や Web 画面から利用可能な属性を登録します。

- 属性名
  - LDAP や Active Directory に登録する属性名を指定します。
  - CSV のカラム名として利用され、大文字・小文字を区別します。
- 説明
  - Web 管理画面で属性欄に表示される名称です。
- 必須属性
  - ユーザー登録時に、必須となる項目です。
- 追加属性
  - ユーザー登録時、更新時に値が指定されている場合に、連携先に値を反映します。必須属性か、追加属性のどちらかが有効になっていない属性は、処理対象となりません。
- 属性表示
  - ユーザー一覧表示時に、一覧に含まれる項目です。
- 属性更新
  - Web 画面でのユーザー登録、更新時に、入力欄が表示される項目です。
- 優先度
  - Web 画面で項目が表示される順番を制御する値です。小さい値ほど、上部に表示されます。

7. 改版履歴

- 2010 年 12 月 18 日　v1.0
  - 初版
- 2011 年 1 月 19 日　v2.0
  - 初期設定方法の追加
- 2011 年 11 月 14 日　v2.1
  - Unicorn ID Manager 2.0 の設定項目を追加
- 2012 年 1 月 17 日　v2.2
  - RHEL6 対応について記載
- 2012 年 5 月 2 日　v2.3
  - Unicorn ID Manager 2.1 の設定項目を追加
- 2013 年 4 月 19 日　v2.4
  - RHEL6 の場合に必要となるパッケージを追加
  - LDAP サーバの場合に指定する objectClass に関する記述を追加
  - Active Directory で事前にホームディレクトリを作成しない場合についての記述を追記
- 2014 年 6 月 26 日　v2.5
  - 「インストールガイド」から「インストール・アップデートガイド」に改題
  - バージョンアップに伴い、パッケージ一覧を更新
  - アップデート手順の追記
- 2014 年 7 月 2 日　v2.6
  - Google バックエンド利用時にアップデート手順を追記
- 2014 年 10 月 28 日　v2.7
  - パッケージ構成を修正
  - パスワード変更画面の変更について記載
  - Google Apps の設定方法をバージョン 2.3 以降のものに修正
- 2014 年 11 月 28 日　v2.8

- 属性設定について記載
- オブジェクトクラス設定について記載

- 2014 年 12 月 11 日　v2.9
  - Google Apps 利用時にサーバーの時刻を正しく設定する必要がある旨を追記
- 2014 年 12 月 17 日　v3.0
  - Google Developers Console サービスの有効化を追記
- 2015 年 2 月 20 日　v3.1
  - スコープをコピーアンドペーストすると間にスペースが入ってしまう問題を修正
- 2015 年 12 月 1 日　v3.2
  - Office365 連携のための設定について追記