

LDAP Integration

sipXecs supports integration with LDAP-enabled directory services. This allows administrators to centrally manage user information including credentials across several applications and including sipXecs.

This page provides implementation details, usage scenarios and instructions on how to use this feature.

- [Configuring the LDAP Server in sipXconfig](#)
 - [The Setup](#)
- [Usage Scenarios](#)
 - [Switching a running system to LDAP](#)
 - [Scheduled Import](#)
 - [Triggered Import](#)
- [LDAP Field Mapping](#)
- [Ldap Authentication](#)
- [Synchronization Schedule](#)
- [Management Settings](#)
- [Users/EditUser Pages](#)
- [Error Reporting](#)
- [Assumptions & Limitations](#)
- [Assigning Multiple Values to User Aliases from AD](#)
- [Further Reading](#)
- [LDAP Clients that can be used to manipulate LDAP directories](#)

Configuring the LDAP Server in sipXconfig

First, navigate to the LDAP / AD screen found under the System tab.

The screenshot shows the 'LDAP Configuration' screen in the sipXecs web interface. The top navigation bar includes 'Users', 'Devices', 'Features', 'System', and 'Diagnostics'. The main content area contains a form with the following fields and options:

- Host:** A text input field containing 'localhost'. Below it is the text: 'IP address or the name of the host on which LDAP server is running.'
- Domain:** A text input field. Below it is the text: 'Specify LDAP Domain.'
- Use TLS:** A checkbox that is currently unchecked. Below it is the text: 'Enable SSL/TLS connections to your LDAP server, default port is usually 636.'
- Port:** A text input field. Below it is the text: 'Port number on which LDAP server is listening for requests. The default port used is 389 or, for a SSL/TLS connection is 636.'
- User:** A text input field. Below it is the text: 'Distinguished Name of the user to bind to LDAP directory. Leave empty for anonymous access.'
- Password:** A text input field.
- Confirm Password:** A text input field. Below it is the text: 'Password for simple authentication.'

At the bottom of the form are 'Apply' and 'Continue' buttons. On the right side of the form, there are links for 'Add LDAP Connection' and 'Remove LDAP Connection'. A 'Quick Links' section on the right includes a link for 'Certificates' and a section for 'Active Directory' with the text: 'It is possible to synchronize user credentials with Microsoft Active Directory using the LDAP interface.'

The user has the option to add one or more LDAP connection(s). Imports can be scheduled independently for each LDAP connection. Also mappings can be done independently for each LDAP connection

The Setup

- **Select LDAP Server** Contains configured LDAP connections
- **LDAP server address** in the form of an IP address, the DNS name and optionally the port number
- **Domain** this specifies the users domain. This value is saved as a user setting and used for authentication (users can use aaa@domain or domain\aaa for authentication)
- **Use TLS:** Enable SSL/TLS connections to your LDAP server. You should import LDAP server certificate for enabling SSL/TLS connections
- **Port:** Port number on which LDAP server is listening for requests. The default port used is 389 or, for a SSL/TLS connection is 636
- **Distinguished name of a directory sub-tree that contains user information:** sipXconfig supports various user-tree organizations as long as all user-trees can be accessed from a single root
- **LDAP attributes to sipXconfig field mapping:** See [LDAP Field Mapping](#) below
- **User's group name:** This is the group that will contain all users imported from the LDAP server
- **Optionally LDAP credentials:** sipXconfig needs read-only access to the LDAP directory. If such access requires authorization, the administrator has to configure appropriate credentials

Configuration
Import
Management Settings

Select LDAP Server: **ldap://192.168.7.103:389**
Select LDAP connection to configure

[Add LDAP Connection](#) [Remove LDAP Connection](#)

Host: 192.168.7.103
IP address or the name of the host on which LDAP server is running.

Domain:
Specify LDAP Domain

Use TLS:
Enable SSL/TLS connections to your LDAP server, default port is usually 636

Port:
Port number on which LDAP server is listening for requests. The default port used is 389 or, for a SSL/TLS connection is 636

User:
Distinguished Name of the user to bind to LDAP directory. Leave empty for anonymous access.

Password:
Confirm Password:
Password for simple authentication.

Quick Links
[Certificates](#)

LDAP server needs to be running and be accessible in order to proceed. If LDAP server requires authentication for read-only access, enter User name and Password for basic authentication. **Import LDAP server certificate for enabling SSL/TLS connections**

Press Continue to proceed to LDAP attribute mapping configuration screen.

Active Directory
It is possible to synchronize user credentials with Microsoft Active Directory using the LDAP interface.

sipXecs (4.6.0.1430.ef2c0.2013-06-28EEST17:06:25 mircea.ezuce.ro) update 6
Copyright (C) 2013 SIPfoundry. Licensed under AGPL v3

Usage Scenarios

Configuration
Import
Settings

Enable periodic import from LDAP

Every Day

Quick Links
[Job Status](#)

Press Preview to verify LDAP import configuration. If LDAP Server connection parameters and attribute mapping are configured properly you will see an example of imported user.

Press Import to initiate importing users from LDAP. Go to Job Status page to monitor the status of the import operation.

Switching a running system to LDAP

During installation of sipXconfig the administrator configures the LDAP server from which sipXecs will import data. The initial import is initiated on demand from the sipXconfig UI. Users are imported and the administrator can proceed to configure the remaining part of the system.

Scheduled Import

In a running sipXecs system sipXconfig already contains a list of users. The easiest way for the administrator to initiate synchronization with an LDAP server is to create a new user group that contains all the users that will be synchronized with the LDAP server. The administrator then configures the LDAP server address and triggers an import. All users in the specified group are updated, new users are added, and users that are in the group but not in LDAP server are removed.

Triggered Import

Automatically scheduled import is performed periodically. Newly added LDAP entries are imported as new sipXconfig users. If any entries were deleted since the last import, sipXconfig will delete those users. If any entries were modified, sipXconfig user data is modified accordingly.

A 3rd party application is used to perform LDAP updates. The SOAP API is used to trigger LDAP import each time the LDAP directory is changed.

LDAP Field Mapping

Please find below some of the mapping attributes, including Alias multi-selection attribute widget. Among others we can enumerate caller id or address attributes

Configuration

Import

Management Settings

Search base: (Default: dc=example,dc=com)

The root of the LDAP entities subtree that will be searched for users.

User object class:

LDAP class that will be used to filter entries corresponding to users. Entries that do not have this class are disregarded during search.

Filter:

Optional filter expression for example 'surname@first'. Only entries selected by this filter will be considered when importing users. You can specify compound filter expression using & and | operators.

User ID attribute:

LDAP attribute representing user ID. Its value needs to be unique. Should be set to user's Extension.

First name attribute:

The user's first name

Last name attribute:

The user's last name

Available

- businessCategory
- carLicense
- cn
- departmentNumber
- destinationIndicator
- displayName
- employeeNumber
- employeeType
- facsimileTelephoneNumber
- givenName

→ ← ↑ ↓

select deselect move up move down

Selected

- audio
- description

If this attribute has more than one value a separate alias will be created for each value of this attribute.

E-Mail attribute:

Used for voicemail notification. If voicemail is not installed or available on this system, email address will not be imported.

User group attribute:

If this attribute has more than one value an imported user will be added to multiple groups. Groups will be created if necessary.

Password:

User password. If no mapping attribute is configured for password, all imported users will be assigned default PIN specified here. This is the same default value for both password and Voicemail PIN.

Voicemail PIN:

User Voicemail PIN. If no mapping attribute is configured for Voicemail PIN, all imported users will be assigned default PIN specified here. This is the same default value for both password and Voicemail PIN.

Default PIN:

Confirm Default PIN:

SIP password attribute:

If no mapping attribute is configured for SIP password, this system will automatically generate random SIP password for each imported user. If you could do this you would need to generate a new phone profile every time this is changed.

IM ID:

The instant message id. A new user with this user name will be created at messaging server level.

Quick Links

[Certificates](#)

During LDAP operation LDAP attributes will be used to create or update user information.

This page allows for associating LDAP attributes with users properties. For example if you choose attribute sn as the Last name attribute the value of sn will be used to create Last name for an imported user.

Press Continue to check the example user imported from LDAP with newly configured attribute mapping.

Active Directory

It is possible to synchronize user credentials with Microsoft Active Directory using the LDAP interface.

sipXconfig Field	LDAP Attribute	Description
user id	ipPhone	An unique user identification. Use 'uid' for other ldap servers but Active Directory. The administrator can use the user's extension (e.g. 1245) as a user id or more readable identifiers, similar to the user part of an e-mail address (e.g. johndoe, john.doe etc.). A single attribute should be mapped to this field. Changing the value of LDAP attribute mapped to the user id field will be interpreted by sipXconfig as removal followed by an addition of a new user. This is the only mandatory mapping.
firstname	givenName	User's first (given) name. This is an optional mapping.
lastname	sn	User's last name. This is an optional mapping.
aliases		Multiple attributes (possibly multi-value attributes) can be mapped to this field. Since sipXconfig requires that all aliases are unique, it will drop any values that are not unique. If non-numeric user ids are configured, administrators may want to add conventional phone (extension) number as one of the aliases. This is an optional mapping. Use 'telephoneNumber' for other ldap servers but Active Directory. For Active Directory use 'sAMAccountName'. There is a Multi Selection widget and you have the option to combine multiple single value and multi-value attributes
Voicemail PIN		Secret used by users to access voice mail. Also used by sipXconfig user portal to access call forwarding, PIN change and other user related functionality. This is an optional mapping. If this field is not mapped, sipXconfig will allow administrators to configure the initial value of PIN. After deployment users will be asked to change PIN using Telephone UI or sipXconfig UI. Subsequent imports will preserve the value of this field.
SIP password		The password used by phones to register with sipXecs. The administrator has the option to: a) map this field to the LDAP attribute; b) set the initial value for all the fields; or c) let sipXconfig randomly generate a value. The last strategy works best if phones, as well as users, are managed by sipXconfig. In this case phones will be automatically configured with randomly generated passwords providing strong security. If the SIP password was randomly generated or preset by the administrator its value will be preserved during subsequent LDAP imports.
Group		Multi-value attribute containing user group name. This is an optional mapping. In addition to groups created by this attribute mapping, sipXconfig will require that administrators provide the name of the group that would contain all imported users.
Contact Information		Job, Office Address, Home Address and other contact information fields are mapped

Ldap Authentication

sipXconfig supports different authentication scenarios including LDAP. The administrator has the option to activate a desired authentication scenario here: menu System, page LDAP/AD and tab Settings as shown in the following picture:

Configuration
Import
Settings

Instant Messaging Authentication

By enabling this feature, the Openfire instant messaging server will validate each user's passwords with the LDAP server configured for this system. The instant messaging server will also update user details displayed to IM clients from the LDAP server directly. IM clients will see the latest contact information without having to wait for the next LDAP import.

Authentication Options: **No LDAP**

Depending on the selected option, the user portal will validate the user PIN or LDAP username and password with the LDAP server configured for this system. This feature does not affect voicemail access from a phone, that remains the user's PIN.

Apply

- Instant Messaging Authentication when enabled, the Openfire instant messaging server will validate each user's passwords with the LDAP server configured for this system
- Authentication Options contains three possible choices:
 - No LDAP, meaning that only User authentication is verified (Credentials entered in the login form will be interpreted only as User/PIN combination and verified against sipXconfig database)
 - LDAP Only, meaning that only LDAP authentication is verified (Credentials entered in the login form will be interpreted only as LDAP user /password combination and verified against configured LDAP(s) server(s) for the system)
 - LDAP and PIN, meaning that both LDAP and User authentications are verified (Credentials entered in the login form will be interpreted first as LDAP user/password combination and, if LDAP authentication fails, as User/PIN combination)

NOTE:

1. superadmin is always verified as User/PIN combination against sipXconfig database, no matter what authentication option is selected
2. No matter if a user is LDAP managed or not, if LDAP Only or LDAP and PIN authentications schemes are set, it will try to authenticate against LDAP

Synchronization Schedule

sipXconfig supports on demand synchronization triggered through the sipXconfig UI. Additionally, the administrator has an option to configure a synchronization schedule. Weekly, daily and hourly schedules are supported (every Friday, every weekday, Every day, every hour time etc.).

Management Settings

This is a new tab on left side that contains different settings and management options for LDAP users

- **LDAP authentication:** when disabled, the LDAP authentication will not be verified for user portal or Openfire
- **Overwrite PIN:** When checked, the user Voicemail PIN will get updated at every LDAP import with the mapped LDAP attribute value, if any. If unchecked, the user Voicemail PIN will be set only once, at user creation
- **Age:** LDAP imported user age. You can configure an age for ldap imported users. Age is the difference between current date and last LDAP imported date (available for view on Edit User page). All LDAP imported users that are older than 'age' can be disabled or deleted. Age is expressed in hours and the default value is 24 hours
- **LDAP Page Size:** During import, LDAP search is performed in pages. This settings represents the page size. Default value is 1000. Please mind that there are LDAP servers that do not let you query more than X users at once, or there are LDAP servers that do not support paged search. So depending on these factors you should configure the page size
- **Disable :** When checked, all LDAP imported users that are older than '**age**' will be disabled. A disabled user is an user that cannot authenticate in user portal or IM, cannot register phones, cannot receive voicemails.
- **Delete:** When checked, all LDAP imported users that are older than '**age**' will be deleted.

LDAP Configuration

Configuration
Import
Management Settings

LDAP authentication When unchecked, LDAP authentication will not be used for user portal or Openfire

Overwrite PIN When checked, the user Voicemail PIN will get updated at every LDAP import with the mapped LDAP attribute value, if any. If unchecked, the user Voicemail PIN will be set only once, at user creation

LDAP Users Management

Age: (Default: 24)
Imported LDAP user age - represented in hours

LDAP Page Size: (Default: 1000)
LDAP users can be read from LDAP in pages. A page size is the number of users that are read in block.

Disable: (Default: unchecked)
Automatically disable users that are not imported from LDAP since age

Delete: (Default: unchecked)
Automatically delete users that are not imported from LDAP since age

Apply

Users/EditUser Pages

Users/EditUser pages contain information about LDAP managed users, or Disabled users. Also EditUser page displays last LDAP imported date and disabled date. Any user can be enabled/disabled or marked as LDAP managed or non LDAP managed

On scheduled import a LDAP user that is not marked as LDAP managed will not be imported again

[Add New User](#)

Filter by...	User ID	First Name	Last Name	IM ID	Aliases	Management
<input type="checkbox"/>	200	Mircea	Carasel	song	Kong song	LDAP
<input type="checkbox"/>	201	George	Niculae	201		LDAP
<input type="checkbox"/>	202	Laurentiu	Ceausescu	202		LDAP
<input type="checkbox"/>	203	Douglas	HUbler	203		LDAP
<input type="checkbox"/>	204	Alex	Mateescu	204		LDAP
<input type="checkbox"/>	205	George	Clooney	205		LDAP
<input type="checkbox"/>	206	Gheorghe	Titeica	206		LDAP
<input type="checkbox"/>	207	Stefan	BanicaJr	207		LDAP
<input type="checkbox"/>	208	Michael	Picher	208		LDAP
<input type="checkbox"/>	209	Ciuc	Starasciuc	209		LDAP
<input type="checkbox"/>	210	Taras	Bulba	210		LDAP
<input type="checkbox"/>	georgen		georgen	georgen		LDAP
<input type="checkbox"/>	georgen0		georgen0	georgen0		LDAP
<input type="checkbox"/>	georgen1		georgen1	georgen1		LDAP
<input type="checkbox"/>	georgen10		georgen10	georgen10		LDAP
<input type="checkbox"/>	georgen100		georgen100	georgen100		LDAP
<input type="checkbox"/>	georgen101		georgen101	georgen101		LDAP
<input type="checkbox"/>	georgen102		georgen102	georgen102		LDAP
<input type="checkbox"/>	georgen103		georgen103	georgen103		LDAP
<input type="checkbox"/>	georgen104		georgen104	georgen104		LDAP

<< 1 2 3 4 5 6 7 >>

Delete More actions...

Select the Add New User link and create a new user.

After user is created you can associate it with one or more managed phones

[Add New User](#)

Filter by...	User ID	First Name	Last Name	IM ID	Aliases	Management
<input type="checkbox"/>	200	Mircea	Carasel	song	Kong song	DISABLED LDAP
<input type="checkbox"/>	201	George	Niculae	201		DISABLED LDAP
<input type="checkbox"/>	202	Laurentiu	Ceausescu	202		DISABLED LDAP
<input type="checkbox"/>	203	Douglas	HUbler	203		DISABLED LDAP
<input type="checkbox"/>	204	Alex	Mateescu	204		DISABLED LDAP
<input type="checkbox"/>	205	George	Clooney	205		DISABLED LDAP
<input type="checkbox"/>	206	Gheorghe	Titeica	206		DISABLED LDAP
<input type="checkbox"/>	207	Stefan	BanicaJr	207		DISABLED LDAP
<input type="checkbox"/>	208	Michael	Picher	208		DISABLED LDAP
<input type="checkbox"/>	209	Ciuc	Starasciuc	209		DISABLED LDAP
<input type="checkbox"/>	210	Taras	Bulba	210		DISABLED LDAP
<input type="checkbox"/>	georgen		georgen	georgen		DISABLED LDAP
<input type="checkbox"/>	georgen0		georgen0	georgen0		DISABLED LDAP
<input type="checkbox"/>	georgen1		georgen1	georgen1		DISABLED LDAP
<input type="checkbox"/>	georgen10		georgen10	georgen10		DISABLED LDAP
<input type="checkbox"/>	georgen100		georgen100	georgen100		DISABLED LDAP
<input type="checkbox"/>	georgen1000		georgen1000	georgen1000		DISABLED LDAP
<input type="checkbox"/>	georgen1001		georgen1001	georgen1001		DISABLED LDAP
<input type="checkbox"/>	georgen1002		georgen1002	georgen1002		DISABLED LDAP
<input type="checkbox"/>	georgen1003		georgen1003	georgen1003		DISABLED LDAP

<< 1 2 3 4 5 6 7 >>

Delete More actions...

Select the / new user.

After user is with one or

Identification

- Contact Information
- Phones
- Call Forwarding
- Schedules
- Speed Dial
- Conferences
- Registrations
- Time Zone
- Hot Desking
- Permissions
- Caller ID
- Domain
- Instant Messaging

User: 209 [Show Advanced Settings](#)

Enabled
If user is disabled, then it cannot register, make calls or receive voicemails

User ID:
The User ID can be a numeric extension like 223 or a name like j.smith. The User ID is displayed by the phone and it is therefore recommended to use the internal extension as the User ID.

Salutation:

Last name:

First name:

Manager:

Employee ID:

Password:

Confirm Password:
This is used for log in into the user portal or XMPP. Minimum length is 8

Voicemail PIN:

Confirm Voicemail PIN:
This is used for log in to voicemail. Numeric PINs are recommended, since only numbers can be dialed. Minimum length is 4

Empty password fields

Groups:
List all groups for this user. If a group does not exist, it will be created. When entering multiple groups, separate them with spaces.

Branch:

Aliases:
Aliases are additional names for the user. Like the user ID, an alias can be either a numeric extension or a name. When entering multiple aliases, separate them with spaces.

E-mail address:

Notified:
Flag that informs if the user has been notified of his system account creation.

LDAP managed:
The user is imported from LDAP and managed as LDAP user. If unchecked, the user will not be managed as LDAP user.

LDAP imported date: **6/29/13 9:03 PM**

Disabled Date: **N/A**

Error Reporting

sipXconfig implements a best effort import strategy. All entries that contain enough "well formatted" data are imported, incomplete or invalid entries will be skipped. sipXconfig leverages its error reporting mechanism to inform about problems encountered during LDAP import. The list of successfully imported entries will be available through the UI (Job Status page). The list of entries that failed to import will be available through the UI and in the sipXconfig.log file.

Assumptions & Limitations

- User information is kept in a single sub-tree of an LDAP directory: sipXconfig searches a single sub-tree only trying to locate all entries that fulfill requirements specified by the administrator during the LDAP support configuration.
- Discrepancies between LDAP data and sipXconfig data: LDAP has priority. The sipXconfig database will be updated with information kept in the directory, sipXconfig will never push users' data to LDAP based directory.
- Only user data is retrieved from LDAP: If the administrator intends to configure phones with sipXconfig, the phone information has to be independently provided through the user interface, the SOAP API or via file import.
- All imported users are placed in a single sipXconfig group (configured by the administrator). If necessary the administrator can configure group membership after an initial import. sipXconfig group structure will be preserved during subsequent synchronizations with the LDAP server.
- There is only limited support for retrieving group information. Administrators can map LDAP attributes, values of which will contain user group names; sipXconfig will not support retrieving group information from the tree structure.

Assigning Multiple Values to User Aliases from AD

-Contributed by Steven Lam

1.) Pick a Multi- Valued schema in the Active Directory LADP, in our case, we picked otherHomePhone as eZuce aliases

Reference : <http://fsuid.fsu.edu/admin/lib/WinADLDAPAttributes.html>

2.) Create a VB script to update aliases in the Active Directory otherHomePhone schema.

```
Const ADS_PROPERTY_UPDATE = 2
```

```
Set objGroup = GetObject _  
("LDAP://cn=MyerKen,ou=HR,dc=NA,dc=fabrikam,dc=com")
```

```
objGroup.PutEx ADS_PROPERTY_UPDATE, _  
"otherHomePhone", Array("2125550180", "2125550182", "john")  
  
objGroup.SetInfo
```

Reference : <http://technet.microsoft.com/en-us/library/ee156515.aspx>

3.) Add otherHomePhone to Active Directory Users and Computers

1. Open ADSI Edit on your Active Directory Server – on server 2008 it would be start > Administrative Tools > ADSI Edit
2. Now ADSI Edit will prompt you with connection settings, ensure that "Select a well known Naming Context:" is set to "Configuration"
3. Now click OK
4. Expand the "Configuration [ServerName.yourdomain.com]" Tree
5. Expand "CN=Configuration,DC=yourdomain.com"
6. Expand "CN=DisplaySpecifiers"
7. Now Expand "CN=409" (This is just the language code for English)
8. Locate "CN=default-Display" in the right pane
9. Right click "CN=default-Display" and select "Properties"
10. Select the "extraColumns" Attribute in the list and you will notice that your "Edit" button becomes active
11. Now click the edit button
12. In the "Value to add:" field type the following otherHomePhone, eZuceAliases,0,100,0
13. Now click "Add:"
14. Click "OK"
15. Click "OK" again

4.) View eZuceAliases in Active Directory

1. Open ADUC
2. Expand "Saved Queries"
3. Right Click "Saved Queries" select "New > Query"
4. In the "Name:" field type "All Users" and select "Define Query..."
5. On the "Users" tab next to the "Name:" field click on the drop down and select "Has a value"
6. Now Click "OK" and "OK" again
7. Expand "Saved Queries" and select "All Users"
8. Now you will have a list of all your users in the right pane.
9. With the query selected click "View > Add/Remove Columns..." at the top of ADUC
10. Now on the left selection box, locate " eZuceAliases " and click "Add" to add it to the "Displayed Columns"
11. Click "OK"

5.) EDIT eZuceAliases in the Active Directory

1. In ADUC click "View > Advanced Features"
2. Now right click on your "All Users" saved query and select "Refresh"
3. Next, right click any user in the right pane and click "Employee Number"
4. Now right click the user again and click "Properties"
5. Locate the tab called "Attribute Editor"
6. Press the letter "E" twice on your keyboard, which should take you straight to "otherHomePhone "
7. To edit it, simply double click " otherHomePhone " or click on the "Edit" button while "otherHomePhone" is highlighted

Reference : <http://iconraja.wordpress.com/2010/12/01/add-employee-number-to-active-directory-users-and-computers-aduc/>

Further Reading

- [Windows Server LDAP Access](#)

LDAP Clients that can be used to manipulate LDAP directories

Moving to LDAP also allows leveraging tools for user and identity data entry and management. LDAP tools are stable, well developed, available for many platforms also in open source.

- Softerra LDAP administrator: <http://www.ldapadministrator.com/> Windows only, Shareware or \$215
- PHP LDAP admin: <http://phpldapadmin.sourceforge.net/screenshots.php> free
- Web based LDAP admin: <http://yala.sourceforge.net/> free
- LDAP browser: <http://www-unix.mcs.anl.gov/~gawor/ldap/index.html> free
- GTK-based LDAP client: <http://gq-project.org/> GNU
- Apache directory: <http://directory.apache.org/studio/> free