

Unicorn ID Manager

管理者ガイド



OSSTech

オープンソース・ソリューション・テクノロジー(株)

文書番号: OSTD-UnicornIDM-AdminGuide

作成日: 2011 年 5 月 17 日

リビジョン: 1.0

目次

1. はじめに	1
2. 一般ユーザー向けパスワード変更ページ	2
3. ユーザー管理機能の利用	4
3.1 管理者ログイン	4
4. 1 ユーザーを対象とした操作	6
4.1 アカウント	6
4.1.1 注意事項	7
4.2 ユーザー情報表示	8
4.3 ユーザー削除	9
4.4 ユーザー情報更新	10
4.5 ユーザーのパスワード変更(管理者向け)	11
4.5.1 パスワード変更履歴の確認	12
4.6 1 ユーザーの有効化、無効化	12
5. CSV を利用したユーザー一括操作	14
5.1 ユーザー一括登録	14
5.1.1 CSV ファイルのアップロード	14
5.2 実行結果一覧	16
5.3 ユーザー一覧取得	17
5.4 ユーザー一括更新	19
5.5 ユーザー一括削除	20
5.6 ユーザー一括無効化・有効化	21
5.7 CSV ファイルで指定可能な項目	22
5.7.1 必須の項目	22
5.7.2 Active Directory において指定可能な項目	22
5.7.3 OpenLDAP において指定可能な項目	22
6. Google Apps 処理時のエラーメッセージ	24
7. 管理者アカウントの管理	25
7.1 管理者の登録	25
7.2 管理者アカウントのパスワード変更	27
8. システム関連情報	28
8.1 関連ファイル一覧	28
8.2 設定のバックアップ	28
9. 注意点	29

9.1 サイトについて.....	29
10. 改版履歴	30

1.はじめに

本書は、Unicorn ID Manager の管理者向けマニュアルです。

Unicorn ID Manager が次の環境に構築されていることを前提に説明を行います。

項目	値
Unicorn ID Manager の管理者ユーザー名	admin
Unicorn ID Manager の管理者パスワード	unicornidm
Unicorn ID Manager の管理対象組織名	example
サーバー名	unicornsv.example.com

実際にご利用の際には、本書で記載しているパラメーターを、お客様のシステムに合わせたパラメーターに読み替えてください。

本書では、ユーザーアカウントが登録されているLDAP、Active Directory、Google Appsなどのことを「ユーザーリポジトリ」と呼びます。お客様のシステム構成によって、ユーザーリポジトリの構成は変わります。

2. 一般ユーザー向けパスワード変更ページ

Unicorn ID Manager が提供するパスワード変更ページは、次の URL で提供されます。

`http://UnicornIDM のホスト名/unicornIDM/passwd/change/[組織名]/`

本ドキュメントの構築例の場合、具体的には次の URL となります。

`http://unicornsv.example.com/unicornIDM/passwd/change/example/`

Unicorn ID Manager の提供するパスワード変更ページに Web ブラウザでアクセスすると、次の画面が表示されます。



The image shows the Unicorn ID Manager password change page. At the top is a blue header with the Unicorn ID Manager logo, which includes a unicorn and the text 'Unicorn ID Manager' and 'ユニコーンIDマネージャー'. Below the header, the page title is '対象組織：統合認証センター'. The main section is titled 'パスワード設定' (Password Setting). It contains a message: 'ユーザー名と現在のパスワード、新しいパスワードを入力してください。' (Please enter your username and current password, and a new password). There are four input fields: 'ユーザー名:' (Username) with the value 'takeda', '現在のパスワード:' (Current Password) with masked characters '*****', '新しいパスワード:' (New Password) with masked characters '*****', and '新しいパスワード(再入力):' (New Password (re-enter)) with masked characters '*****'. A 'パスワード変更' (Change Password) button is located below the input fields. At the bottom, there is a note: '新しいパスワードは8文字以上で設定してください。' (Please set a new password of 8 or more characters).

パスワードの変更が成功すると、次の画面が表示されます。



The image shows the Unicorn ID Manager password change success page. It has the same blue header and title '対象組織：統合認証センター' as the previous page. The main message is 'パスワードの変更に成功しました。' (Password change was successful). Below this message is a link: 'パスワード変更画面に戻る' (Return to the password change screen).

パスワードの変更に失敗すると、エラーメッセージが表示されます。

 Unicorn ID Manager
ユニコーンIDマネージャー

対象組織：統合認証センター

■ パスワード設定

パスワードの変更に失敗しました。

ユーザー名とパスワードが一致しません。

ユーザー名と現在のパスワード、新しいパスワードを入力してください。

ユーザー名:

takeda

現在のパスワード:

新しいパスワード:

新しいパスワード(再入力):

パスワード変更

新しいパスワードは8文字以上で設定してください。

3. ユーザー管理機能の利用

本章では、Unicorn IDM によるユーザー情報の管理手順を説明します。

3.1 管理者ログイン

Unicorn IDM からユーザー情報を管理するためには、Unicorn IDM の管理者アカウントでログインする必要があります。ブラウザで下記の URL にアクセスし、Unicorn ID Manager に管理者アカウントでログインしてください (※URL の最後のスラッシュまで必要です)。

- <https://unicornsv.example.com/unicornIDM/idm/index/>

ログイン画面が表示されますので、インストール時に設定した Unicorn IDM の管理者アカウントでログインします。



The login screen for Unicorn ID Manager features a blue header with a unicorn logo and the text 'Unicorn ID Manager'. Below the header, a message states '管理者は最初にログインしなければなりません。' (Administrators must log in first). There are input fields for 'ユーザー名' (Username) and 'パスワード' (Password), followed by a 'ログイン' (Login) button. At the bottom, a copyright notice reads '© 2011 Open Source Solution Technology Corporation, All Rights Reserved.'

OpenLDAP や Active Directory に登録されているユーザーを管理者として追加登録済みの場合は、それらのシステムに登録されているユーザーのパスワードでログインすることも可能です。

認証が成功すると、操作対象の組織を選択する画面が表示されます。複数の組織単位を設定している場合は、複数の組織が表示されます。



The organization selection screen has a blue header with the Unicorn ID Manager logo. On the left, a 'Menu' sidebar lists '対象組織' (Target Organization), 'システム設定' (System Settings), and 'ログアウト' (Logout). The main area is titled '操作対象の組織の選択' (Select target organization) and includes the instruction '操作対象の組織を選択してください。' (Please select the target organization). Below this is a section '組織の一覧' (List of organizations) with a button labeled 'example'. A copyright notice '© 2011 Open Source Solution Technology Corporation, All Rights Reserved.' is at the bottom.

表示されている「組織の一覧」から操作対象の組織を選択することで、ユーザー情報管理操作のメニューが表示されます。

選択した組織に対するユーザー管理画面となりますので、各メニューから操作を開始します。

 **Unicorn ID Manager**
ユニコーンIDマネージャー

Menu
トップ
ユーザー一覧
実行結果一覧
パスワード変更履歴
対象組織
システム設定
ログアウト

対象組織 : example

アカウント管理
ユーザー名

CSV一括処理

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

4.1 ユーザーを対象とした操作

4.1 アカウント

ユーザーを1名登録したい場合は、「アカウント登録」を選択します。

画面に表示される設定項目は、Unicorn ID Manager の設定内容によって異なります。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example
アカウント登録

説明(属性名)	値
ユーザー名(username)	
パスワード(password)	
姓 (sn)	
名 (givenName)	
UID番号 (uidNumber)	1006
GID番号 (gidNumber)	1000
UNIXホームディレクトリ (unixHomeDirectory)	/home/%USERNAME%
ログインシェル (loginShell)	/bin/bash
GECOS (gecos)	
説明 (description)	
メールアドレス (mail)	
Windows プロファイルパス (profilePath)	\\\\adserver1\\profiles\\%USER
Windows ホームドライブ (homeDrive)	X:
Windows ホームディレクトリ (homeDirectory)	\\\\adserver1\\homes\\%USER
LDAP所属グループ (LdapGroups)	
Active Directory 所属グループ (AdGroups)	

対象組織
☒ ldapsv1 ☒ adserver1

デフォルト値が設定されている項目には、値が入力されています。

赤字となっている箇所は値の入力が必須の項目です。それ以外の値については、空白のままでも構いません。

なお、上記画面で表示されている括弧内の英字は、CSV ファイルでユーザーの一括登録を実施する際のカラム名と同一です。

各項目の入力を完了した後に、最下段の「対象組織」を選択します。

チェックを外した「対象組織」に対しては、ユーザーの登録が行われませんので、ユーザー登録を行いたくない

レポジトリがある場合に選択してください。



いずれかのレポジトリへのがエラーになった場合でも、「OK」が表示されているレポジトリに対するユーザー登録は成功していますので、エラーになったレポジトリに対してのみ再登録を実施してください。

※ 既にユーザー登録済みのレポジトリに対するユーザー登録操作を行っても、「ユーザーが既に存在します」というエラーになるのみですので、再登録の操作を実施しても問題ありません。

|| 4.1.1 注意事項

ユーザー登録時に値を入力する際の注意事項です。

- AdGroups
 - Active Directory のプライマリグループ以外のグループに所属させたいとき、グループ名を指定してください。「,」で区切って、複数のグループ名を指定することもできます。(事前に Active Directory 上にグループを作成してください)
- LdapGroups
 - OpenLDAP のプライマリグループ以外のグループに所属させたいときは、LdapGroups 属性に、グループ名を指定してください。「,」で区切って、複数のグループ名を指定することもできます。事前に OpenLDAP にグループを作成してください。
- unixHomeDirectory
 - UNIX 用のホームディレクトリの属性は、「homeDirectory」ではなく、「unixHomeDirectory」にホームディレクトリのパスを指定してください。(「home Directory」は Active Directory でのホームディレクトリ属性となります)

4.2 ユーザー情報表示

登録済みのユーザーのユーザー情報を確認するときは、「トップ」ページの「アカウント管理」のユーザー名の入力フィールドにユーザー名を入力し、「ユーザー情報表示」を押します。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example
アカウント管理
 ユーザー名 [ユーザー情報表示](#)

[アカウント登録](#)
[ユーザー削除](#)

[ユーザー情報更新](#)
[パスワード変更](#)

[ユーザー有効化](#)
[ユーザー無効化](#)

各レポジトリから収集した情報を統合し、次の画面で表示します。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example
ユーザー情報
 ユーザー名 : takasaki

[更新](#)
[有効化](#)
[無効化](#)
[削除](#)

説明(属性名)	値
姓(sn)	高崎
名(givenName)	圭太
UNIXホームディレクトリ(unixHomeDirectory)	/home/takasaki
GID番号(gidNumber)	1000
UID番号(uidNumber)	1006
ログインシェル(loginShell)	/bin/bash
GECOS(gecos)	Keita Takasaki
メールアドレス(mail)	takasaki@example.com
Windows プロファイルパス(profilePath)	\\adserver1\profiles\takasaki
表示名(displayName)	高崎 圭太
Windows ホームドライブ(homeDrive)	X:
Windows ホームディレクトリ(homeDirectory)	\\adserver1\homes\takasaki
LdapGroups	
AdGroups	

ログインステータス
 Idapsv1 ログイン可
 adserver1 ログイン可

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

画面下部の「ログインステータス」には、各サービスの利用許可状況が表示されています。

そのレポジトリを利用可能な場合は「ログイン可」と表示され、利用不可能な場合は「ログイン不可」と表示されます。

4.3 ユーザー削除

1 ユーザーを削除したい場合は、「ユーザー削除」を選択します。

ユーザー名の入力画面が表示されますので、削除するユーザーのユーザー名を入力し、「次へ」をクリックします。



Menu

- トップ
- ユーザー一覧
- 実行結果一覧
- パスワード変更履歴
- 対象組織
- システム設定
- ログアウト

対象組織 : example

ユーザー削除

削除するユーザー名を入力

takasaki

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

削除対象のユーザー情報の一部の情報が表示されますので、対象ユーザーに間違いが無いことを確認してから、「削除」をクリックします。

チェックを外した「対象組織」からはユーザーの削除は行われません。



Menu

- トップ
- ユーザー一覧
- 実行結果一覧
- パスワード変更履歴
- 対象組織
- システム設定
- ログアウト

対象組織 : example

ユーザー削除

ユーザー名 : takasaki

姓 高崎
名 圭太

ログインステータス

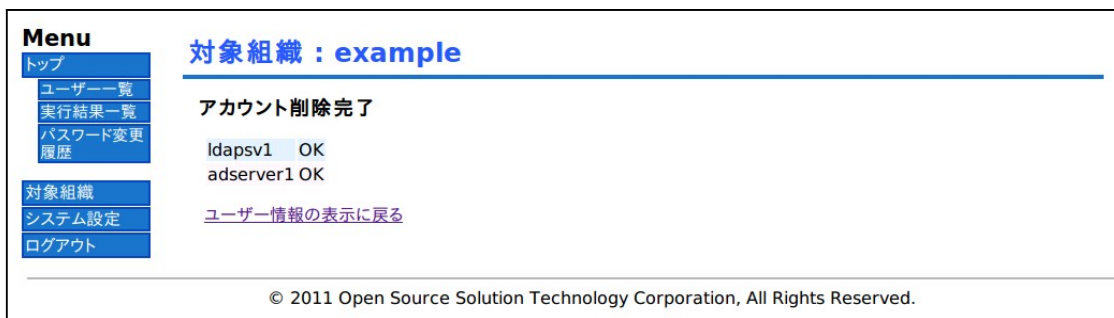
ldapsv1 ログイン可
adserver1 ログイン可

対象組織

☒ ldapsv1 ☒ adserver1

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

ユーザー削除が完了すると、次の画面が表示されます。



Menu

- トップ
- ユーザー一覧
- 実行結果一覧
- パスワード変更履歴
- 対象組織
- システム設定
- ログアウト

対象組織 : example

アカウント削除完了

ldapsv1 OK
adserver1 OK

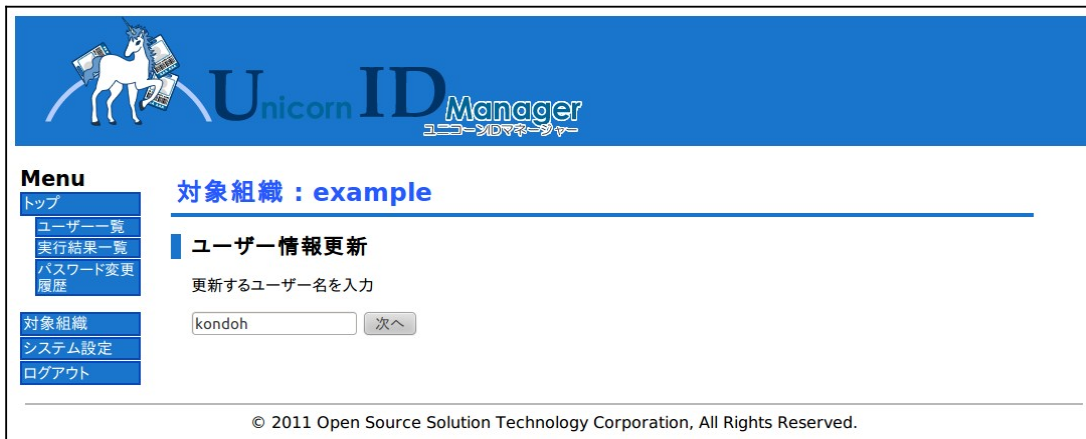
[ユーザー情報の表示に戻る](#)

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

4.4 ユーザー情報更新

1 ユーザーの情報を更新したい場合は、「トップ」ページの「ユーザー情報更新」を選択します。

ユーザー名を入力画面が表示されますので、更新するユーザーのユーザー名を入力し、「次へ」をクリックします。



更新対象のユーザーのユーザー情報が表示されますので、更新後の値を入力後、「ユーザー情報更新」をクリックすることで、ユーザー情報の更新が行われます。



説明(属性名)	値
姓(sn)	近藤
名(givenName)	徹
UID番号(uidNumber)	1006
GID番号(gidNumber)	1000
UNIXホームディレクトリ(unixHomeDirectory)	/home/kondoh
ログインシェル(loginShell)	/bin/bash
GECOS(gecos)	Toru Kondoh
説明(description)	
メールアドレス(mail)	kondoh@example.com
Windows プロファイルパス(profilePath)	\\adserver1\profiles\kondoh
Windows ホームドライブ(homeDrive)	X:
Windows ホームディレクトリ(homeDirectory)	\\adserver1\homes\kondoh
LDAP所属グループ(LdapGroups)	
Active Directory 所属グループ(AdGroups)	

対象組織

☒ ldapsv1 ☒ adserver1

ユーザー情報更新

4.5 ユーザーのパスワード変更(管理者向け)

管理者がユーザーのパスワードを強制的に変更するときは、「トップ」ページの「パスワード変更」をクリックします。

ユーザー名の入力画面が表示されますので、パスワードを変更するユーザーのユーザー名を入力し、「次へ」をクリックします。



表示されたユーザー情報を確認し、対象ユーザーに間違いが無ければ、「新しいパスワード」、「新しいパスワード(再入力)」に、新しく割り当てるパスワードを入力してから、「変更」をクリックします。



パスワードの変更が完了すると、次のメッセージが表示されます。



4.5.1 パスワード変更履歴の確認

画面左の「パスワード変更履歴」から、Unicorn ID Manager 経由でパスワードを変更したユーザーの変更履歴を確認することができます。

Menu

トップ

ユーザー一覧

実行結果一覧

パスワード変更履歴

対象組織

システム設定

ログアウト

対象組織 : example

パスワード変更履歴

日時	実行ユーザー	ユーザー名	結果	理由
2011-05-17 20:15:39,762	admin	kondoh	成功	
2011-05-17 18:31:11,628	takeda	takeda	失敗	ユーザー名とパスワードが一致しません。
2011-05-17 18:29:08,673	takeda	takeda	成功	

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

パスワードを変更したユーザーが管理者ユーザーの場合は、「実行ユーザー」の欄が黄色になります。

「ユーザー名」にパスワードの変更対象のユーザー名が表示され、パスワード変更処理の結果を確認することが可能です。

4.6 1 ユーザーの有効化、無効化

ユーザーを無効化すると、レポジトリにユーザーを登録したまま、そのレポジトリを利用したログインを禁止することができます。

無効化したユーザーを、有効化すると、再度、そのユーザーはログイン可能となります。

1 ユーザーを有効化、無効化したい場合は、「トップ」ページの「ユーザー有効化」、あるいは「ユーザー無効化」を選択します。

ユーザー名の入力画面が表示されますので、無効化(有効化)したいユーザー名を入力後、「次へ」をクリックし

ます。(画面は無効化の場合)



指定したユーザーの情報が表示されますので、対象ユーザーに間違いが無いことを確認し、「無効化」もしくは「有効化」をクリックします。

「ログインステータス」には、各レポジトリでユーザーのアカウントの状態が表示されており、「ログイン可」、「ログイン不可」のいずれかが表示されます。



5. CSV を利用したユーザー一括操作

5.1 ユーザー一括登録

CSV ファイルに記載したユーザーを一括登録したい場合は、登録対象のユーザー情報を CSV ファイルに記載します。

一括登録時の CSV ファイルの書式は、次の形式となります。

username	sn	givenName	password	
suzuki	鈴木	太郎	Haen8toh	
yamada	山田	花子	Ciaw7tu4	

- 1 行目は各列の属性を表すヘッダを意味します。
- 1 列目は必ず”username”としてください。ユーザーのユーザー名として扱われます。2 列目以降は、ヘッダに記載された属性として扱われるため、列に記載する属性の順番は自由です。
- 必須属性以外の属性は、デフォルト値以外の値を指定するときに記載してください。
- 1 行目のヘッダ部分は太文字、小文字も区別されますので、givenName などの記述に注意してください。
- 各項目の値にて、最初の空白、最後の空白については削除して登録されます。ただし、全角の空白は削除しません。（全角空白は最初、最後に存在していても登録されます。）
- CSV ファイルで処理可能な属性については、各レポジトリ、および Unicorn ID Manager の設定に基づきます。
- CSV ファイルの書式は RFC に準拠しています(RFC4180)。RFC には、カラムのデータをダブルクォーテーションで囲む必要がある場合の説明などが記載されているため、CSV の書式に関しては RFC4180 をご参照ください(<http://www.ietf.org/rfc/rfc4180.txt>)。例えば、カラムにダブルクォーテーション、カンマなどを含む場合は、カラムをダブルクォーテーションで囲む必要があります。

5.1.1 CSV ファイルのアップロード

CSV ファイルの準備が完了したら、管理ツールの「ユーザー一括登録」を選択します。

ファイルの選択画面となりますので、「参照」をクリックし、ユーザー登録に利用する CSV ファイルを選択します。

CSV ファイルを Excel で作成した場合は「エンコーディング」として、「シフト JIS」を選択します。

CSV ファイルを OpenOffice などで作成した場合は「エンコーディング」として、「UTF-8」を選択します。

エンコーディングを正しく選択したら、「アップロード(プレビュー)」をクリックします。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

CSVファイルでユーザーを登録

ユーザーの情報を記載したCSVファイルを選択してください。

ファイル: [参照...](#)

エンコーディング: [シフトJIS](#) ▼

[アップロード\(プレビュー\)](#)

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

CSV ファイルの先頭 5 エントリがプレビューとして表示されます。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

CSVファイルでユーザーを登録

CSVファイルのエントリを表示しています。これは、最初の 5 個のエントリのみ表示しています。

CSVファイルのエントリに問題が無ければ、ユーザー登録 を押してください。

ユーザー名	sn	givenName	password	gidNumber
suzuki	鈴木	太郎	Haen8toh	3000
yamada	山田	花子	Ciaw7tu4	3000

[ユーザー登録](#)

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

CSV ファイルの誤りによるカラムのずれなどが無ければ、「ユーザー登録」をクリックします。

画面が切り替わり、各レポジトリに対するユーザー登録処理が開始されます。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

CSVファイルでユーザーを登録

実行結果

ldapsv1 実行中

adserver1 実行中

新しい操作を実行可能です。次に行う操作を選択してください。

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

ユーザー一括操作は、各レポジトリごとに、別々に処理が行われます。

ユーザー一括操作の操作結果を確認するためには、画面左の「実行結果一覧」をクリックします。

5.2 実行結果一覧

CSV ファイルを用いたユーザー一括操作の実行結果は、画面左側の「実行結果一覧」から確認します。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)

[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

実行結果の一覧

詳細を選択してください。

日時	操作内容	対象組織	全部	成功	失敗	詳細情報
2011-05-17 20:41:54	ユーザー登録	ldapsv1	2	0	2	詳細 ダウンロード
2011-05-17 20:41:54	ユーザー登録	adserver1	2	0	2	詳細 ダウンロード
2011-05-17 20:35:54	ユーザー登録	ldapsv1	2	2	0	詳細 ダウンロード
2011-05-17 20:35:54	ユーザー登録	adserver1	2	2	0	詳細 ダウンロード
2011-05-17 18:58:35	ユーザー削除	ldapsv1	6	6	0	詳細 ダウンロード
2011-05-17 18:58:35	ユーザー削除	adserver1	6	6	0	詳細 ダウンロード
2011-05-17 18:20:03	ユーザー登録	ldapsv1	6	6	0	詳細 ダウンロード
2011-05-17 18:20:03	ユーザー登録	adserver1	6	6	0	詳細 ダウンロード

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

ユーザー登録に失敗したエントリがある場合には、右側の「詳細」をクリックすることで、各レポジトリに対する処理結果の詳細が表示されます。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)

[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

実行結果の一覧情報

日時 2011-05-17 20:41:54
操作内容 ユーザー登録
対象組織 ldapsv1

操作結果

suzuki User already exists.
yamada User already exists.

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

「ダウンロード」をクリックすることで「操作結果」の内容をテキストファイルとしてダウンロードすることが可能です。

5.3 ユーザー一覧取得

各レポジトリに登録されたユーザー情報の一覧を取得したいときは、画面左側の「ユーザー一覧」を選択します。

画面には、「ユーザー一覧取得」、および、これまでに取得したユーザー一覧情報へのリンクが表示されます。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

ユーザー一覧の取得メニュー

現在のユーザー一覧を取得したいときは、「ユーザー一覧取得」をクリックしてください。

[ユーザー一覧取得](#)

表示したいユーザー一覧情報を選択してください。

日時	ユーザー一覧情報	詳細	詳細
2011-05-17 20:32:29	HTML CSV	ldapsv1	adserver1
2011-05-17 18:20:12	HTML CSV	ldapsv1	adserver1

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

「ユーザー一覧取得」をクリックすると、ユーザー一覧の取得処理がバックグラウンドで開始されます。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

ユーザー一覧の取得結果

各サーバーからユーザー一覧の取得完了

ldapsv1 実行中
adserver1 実行中

[ユーザー一覧に戻る](#)

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

取得したユーザー一覧の情報は、「HTML」「CSV」などのリンクから確認することができます。

「HTML」のリンクをクリックすると、各レポジトリから取得したユーザー情報を統合した形式で、ユーザー一覧情報がアルファベット順に表示されます。

Menu トップ ユーザー一覧 実行結果一覧 パスワード変更履歴 対象組織 システム設定 ログアウト		対象組織 : example																																																												
		ユーザー一覧																																																												
		<table> <tr> <th>username</th><th>sn</th><th>givenName</th><th>uidNumber</th><th>gidNumber</th><th>unixHomeDirectory</th><th>loginShell</th></tr> <tr> <td>Administrator</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>Guest</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>kondoh</td><td>近藤</td><td>徹</td><td>1006</td><td>1000</td><td>/home/kondoh</td><td>/bin/bash</td></tr> <tr> <td>krbtgt</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>suzuki</td><td>鈴木</td><td>太郎</td><td>1007</td><td>3000</td><td>/home/suzuki</td><td>/bin/bash</td></tr> <tr> <td>unicornidm</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>yamada</td><td>山田</td><td>花子</td><td>1008</td><td>3000</td><td>/home/yamada</td><td>/bin/bash</td></tr> </table>					username	sn	givenName	uidNumber	gidNumber	unixHomeDirectory	loginShell	Administrator							Guest							kondoh	近藤	徹	1006	1000	/home/kondoh	/bin/bash	krbtgt							suzuki	鈴木	太郎	1007	3000	/home/suzuki	/bin/bash	unicornidm							yamada	山田	花子	1008	3000	/home/yamada	/bin/bash
username	sn	givenName	uidNumber	gidNumber	unixHomeDirectory	loginShell																																																								
Administrator																																																														
Guest																																																														
kondoh	近藤	徹	1006	1000	/home/kondoh	/bin/bash																																																								
krbtgt																																																														
suzuki	鈴木	太郎	1007	3000	/home/suzuki	/bin/bash																																																								
unicornidm																																																														
yamada	山田	花子	1008	3000	/home/yamada	/bin/bash																																																								
		© 2011 Open Source Solution Technology Corporation, All Rights Reserved.																																																												

- 表の1行目は、CSV 登録時に利用するヘッダー名が表示されます。
- 表の最後のカラムは、各レポジトリにおけるアカウントのログイン許可状況です。以下の3つのステータスがあります。
 - 「True」：ユーザーが登録されており、ログイン可能です。
 - 「False」：ユーザーが登録されていますが、ログイン禁止です。
 - 「空白」：ユーザーが登録されていません。

また、各ユーザーのユーザー名をクリックすると、各ユーザーごとの詳細情報の表示画面となります。

「CSV」のリンクをクリックすると、一覧情報を CSV ファイルとしてダウンロードすることができます。このファイルを編集することで、「ユーザー情報一括更新」などのメニューで再利用することが可能です。

「各レポジトリ」の名称のリンクをクリックすると、各レポジトリごとの登録ユーザーの情報がテキストファイルとして表示されます。このテキストファイルに含まれる最後のカラム「active」は、ユーザーアカウントの有効(True)・無効(False)を表します。

5.4 ユーザー一括更新

各レポジトリに登録されているユーザー情報を一括更新することができます。

更新可能な情報は、ユーザー登録時に利用した属性の値で、次の書式の CSV ファイルを作成します。

username	sn	givenName	password	その他の項目…
yamada	山田	太郎	ds4gU!fd6s	
kondoh	近藤	たつや	kLifj430kd	
suzuki			TfdGaq0-	

- 1 行目はヘッダとして、更新対象とする項目の属性名を記載します。
- 値が指定されていないフィールドの情報は更新されません。
- 更新が不要な属性をヘッダに含める必要はありません。

例えば、ユーザーのパスワードのみを一括更新したい場合は、次の書式の CSV ファイルを作成します。

username	password
yamada	paiV5oon
kondoh	chaiS2ya
suzuki	Muwah6ch

CSV ファイルの準備完了後に、「トップ」から「ユーザー一括更新」を選択します。

「参照」ボタンをクリックし、ユーザー更新に利用する CSV ファイルを選択します。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

CSVファイルでユーザー情報を更新

ユーザーの情報を記載したCSVファイルを選択してください。

ファイル: [参照...](#)

エンコーディング: UTF-8 ▼

[アップロード\(プレビュー\)](#)

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

CSV ファイルのエンコーディングを選択し、「アップロード」をクリックします。

CSV ファイルの先頭 5 エントリが表示されますので、CSV ファイルの誤りによるカラムのずれなどが無いことを確認します。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

CSVファイルでユーザー情報を更新

CSVファイルのエントリを表示しています。これは、最初の 5 個のエントリのみ表示しています。

CSVファイルのエントリに問題が無ければ、ユーザー更新 を押してください。

ユーザー名	password
yamada	paiV5oon
kondoh	chaiS2ya
suzuki	Muwah6ch

[ユーザー更新](#)

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

問題無ければ、「ユーザー更新」をクリックして、ユーザー一括更新処理を開始します。

Menu
[トップ](#)
[ユーザー一覧](#)
[実行結果一覧](#)
[パスワード変更履歴](#)
[対象組織](#)
[システム設定](#)
[ログアウト](#)

対象組織 : example

CSVファイルでユーザー情報を更新

実行結果

ldapsv1	実行中
adserver1	実行中

新しい操作を実行可能です。次に行う操作を選択してください。

© 2011 Open Source Solution Technology Corporation, All Rights Reserved.

ユーザー情報の更新結果の確認は、「実行結果一覧」で確認します。

5.5 ユーザー一括削除

複数のユーザーを一括削除したい場合、次の書式の CSV ファイルを作成します。

username
yamada
kondoh
suzuki
....

- 1 行目はヘッダとして「username」を指定します。
- 必要な項目はユーザー名のみです。CSV ファイルの 2 列目以降に項目を記述しても無視されます(例

例えばユーザー登録に使用した CSV をそのまま流用してユーザー削除に使用することも可能です。

CSV ファイル作成後、「トップ」から「ユーザー一括削除」を選択します。

CSV ファイルの選択後の操作は、ユーザー登録時と同じです。

ユーザー削除を行う際には以下の点にご注意ください。

- Active Directory
 - ユーザーを削除すると、同じ名前でユーザーを作成しても、削除前のユーザーとは SID が異なるため、違うユーザーとして扱われます。そのため、削除前のユーザーが作成したファイルやフォルダにアクセスすることはできなくなります。
- Google Apps
 - ユーザーを削除すると、Google Apps に保存されていたユーザーの全てのメールも削除されます。削除されたメールを元に戻すことはできませんので、一時的にユーザーのログインを禁止したい場合は、「ユーザー削除」ではなく、「ユーザー無効化」を実施してください。
 - Google Apps では、一度削除したユーザーは 5 日間が経過するまで、同じユーザー名のユーザーを作成することができません。

5.6 ユーザー一括無効化・有効化

ユーザー情報を登録したまま、各レポジトリへのログインを一括で禁止したい場合、「ユーザー一括無効化」を行います。無効化された複数のユーザーを一括で有効化したい場合、「ユーザー一括有効化」を行います。

複数のユーザーを一括無効化、一括有効化したい場合、次の書式の CSV ファイルを作成します。

username
yamada
kondoh
suzuki
....

- 1 行目はヘッダとして「username」を指定します。
- 必要な項目はユーザー名のみです。CSV ファイルの 2 列目以降に項目を記述しても無視されます(例えばユーザー登録に使用した CSV をそのまま流用してユーザー削除に使用することも可能です)。

CSV ファイル作成後、「トップ」から「ユーザー一括無効化」、もしくは「ユーザー一括有効化」を選択します。

CSV ファイルの選択後の操作は、ユーザー一括登録時と同じです。

5.7 CSV ファイルで指定可能な項目

各ユーザーリポジトリに対するユーザー登録時には、ユーザーに設定するパラメータとして Unicorn ID Manager のデフォルトの設定値が利用されます。デフォルト値以外を指定したい場合、追加の項目を指定したいなどの場合は、CSV にその項目と値を記述してください。

なお、Unicorn ID Manager では、各レポジトリごとに設定を行うことで、設定可能な属性をカスタマイズすることができます。

5.7.1 必須の項目

以下の項目は、どのユーザーリポジトリにおいても、ユーザーを登録する際に必須の項目となります。

CSV における項目名	説明	記述形式
username	ユーザー名	アルファベット
sn	姓	アルファベット、日本語
givenName	名	アルファベット、日本語
password	パスワード	アルファベット

5.7.2 Active Directory において指定可能な項目

CSV における項目名	説明	記述形式
scriptPath	ログオンスクリプト	logon.bat
profilePath	プロファイルパス	Windows ファイルパス(¥¥server¥...)
homeDirectory	ホームディレクトリ	Windows ファイルパス(¥¥server¥...)
AdUserSuffix	ユーザーを登録する OU	“ou=学科,ou=学部”
AdPrimaryGroup	ユーザーが所属するプライマリグループ	アルファベット
AdGroups	グループ	アルファベット

5.7.3 OpenLDAP において指定可能な項目

CSV における項目名	説明	記述形式
unixHomeDirectory	ホームディレクトリ	UNIX のディレクトリパス(例: /home/A/ユーザー名)
loginShell	ログインシェル	UNIX のファイルパス(例: /bin/bash)
uidNumber	ユーザー ID	数字(例: 2001)
gidNumber	グループ ID	数字(例: 1000)

LdapPrimaryGroup	ユーザーが所属するプライマリ グループ名	グループ名
LdapGroups	ユーザーが所属するグループ	“group1,group2,group3”
LdapUserSuffix	ユーザーを登録するLDAP の OU	“ou=sales”

6. Google Apps 処理時のエラーメッセージ

Google Apps に対するユーザー登録、削除、更新時などに履歴の詳細にエラーが記録されることがあります。記録されるエラーとその原因について下記を参照してください。

エラーメッセージ	原因
UnknownError(1000)	原因不明のエラーです。
UserDeletedRecently(1100)	削除してから 5 日以内に同じユーザー名のアカウントを作成しようとしています。
DomainUserLimitExceeded(1200)	ドメインに作成できるユーザー数が制限に達しています。
EntityExists(1300)	既に存在するユーザーのアカウントを作成しようとしています。
EntityDoesNotExist(1301)	指定したユーザー名のアカウントが存在しません。
EntityNameIsReserved(1302)	指定したユーザー名は Google 側で予約されていて利用できません。
InvalidGivenName(1400)	givenName に指定した値が不適切です。
InvalidFamilyName(1401)	sn に指定した値が不適切です。
InvalidPassword(1402)	指定したパスワードが不適切です。
InvalidUsername(1403)	指定したユーザー名が不適切です。

7. 管理者アカウントの管理

本章では、Unicorn IDM の管理者アカウントの管理について説明します。

7.1 管理者の登録

通常は Unicorn IDM の初期設定時に管理者(スーパーユーザー)を1名登録済みです。管理者ユーザーを追加したい場合は、次の手順で登録します。

1. Unicorn IDM の管理画面にアクセスし、管理者ユーザーでログインします。

<https://unicornsv.example.com/unicornIDM/admin/>

2. 管理者メニュー画面の「サイト管理」→「Auth」→「ユーザ」の「追加」をクリックします。



The screenshot shows the '管理者メニュー' (Admin Menu) interface. At the top, it says 'ようこそ admin. パスワード変更 / ログアウト'. The main section is 'サイト管理' (Site Management). Under 'Auth', there are links for 'グループ' (Groups) and 'ユーザ' (Users), each with '追加' (Add) and '変更' (Edit) icons. Below 'Auth' is the 'Backends' section, which lists various authentication backends like LDAP, Active Directory, Google Apps, etc., each with '追加' and '変更' icons. At the bottom is the 'Sites' section with a 'サイト' (Site) link and '追加' and '変更' icons. On the right side, there is a '最近行った操作' (Recent Operations) section showing a list of actions performed, such as adding a new user or changing a password.

3. ユーザー名とパスワードを入力し、右下の「保存」をクリックします。ユーザー名には、「a-z」、「A-Z」、「0-9」の文字のみ利用可能です。

管理者メニュー		ようこそ admin. パスワードの変更 / ログアウト
ホーム > Auth > ユーザ > 追加 ユーザ		
ユーザを追加		
まずユーザ名とパスワードを登録してください。その後詳細情報が編集可能になります。		
ユーザー名: この項目は必須です。半角アルファベット、半角数字、半角アンダーバーで30文字以下にしてください。		
パスワード: 		
パスワード(確認用): 確認のため、再度パスワードを入力してください。		
保存してもう一つ追加 保存して編集を続ける 保存		

なお、管理メニューへのログインは、上記で登録したパスワードの他に、ユーザーリポジトリでも認証が行われますので、いずれかの認証に成功すれば、Unicorn ID Manager にログイン可能です。

上記の手順で登録した管理者はスーパーユーザー権限を持たないため、管理者ユーザーの登録作業や、Unicorn ID Manager の「システム設定」(<https://unicornsv.example.com/unicornIDM/admin/>)を行なえません。

新たに作成した管理者でシステム設定も行ないたい場合には、ユーザー登録後に、「パーミッション」設定の「スタッフ権限」、「スーパーユーザー権限」の両方にチェックを入れてください。

ユーザー名: XXXXXX この項目は必須です。半角アルファベット、半角数字、半角アンダーバーで30文字以下にしてください。	
パスワード: sha1\$4d31f\$2dabd389e8e32f31990a9176b7f; '[algo]\$[salt]\$[hexdigest]'形式か、パスワード変更フォームを使ってください。	
個人情報	
名: 	
姓: 	
メールアドレス: 	
パーミッション	
☐ スタッフ権限 ユーザが管理サイトにログイン可能かどうかを示します。	
☒ 有効 ユーザがアクティブかどうかを示します。アカウントを消す代わりに選択を解除してください。	
☐ スーパーユーザー権限 全ての権限を持っているとみなされます。	

7.2 管理者アカウントのパスワード変更

管理者アカウントのパスワードは次の手順で変更します。

1. Unicorn IDM の管理画面にアクセスし、管理者ユーザーでログインします。

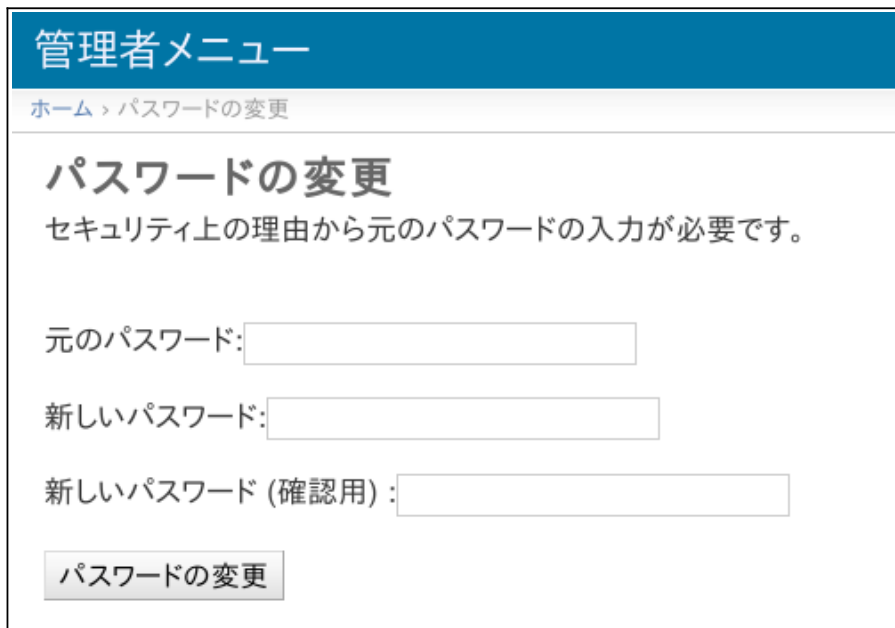
<https://unicornsv.example.com/unicornIDM/admin/>

2. 画面右上部の「パスワード変更」をクリックします。



The screenshot shows the administrator menu. At the top, there is a blue header with the text '管理者メニュー' (Administrator Menu) on the left and 'ようこそ admin. パスワードの変更 ログアウト' (Welcome admin. Change Password Logout) on the right. Below the header, there is a section titled 'サイト管理' (Site Management). Under 'サイト管理', there is a table with two columns: 'Auth' and '操作' (Action). The 'Auth' column has two rows: 'グループ' (Group) and 'ユーザ' (User). The '操作' column has two rows: '追加' (Add) and '変更' (Change). The 'パスワードの変更' (Change Password) link is highlighted in red in the top right corner of the menu.

3. 「元のパスワード」と「新しいパスワード」を入力し、「パスワードの変更」をクリックします。



The screenshot shows the 'パスワードの変更' (Change Password) form. The form has a blue header with the text '管理者メニュー' (Administrator Menu). Below the header, there is a breadcrumb trail: 'ホーム > パスワードの変更' (Home > Change Password). The main title of the form is 'パスワードの変更' (Change Password). Below the title, there is a message: 'セキュリティ上の理由から元のパスワードの入力が必要です。' (For security reasons, you must enter the original password). The form contains three input fields: '元のパスワード:' (Original Password:), '新しいパスワード:' (New Password:), and '新しいパスワード (確認用):' (New Password (Confirmation:)). Below the input fields, there is a button labeled 'パスワードの変更' (Change Password).

4. 以上で完了です。

8. システム関連情報

本章では、Unicorn IDM のシステム関連情報について説明します。

8.1 関連ファイル一覧

Unicorn IDM に関連するファイルは、以下に配置されています。

ファイル	内容
/opt/osstech/lib/unicornIDM	システムのプログラム一式
/opt/osstech/var/lib/unicornIDM/unicornIDM.db	システムの設定パラメーターなど
/opt/osstech/var/lib/unicornIDM/uploads/	アップロードした CSV ファイル
/opt/osstech/var/lib/unicornIDM/results/	各操作ごとの操作結果
/opt/osstech/var/lib/unicornIDM/summary/	操作結果のサマリ情報
/opt/osstech/var/log/unicornIDM/	システムのログ情報

8.2 設定のバックアップ

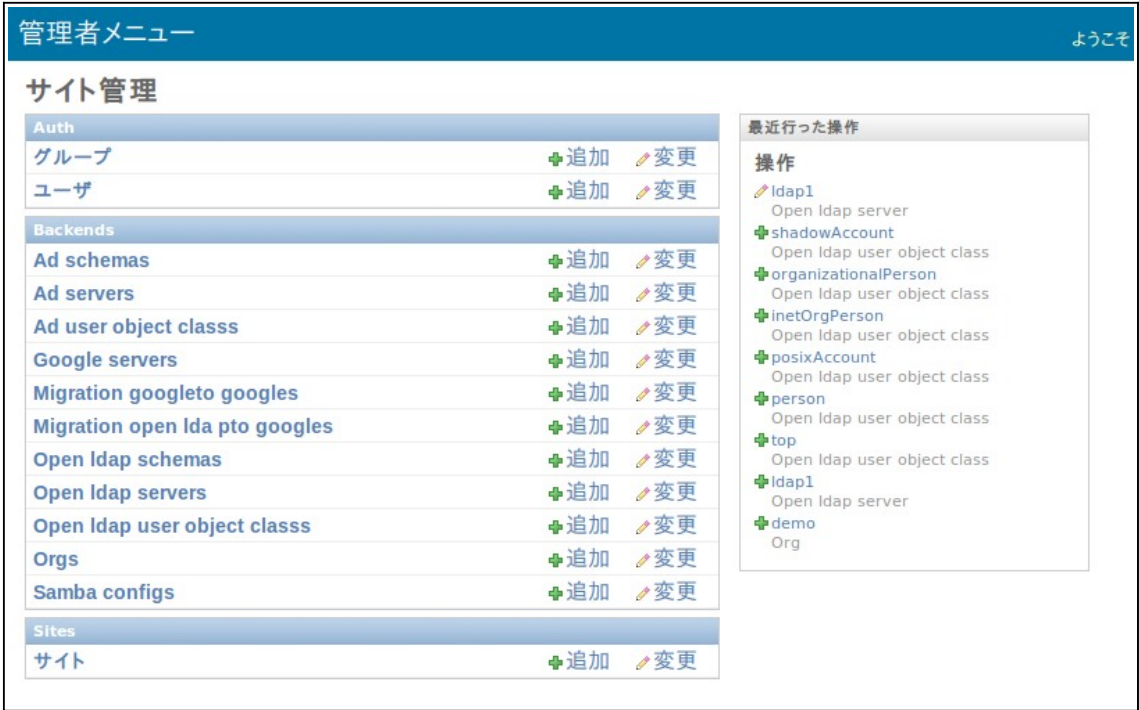
Unicorn IDM の設定をバックアップする場合は、以下のファイルを保存してください。

ファイル	内容
/opt/osstech/var/lib/unicornIDM/unicornIDM.db	システムの設定パラメーターなど
/etc/httpd/conf.d/unicornIDM.conf	Apache 用設定ファイル

9. 注意点

9.1 サイトについて

管理者メニューに「サイト」という項目があり、ここにデフォルトで「example.com」というサイトが登録されています。



管理者メニュー ようこそ

サイト管理

Auth	
グループ	追加 変更
ユーザ	追加 変更

Backends

Ad schemas	追加 変更
Ad servers	追加 変更
Ad user object classes	追加 変更
Google servers	追加 変更
Migration googlet to googles	追加 変更
Migration open Ida pto googles	追加 変更
Open Idap schemas	追加 変更
Open Idap servers	追加 変更
Open Idap user object classes	追加 変更
Orgs	追加 変更
Samba configs	追加 変更

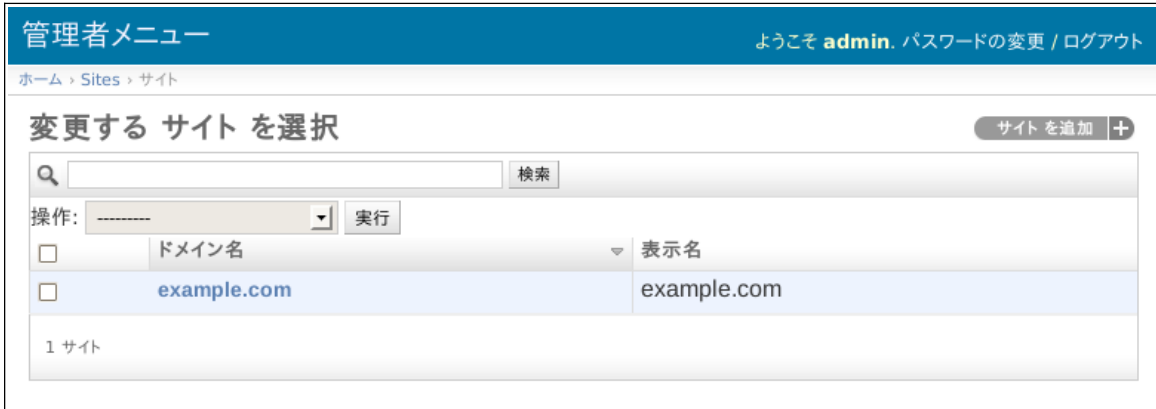
Sites

サイト	追加 変更
-----	---------------------------------------

最近行った操作

操作

- Idap1
Open Idap server
- shadowAccount
Open Idap user object class
- organizationalPerson
Open Idap user object class
- inetOrgPerson
Open Idap user object class
- posixAccount
Open Idap user object class
- person
Open Idap user object class
- top
Open Idap user object class
- Idap1
Open Idap server
- demo
Org



管理者メニュー ようこそ **admin.** パスワードの変更 / ログアウト

ホーム > Sites > サイト

変更する サイト を選択 [サイトを追加](#) [+](#)

検索

操作: ----- [実行](#)

☐	ドメイン名	表示名
☐	example.com	example.com

1 サイト

このサイトの設定は、Unicorn IDM の内部で使用しているライブラリの仕様上、必ず一つは必要になります。そのため、「example.com」の設定を削除しないようご注意ください。

10. 改版履歴

- 2011 年 5 月 17 日
 - Unicorn ID Manager 最新版対応