Obidos Administration Guide

https://spenego.com

Chapter 1

Administrators

There are two types of accounts in Obidos. One is administrative accounts and the other is user accounts. An administrator account is used to manage Obidos. This includes managing administrative accounts, managing user accounts, setting up preferences, managing license, managing audits, etc. An Administrator (herienafter referred to as admin) cannot store digital artifacts in Obidos. An admin cannot assume the role of a user and a user cannot assume the role of an admin. All admin accounts are local accounts. This means those accounts are maintained within Obidos. Local accounts will have their passwords set according to the password policy in Obidos.

Obidos has a built-in admin account 'admin'. The password for this account is set at the time of installation. Using this 'admin' account additional admin accounts can be created. The built-in 'admin' account inherits every capability that is possible for an administrative account. Such an account is referred to as a 'root admin'. The 'admin' account can be used to create other root admin accounts or less capable admin accounts. If your institutional security policiy requires renaming the default 'admin' account, that can be done at the time of installation. Admin account operations are described in the sections to follow.

1.1 License and number of users

Obidos license is based on number of users. Only the count of active regular user accounts is considered for license units. Admin accounts do not count towards license. So if there are 112 active regular user accounts and 7 admin accounts, only the 112 user accounts are counted for license units. Once the active number of regular users reach the license limit, no new users can be added by admins.

1.2 Create Administrators

To create an admin account, log into Obidos using the 'admin' account (or another admin account). From the "Admin Accounts" top navigation menu, select "Create New Admin". The password assigned to this admin account during the account creation process is a temporary password. The admin user will have to change the password when logging into Obidos for the first time.

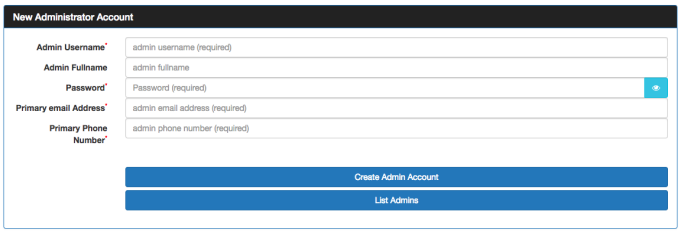

Figure 1.1: Create New Admin Account

1.3 List Administrators

Log into Obidos using an admin account. From the ”Admin Accounts” top navigation menu, select ”List Admins”.

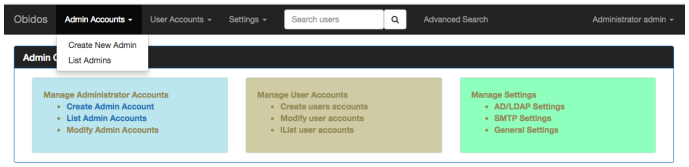

Figure 1.2: Admin Accounts Menu

1.4 Edit Administrator

If the Fullname, Primary email, Primary phone number, or password has to be changed, it can be done by editing the profile. To get to the ”Edit” task, first the admins must be listed. This can be done by selecting ”List Admins” from the ”Admin Accounts” top navigation menu. From the list of admins, click on the ”Edit” button. This will open up an edit window.

1.5 Delete Administrator

Accounts can only be ’tombstoned’. They cannot be deleted. Only a root admin account can be used to tombstone another administrator account. The built-in ’admin’ account cannot be deleted. Once an admin account is tombstoned, the whole profile associated with that account will be frozen. To get to the ”Tombstone” task, first the admins must be listed. This can be done by selecting ”List Admins” from the ”Admin Accounts” top navigation menu. From the list of admins, select the admin(s) of interest click on ”Tombstone” button. A confirmation pop-up window will show up. Select ”Yes” to confirm or ”No” to cancel.

Chapter 2

Users

An administrator (hereinafter referred to as admin) has to create/manage users in Obidos. A user cannot assume the role of an admin. Similarly an admin cannot assume the role of a user. Users can store digital artifacts in Obidos. Users must be explicitly granted permission by admin to manage Global Templates.

Users can be set up with single signon to corporate directory service (Active Directory or LDAP). In such cases users can log into Obidos with their corporate username and password. These users must have username registered in Obidos exactly as it appears in corporate Directory Service. Since such accounts are meant to be single signon, the passwords are not set in Obidos; rather these accounts are authenticated against the corporate Directory Service.

Users created with authentication done by Obidos are referred to as local accounts. All admin accounts are local accounts. You can create local accounts for users. Passwords for local accounts will follow the password policy in Obidos.

All types of active user accounts (local and maintained in corporate directory) are counted towards license limit.

2.1 Create A User Account

To create a user account, select ”Create New User” item from the top ”User Accounts” menu.

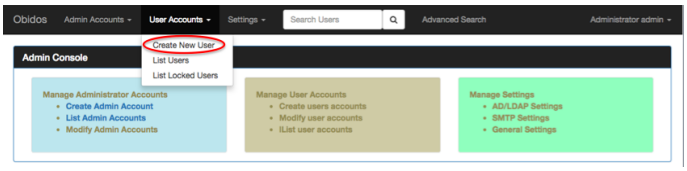

Figure 2.1: Create New User

The admin has to fill in the details for the user.

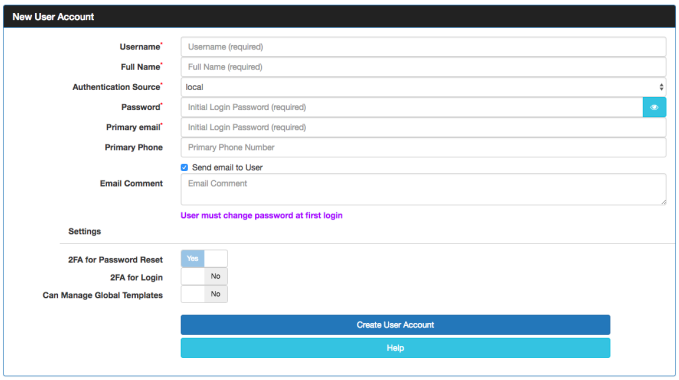

Figure 2.2: New User Details

2.2 Bulk Importing Users

Large number of users can be imported to Obidos from command line as user **obidosadmin**. The user attributes must be defined in a file in LDIF format. The following attributes are required in the LDIF file:

Attribute	Maps to
cn	Full name
mail	Email address
sAMAccountName	username
password	For local Obidos users only

Before importing users, the following steps must be taken into account:

- Make sure to dump the Obidos mariadb database in case something goes wrong.
- Make sure to configure SMTP setting in Obidos. By default, the initial password will be included in the notification email sent to the users.
- Make sure to configure AD/LDAP settings in Obidos if the users will be imported from Active Directory or LDAP.

2.2.1 Bulk Exporting and Importing Users from Active Directory

The following are the steps to import users from Active Directory using ldif.

1. Export users from AD using ldifde command on Windows.
2. Upload the ldif file to Obidos server using the 'obidosadmin' account.
3. Run the import_users command to create accounts in Obidos.

2.2.1.1 Export Users from Active Directory

Use the tool ldifde to export users. Example:

```
ldifde.exe -f adusers.ldif
```

A sample LDIF file is shown below.

```
dn: cn=Lloyd Kerluke
cn: Lloyd Kerluke
mail: lloyedka@example.com
sAMAccountName: lloydk

dn: cn=Marvin Cummerata
cn: Marvin Cummerata
mail: marvinc@example.com
sAMAccountName: marvinc

dn: cn=Annita Senger DC
cn: Annita Senger DC
mail: annitas@example.com
sAMAccountName: annitas
```

2.2.1.2 Upload the ldif file adusers.ldif to Obidos server

Log in to the Obidos system using *ssh* (or the web console) as the user **obidosadmin**. The default password is **obidosadmin**. The password must be changed at the very first login. It is a good idea to save the password in Obidos. Once the password has been changed for the obidosadmin user, use any sftp program (or web console) to upload the adusers.ldif file to the Obidos server.

2.2.1.3 Import users from adusers.ldif

Be logged in to the Obidos server using *ssh* or web console as **obidosadmin**. To see the usage of the import users program, run the following command:

```
$ import_users --help
usage: ImportUsers
    --ldapConfigName <ldapConfigName>   AD/LDAP Config name. Find it out
                                        from Settings > List AD/DLAP
                                        Settings. Requires for adding
                                        AD/LDAP users.
    --ldifFile <ldifFile>               LDIF file. Required.
    --noEmail                           Don't send initial password in
                                        notification email
    --requiers2FA                       2FA requires for password and
                                        passphrase reset
```

```
    --uidAttr <uidAttr>                uid attribute. The default is
                                       sAMAccountName
```

- To import AD/LDAP users into Obidos, type:

```
$ import_users \
    --ldapConfigName "AD Config Name" \
    --ldifFile adusers.ldif
```

Note: "AD Config Name" is the AD/LDAP configuration that you set up as administrator in Obidos. A notification email will be sent to the user. The users imported this way can log into Obidos using their username and AD password.

2.2.2 Creating multiple local Obidos users from ldif

If you just want to create multiple local Obidos users from an LDIF file:

1. Create an ldif file with password field.
2. Upload the file to Obidos server as the user obidosadmin.
3. Run the import_users command.

2.2.2.1 Create an LDIF file with the users.

Use your favorite text editor to create the LDIF file. A sample LDIF file "localusers.ldif" with password is shown below.

```
dn: cn=Lloyd Kerluke
cn: Lloyd Kerluke
mail: lloyedka@example.com
password: test
sAMAccountName: lloydk

dn: cn=Marvin Cummerata
cn: Marvin Cummerata
mail: marvinc@example.com
password: test
sAMAccountName: marvinc

dn: cn=Annita Senger DC
cn: Annita Senger DC
mail: annitas@example.com
password: test
sAMAccountName: annitas
```

If the LDIF file does not have the **password** attribute, a random password will be generated when the account is created in Obidos and will be included in the notification email sent to the users. The users will be prompted to change the password at the first login to Obidos.

2.2.2.2 Upload the ldif file to Obidos server.

Using the obidosadmin account, upload the file ”localusers.ldif” to the Obidos server.

2.2.2.3 Import ldif users.

Run the command ’import_users’ on the Obidos server after logging in (via ssh or web console) as the user ’obidosadmin’.

```
$ import_users \
    --ldifFile localusers.ldif
```

The user will be prompted to change the password at the first login to Obidos application.

2.3 List User Accounts

In order to get the list of users, select ”List Users” from top level ”User Accounts” menu.

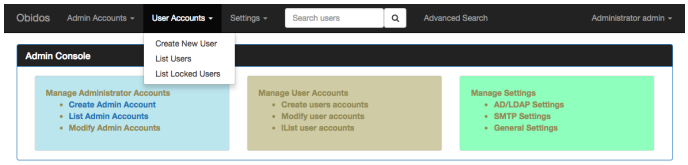

Figure 2.3: List User Menu

The list of users will be displayed similar to the following figure.

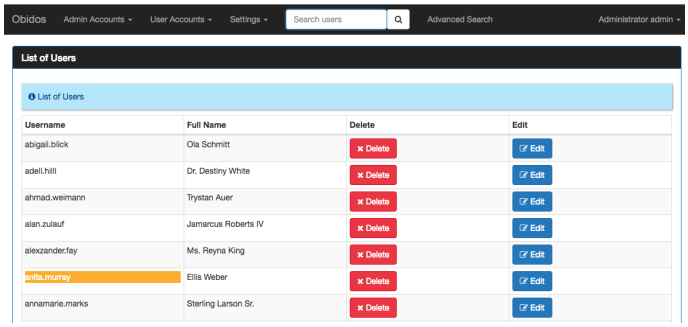

Figure 2.4: List of Users

2.4 Reset User Password

This action is allowed only for local accounts. In the Edit User screen, there is option to reset password.

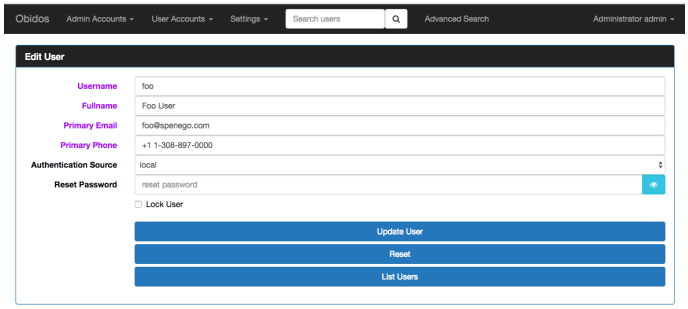

Figure 2.5: Reset Password

2.5 Lock a User Account

This can be done from the screen for editing a user. To do that, first select ”List Users” from top level ”User Accounts” menu. From the list of users, click ”Edit” button on the line corresponding to the user

in the list. When the edit menu shows up, there is a selection to Lock the user. See the following figure.

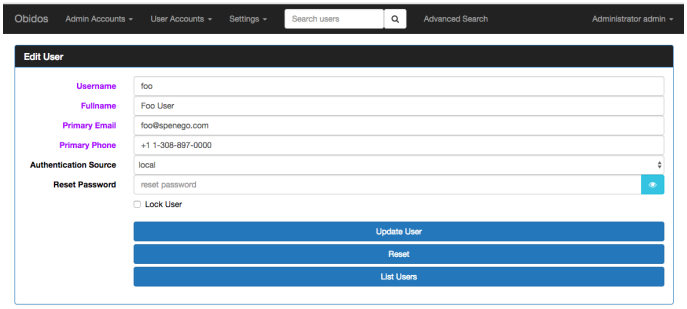

Figure 2.6: Lock User

2.6 Unlock a User Account

Unlocking a User Account can be done only from the screen for editing a user account. It is easy to the edit screen from the list of locked users. The list of locked users can be obtained by selecting ”List Locked Users” from top level ”User Accounts” menu. From the list of users, click ”Edit” button on the line corresponding to the user in the list. When the edit menu shows up, there is a selection to Unlock the user. See the following figure.

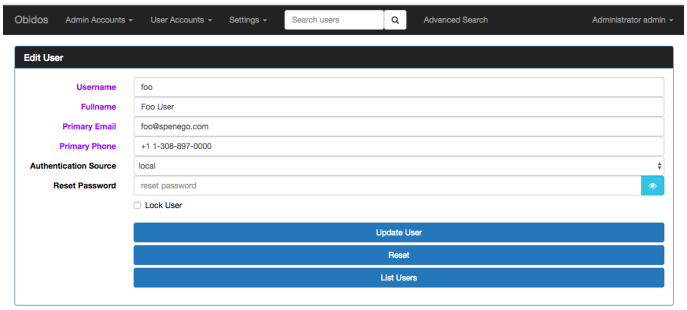

Figure 2.7: Unlock User

2.7 Tombstone a User Account

Accounts can only be ’tombstoned’. They cannot be deleted. To get to the ”Tombstone” task, first the users must be listed. This can be done by selecting ”Manage Users” from the ”Users” top navigation menu. From the list of users, select the users of interest and click on ”Tombstone” button. A confirmation pop-up window will show up. Select ”Yes” to confirm or ”No” to cancel.

Chapter 3

Password Strength

The password strength is determined by calculating entropy of the password. An entropy is described in terms of bits. The higher the bits in entropy the stronger the password will be. An entropy indicates how hard it will be to crack the password by brute-force. In password strength calculation, the entropy is not the same entropy as described in information theory. Rather the raw entropy is lowered by using various password cracking techniques before accepting.

3.1 Entropy Calculation

This section describes the basics of entropy calculation. Please note that we do not calculate password or passphrase entropy this way, rather we use various password cracking techniques to lower the raw entropy and if the entropy is higher or equal to the configured entropy, only then the password is accepted.

If the password length is L and the password can be chosen from N number of characters, the possible number of passwords will be N^L. To calculate the raw entropy H in that character space, the H has to be a number so that $2^H = N^L$. Therefore, the entropy calculation formula can be derived as follows:

$$2^H = N^L \tag{3.1}$$

$$\log(2^H) = \log(N^L) \tag{3.2}$$

$$H \times \log(2) = L \times \log(N) \tag{3.3}$$

$$H = L \times \frac{\log(N)}{\log(2)} \tag{3.4}$$

$$= L \times \log_2(N) \tag{3.5}$$

Given a password entropy H and the number to guess a password per second is (gps), the time in seconds T_s to brute force a password can be calculated with the following formula:

[1] $\log_b(x^p) = p \log_b(x)$

[2] $\log_b(x) = \frac{\log(x)}{\log(b)}$

$$T_s = \frac{2^H}{gps}$$

The following xkcd comic illustrates entropy calculation of password in a different way.

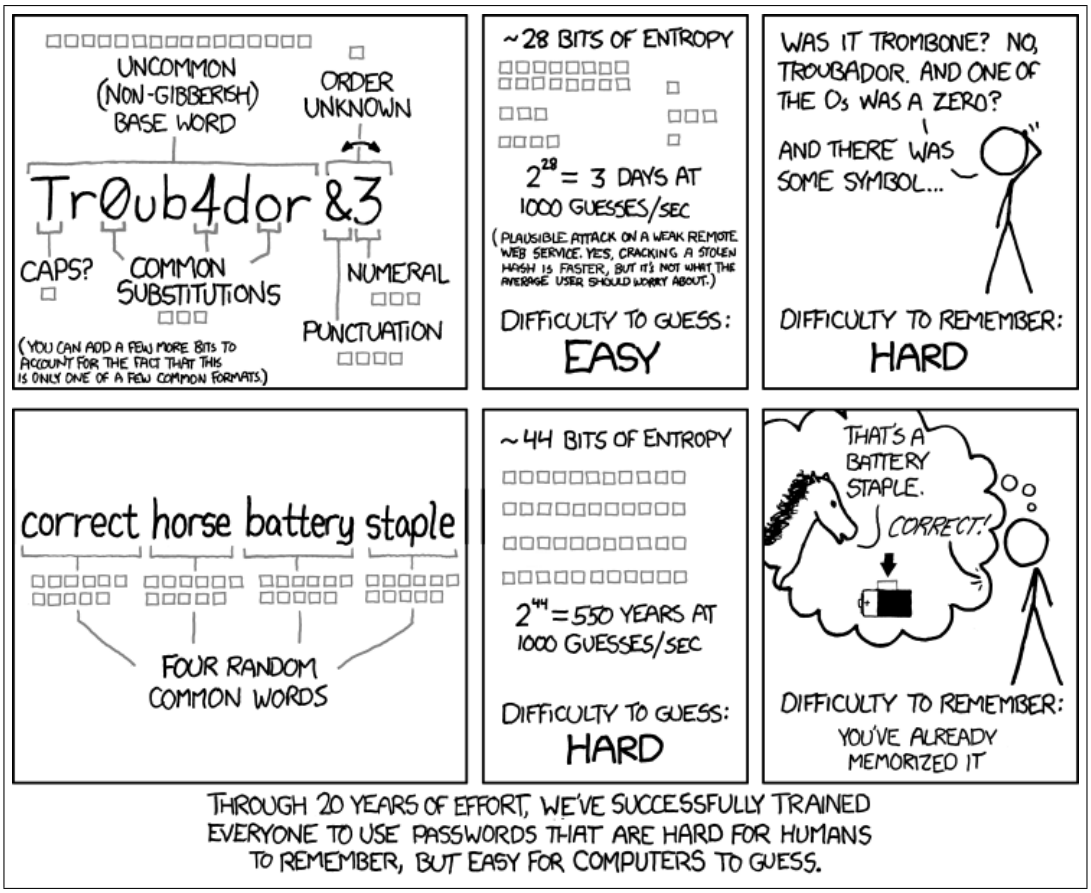

Figure 3.1: xkcd comic for password strength

Let's calculate the entropy of `Tr0ub4dor&3` with our formula $H = L \times \log_2(N)$. The password has upper case, lower case, numbers and a special character in it. There are 26 upper case, 26 lower case, 10 numbers and 32 special characters (including space) in English keyboard and the length L of the password is 11.

$$N = 26 + 26 + 10 + 32 = 94$$
$$H = 11 \times \frac{\log(94)}{\log(2)} = 72.10047736845401109442 \approx 72$$

Assuming that the attacker knows the length of the password L and character space N, if $gps = 1000$, it will take $\frac{2^{72}}{1000} \approx 150\ billion$ years to crack the password. If $gps = 350\ billion$, it will take ≈ 428 years

to crack the password. if $gps = 1\ trillion$, it will take $\approx 150\ years$ to crack the password. So if brute force is used, it is really a good password, even with the most powerful computer, it will take a long time to crack.

According to xkcd, the password is not strong, lets see how xkcd calculates the entropy. Each of the tiny square box in the comic indicates a bit.

- The 16 bits implies that the word `Troubador` is chosen from a dictionary with 65536 words ($2^{16} = 65536$).
- Make the first letter upper case, there is only $1\ bit$.
- Two characters were substituted $o \rightarrow 0$, $a \rightarrow 4$ and o was not substituted, therefore $3bits$ of information.
- The string `&3` was appended at the end. The order is unknown, therefore $1\ bit$
- There are 32 special characters (including space) in English keyboard, therefore the entropy should be $1 \times \frac{\log(32)}{\log(2)} = 5$. For some reason $4bit$ was selected.

Therefore, the entropy of `Tr0ub4dor&3` is $16+1+3+1+4+3 = 28$, which much is lower than 72 and makes it a bad password, because the attacker might follow the similar technique than brute-forcing it.

3.2 Entropy calculation in Obidos

The technique we used in Obidos, the entropy for the password `Tr0ub4dor&3` comes down to 19.625. we used similar techniques used the ruby gem strong_password

1. Calculate entropy according to NIST Special Publication 800-63 Version 1.0.2 Appending A.2.1
   - The first character gets 4 bits
   - The next 7 characters get 2 bits/character
   - The next 12 characters (9-20) get 1.5 bits/character
   - Any character beyond 20 gets 1 bit/character
   - If there are mixed case and special character, give 6 bits bonus

   Using these rules, the entropy of `Tr0ub4dor&3` comes down to 26.125
2. Calculate the entropy by lowering the case, which is also 26.125
3. Adjust entropy by checking if the password has any pattern of Qwerty keyboard (e.g. zxcvbn, qwertyuiop etc.) which is 26.125
4. Adjust the entropy by looking at dictionary, doing normal substitutions like xkcd, checking for leet speak pattern etc. The entropy comes down to 19.625.

5. Finally select the lowest entropy, which is 19.625

The entropy of `correcthorsebatterystaple` comes down to 30.953125 which is much lower than xkcd's 44 bit entropy.

3.3 Suggestions for strong passwords

Please think passphrase when picking a password. Passphrases are longer and easier to remember than a cryptic random password which is difficult to remember. The longer the password is, the stronger it will be. Refer to the equation (3.5).

- Think passphrase. The longer, the better! Avoid using repeating characters
- Use a line from a poem or a song and mix with Upper, lower case letters and numbers
- Use uncommon words. Capitalization does not help much
- Add typos, space, special characters # $ % ~ ^ & etc. here and there. If the password is a long passphrase, there is no requirement to use any special character. However, your organization might have a password policy that requires them.
- Do not use username, email, phone numbers etc.

3.4 Password storage

A password is never stored in the disk, rather a memory-hardened, brute- force resisting key is derived from the given password and a stored salt. To verify a password, the same key is derived from the password and the salt and compared. The function deriving the key from the password and the salt is CPU intensive and intentionally requires a fair amount of memory. Therefore, it mitigates brute-force attacks by requiring a significant effort to verify each password.

The password is hashed using Argon2id algorithm.

Chapter 4

Active Directory/LDAP Configuration

In order to facilitate single signon for users, the details of the directory service must be registered with Obidos. This can be Active Directory or LDAP. More than one Configuration can be stored in Obidos.

4.1 New AD/LDAP Configuration

In order to create a new Configuration, select ”Create AD/LDAP Settings” from the top level ”Settings” menu.

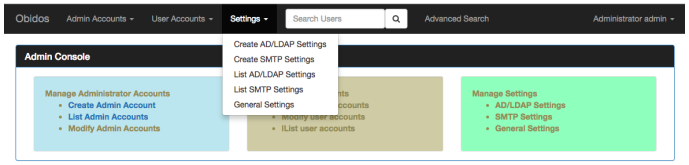

Figure 4.1: Menu for new AD/LDAP Configuration

The resulting screen to input the fields for a Configuration are as shown in the following figure.

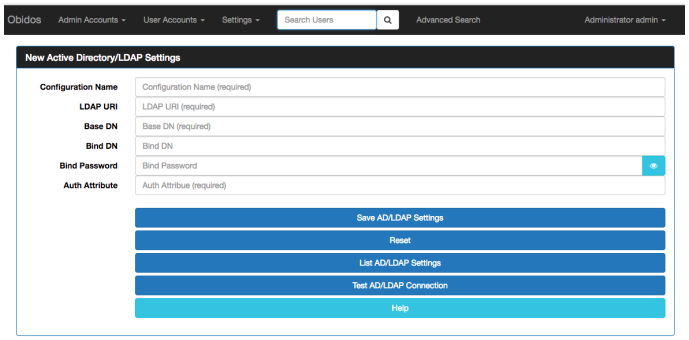

Figure 4.2: Fields for Directory Service

The Configuration Name is the identifier for the Configuration. This will be used to identify the Directory service for single signon when a user account is created.

The LDAP URI field is usually of the form ldap://<hostname >:<port >.
An example is ldap://spenego.com:389, where 389 is the port for the LDAP server.

Chapter 5

SMTP Configuration

Obidos uses the SMTP configurations for sending email to users for various purposes. For example, the admin can chose to send email confirmation for new user account. When a user shares an Item with another user, an email is sent to the beneficiary. In order to send emails, Obidos needs information about the SMTP server. Only one SMTP Configuration can be created per Obidos instance.

5.1 Create New SMTP Configuration

From the top level ”Settings” menu select ”Create SMTP Settings”.

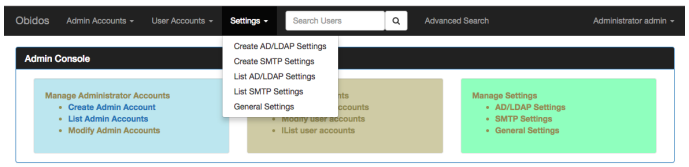

Figure 5.1: Create New SMTP Configuration

The fields of the Configuration are as shown in the following figure.

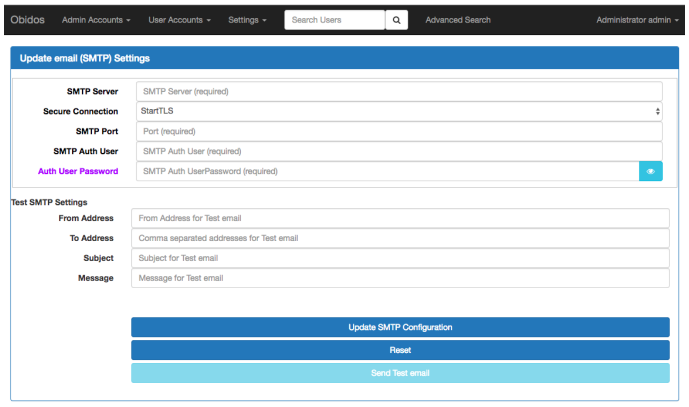

Figure 5.2: SMTP Configuration Fields

The SMTP Server field is the fully qualified hostname of the server.

The ”Secure Connection” field can be StartTLS or SSL or ’Not Secure’.

SMTP Port is the TCP/IP port on which the mail server (MTA) is listening for incoming connections. Traditionally, for Non-secure connections this is 25. Implicit encrypted (i.e., SSL or TLS) SMTP uses port 465. StartTLS popularly uses port 587.

SMTP Auth User is the account using which authentication is done to the mail server.

The password for this account should be provided in the field ”Auth User Password”.

5.2 List SMTP Configuration

From the top level ”Settings” menu select ”List SMTP Settings”.

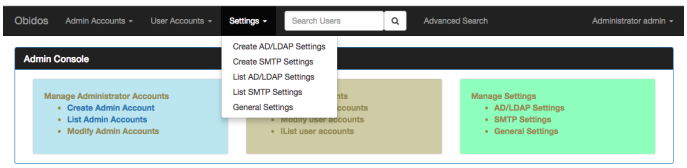

Figure 5.3: List SMTP Configuration

5.3 Edit SMTP Configuration

From the top level ”Settings” menu select ”List SMTP Settings”. The result will be as shown in the following figure.

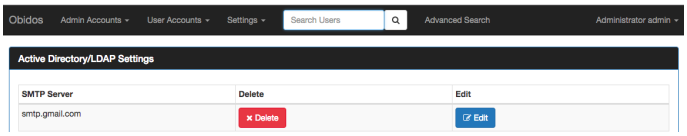

Figure 5.4: Edit SMTP Configuration

Click on the ”Edit” button and the screen will show the existing details.