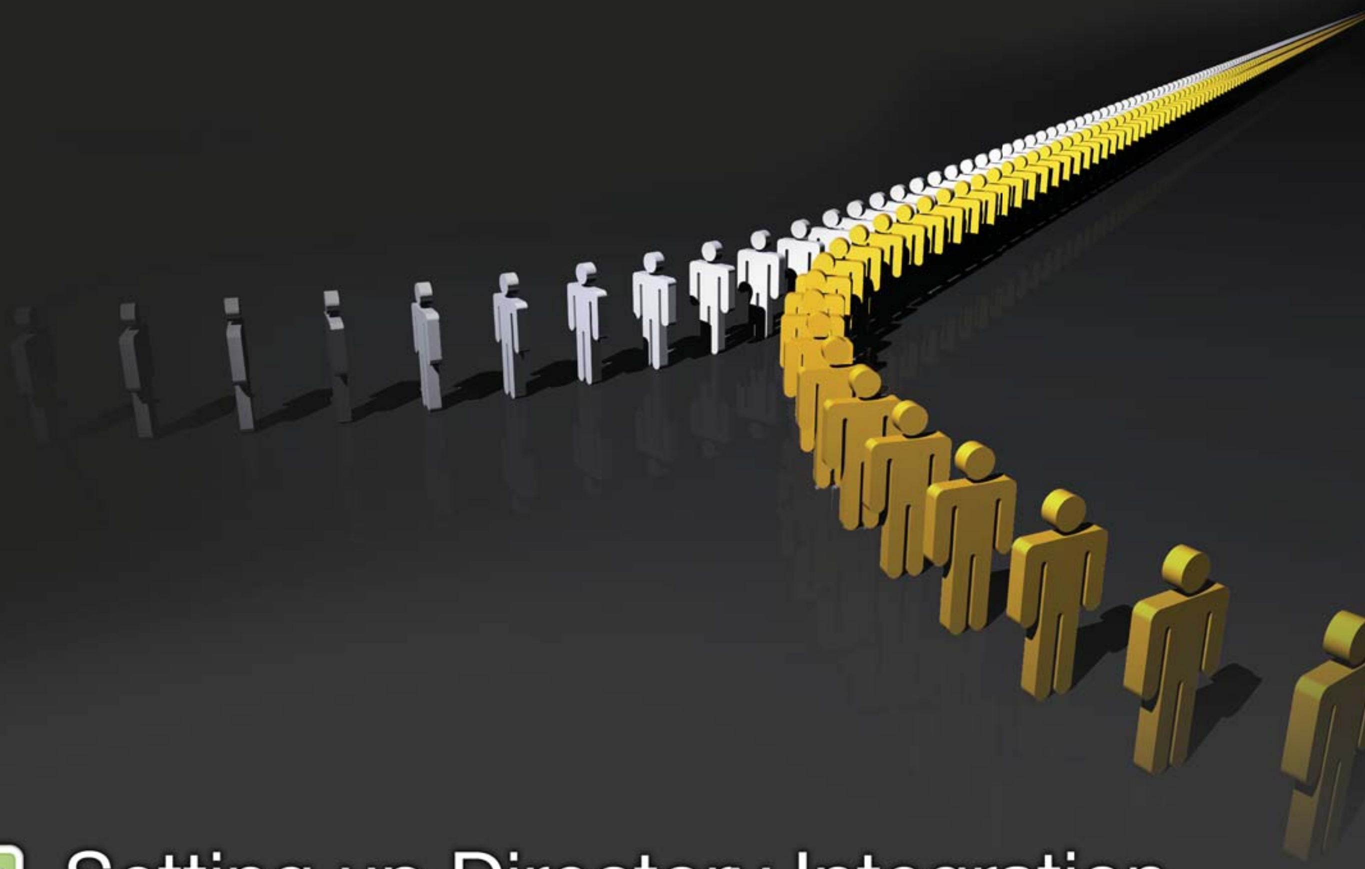


Setting up Directory Integration with LotusLive™ iNotes

Version 1.0

Notices

International Business Machines Corporation provides this publication “as is” without warranty of any kind, either express or implied. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore this statement may not apply to you.

This publication may contain technical inaccuracies or typographical errors. While every precaution has been taken in the preparation of this document, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/ or changes in the product(s) and/or the program(s) described in this publication at any time.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license enquiries, in writing, to the IBM Director of Commercial Relations, IBM Corporation.

The following terms, used in this publication, are trademarks or service marks of corporations in the United States or other countries:

Contents

1 Introduction

1.1. Terminology

Enterprise Directory: The customer's directory of person and group entries.

Corporate Directory: LotusLive iNotes directory of all corporate persona and group entries, typically created from and synchronized with the Enterprise Directory.

Contacts: Address information on individuals and groups in each user's own personal list.

LDIF (LDAP Data Interchange Format): A standard format for exchanging information about directory entries via text files.

1.2. What Directory Integration with LotusLive iNotes is

Directory integration in LotusLive iNotes, today, is a means of synchronizing a company's enterprise directory with the Corporate Directory in LotusLive iNotes. Two options are available, which are described below. Note that one of these options (synchronization) is strongly preferred over the other, by the LotusLive team.

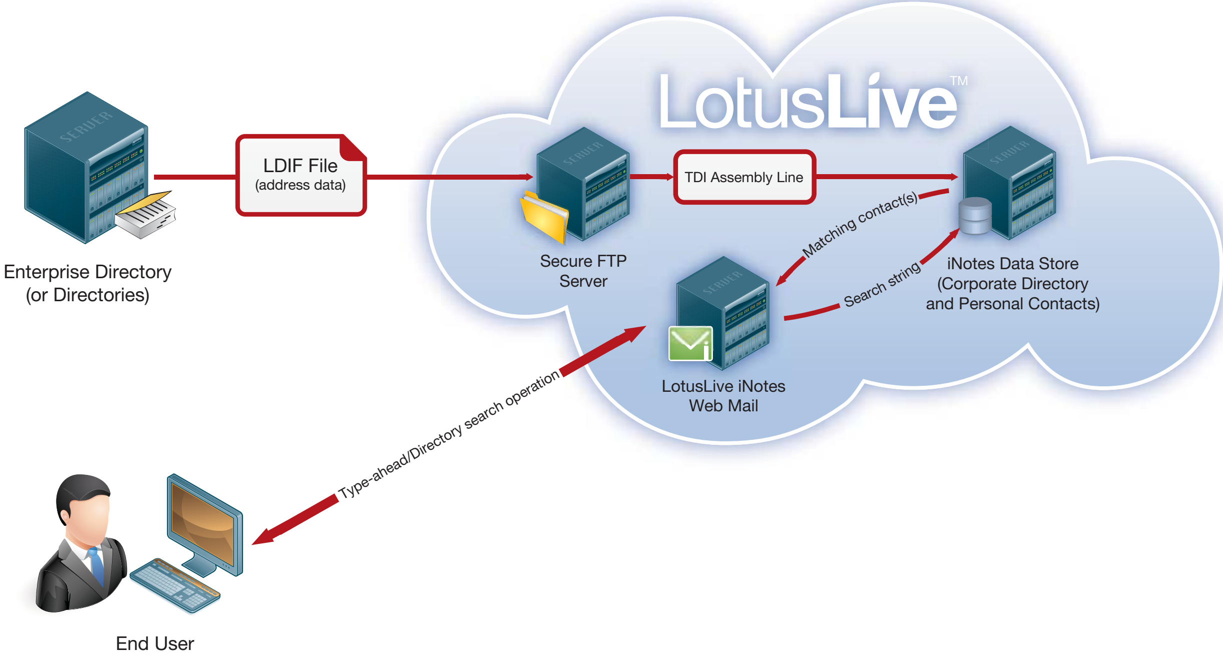
1.3. and what it is not.

In the current release of LotusLive iNotes, directory integration does not cover provisioning (the setting up of accounts). That is, when a user is created in your Enterprise Directory, and that information is synchronized with the Corporate Directory in LotusLive iNotes, this does not also create, modify or delete user accounts in LotusLive iNotes.

2 Corporate Directory Synchronization

2.1. Overview

With Corporate Directory Synchronization, some of the data from the Enterprise Directory is copied to, and stored within, LotusLive iNotes. Users are then able to access these entries in the LotusLive iNotes Corporate Directory at the same speed with which they can access their Personal Contacts inside LotusLive iNotes. In particular, automatic address completion (also known as “type-ahead addressing”) and address book browsing can be supported across all users and groups in the combination of the user’s local address book, and the integrated Corporate Directory. Synchronization also permits a larger range of contact information to be loaded into LotusLive iNotes, and made available to users, than the alternative.


LotusLive™
Enterprise Directory (or Directories)
LDIF File (address data)
Secure FTP Server
TDI Assembly Line
iNotes Data Store (Corporate Directory and Personal Contacts)
Matching contact(s)
Search string
LotusLive iNotes Web Mail
Type-ahead/Directory search operation
End User

In order to implement Corporate Directory synchronization, the client is responsible for creating an LDIF file which includes additions, updates and deletions from the Enterprise Directory (or Directories), and place it (them) on a secure FTP server.

Most LDAP server implementations, such as Tivoli Directory Server or Active Directory, provide a capability for easily generating a change file, which specifies the additions, deletions, and modifications of person and group entries in the Enterprise Directory since the previous change file was generated. In this case the format of the file would be LDIF. Other non-LDAP directory systems or corporate HR workflows also make it relatively easy for a customer to generate change files. In some cases these systems may only support other formats, such as XML and comma separated values (CSV). If this is the case please bring this to the attention of your IBM sales executive and implementation project manager. The Tivoli Directory Integrator (TDI) process is capable of reading other file formats; including XML and CSV, but at this time only the LDIF file format has been defined for this process.

2.2. How to send it

The Customer runs a job to create and upload the LDIF files using secure FTP to a specified location on the LotusLive Site. The drop-off location is a private subdirectory dedicated to the customer, and the file must be delivered in plain-text with no additional encryption.

LotusLive utilizes Tivoli Directory Integrator (TDI) to process and maintain directory updates. The TDI assembly line will periodically check for the existence of a new change file and perform the specified operations to the LotusLive iNotes Corporate Directory.

The specific instructions regarding where to send files will be provided during the implementation process.

2.3. How often is the process run

There is no set expectation as to how often a new LDIF file is transferred to LotusLive. Factors affecting how frequently the synchronization should be performed include:

- Frequency of updates to the source Enterprise Directory system(s).
- Acceptable delay in having the Enterprise Directory and Corporate Directory entries perfectly synchronized.
- Resource considerations for the Enterprise Directory system’s availability to produce and transfer new LDIF files.
- Resource considerations on the LotusLive’s capacity to process additional files. IBM will make reasonable commercial efforts to meet a requested schedule, but must also balance the needs of all its clients when allocating resources.

2.4. LDIF file definition

2.4.1 File naming convention

Ensuring that each file produced is correctly named and sequenced is the responsibility of the system that creates the file – the source system. LotusLive cannot rename or re-sequence files on arrival. Files are to be named using a convention such as:

<client>_<filetype>_<date>_<seq>.txt

E.g. Example_LDIF_20091028_001.txt

Where:

- The company name is “Example”
- File type is “LDIF” (CSV and XML may be supported in the future)
- Date section format is: YYYYMMDD
- <Seq>uence is a three character numeric string starting with 001 and incrementing until 999.
- Date and sequence numbers are defined by the source (client’s) system and time zone. Synchronization of dates between the client’s source system and IBM is not required.

The exact file name format, and any related requirements, will be communicated to the client before the implementation begins. During the implementation process the value of the <client> field, which will be unique to each client, will be assigned by IBM, and communicated to the client. Should there be a need for more than one independent file feed, from independent directory sources within the client, such that the file names cannot be coordinated at the source, each set will be identified by a distinct <client> value, such as example01, example02, etc.

When there are multiple data sources it is also essential to ensure that that all updates for a unique user or group entry are restrict to a single authoritative source.

2.4.2 What to include in the file

Once this process is initiated, the LotusLive iNotes Corporate Directory will rely entirely on these uploaded files for everything stored within it. As such, everything that the end users need to have available and searchable by them must be sent, updated and deleted when necessary, using this file transfer process. LotusLive iNotes will not automatically include data from any other source.

Consider for inclusion:

- All the internal email accounts for users on: LotusLive iNotes, LotusLive Notes or Hosted Notes, On-premises Lotus Notes, Exchange or other mail systems, third party hosted mail systems.

- All Distribution lists, mailing lists, and aliases: Include email addresses that can normally be sent to from outside the domain, and are available as a fully qualified SMTP style email address such as “sales@example.com”. LotusLive iNotes needs only the list email address, as it does not expand lists into individual user addresses prior to sending email. LotusLive iNotes treats list names as a single, ordinary, email address. List expansion will be performed by the recipient system – i.e. the system on which the list was defined, and to which the email will be delivered. This reduces outbound traffic, and means that list members never have to be synchronized with LotusLive iNotes.

- Outside or third party entries: Any email addresses that may belong to outside organizations, but you wish to have available for lookup. This might include email addresses from sister companies or divisions using different domain names, suppliers, clients, and so on.

2.4.3 Data Fields for Person Entries

Person entries (individuals) in the change file should be specified in terms of the inetOrgPerson schema. Mandatory attributes in the table below are in bold, the rest are optional. The table also shows the mapping for other LotusLive supported attributes which have no inetOrgPerson equivalent.

Field	Length or Type	inetOrgPerson attribute	other attributes
Basic info			
First Name	32	givenName	
Middle Name	64	-	middleName
Last Name	32	sn (surname)	
Alias Name	32	-	aliasName
Display Name	**100**	**displayName**	
Email Address	**64**	**mail**	
Alternative Email	128	-	alternativeEmail
Category	32	businessCategory	
Work Phone	32	telephoneNumber	
Pager	32	pager	
Mobile	32	mobile	
Fax	32	facsimileTelephoneNumber	
Other	128	-	other
Personal info			
City	32	-	homeCity
State/Province	32	-	homeState
Postal Code	32	-	homePostalCode
Country	32	-	homeCountry

Field	Length or Type	inetOrgPerson attribute	other attributes
Business info			
Company Name	128	o (organizationName)	
Title	128	title	
Address	255	street	
City	32	l (localityName)	
State/Province	32	st	
Postal Code	32	postalCode	
Country	32	c	
Personal Website	128	-	personalWebsite
Business Website	128	labeledURI	
ICQ UIN	16	-	icqUin
Birthday	date	-	birthday
Anniversary	date	-	anniversary
Comment	255	description	

The set of available directory entries (above) is subject to change, and the most recent set should be verified at the beginning of the implementation project.

After processing the change file a summary document containing the status of each change will be emailed to an email address specified by the customer.

2.4.4 Data fields for group entries

Group entries in the change file are a subset of the groupOfNames schema. Mandatory attributes in the table below are in bold, the rest are optional.

LotusLive iNotes does not need to expand the groups before sending them, and hence does not need to have the list of unique members. Group expansion will be performed by the system on which the group was defined.

Field	Length or Type	groupOfNames attribute	other attributes
Basic info			
Group Name	**64**	**cn** (commonName)	
Comment	255	description	
Company Name	128	o (organizationName)	
Email Address	**64**		**mail**

The set of available directory entries (above) is subject to change, and the most recent set should be verified at the beginning of the implementation project.

After processing the change file a summary document containing the status of each change will be emailed to an email address specified by the customer.

2.5. Examples of LDIF file entries

The following example shows most of the types of operations that can be encoded in the LDIF change file.

```
# Add this new person to the directory.  If this were a group objectClass would be
# groupOfNames rather than inetOrgPerson.  The displayname and mail attributes are
# mandatory, all others are optional.
DN: cn=Sam West,ou=Development,o=Example
changeType: add
objectClass: inetOrgPerson
displayName: Sam West
mail: new.guy@example.com
givenName: Sam
sn: West
telephoneNumber: 999 123-9876
```

```
# Finally traded in his pager for a cell phone!
DN: cn=Fred Flintstone,ou=Accounting,o=Example
changeType: modify
delete: pager
replace: mobile
mobile: 123 456-7890
```

```
# Append two more phone numbers to this users existing number(s)
DN: cn=Francis Baker,ou=Marketing,o=Example
changeType: modify
add: telephoneNumber
telephoneNumber: 111 222-3333
telephoneNumber: 444 555-6666
```

```
# Replace any existing title with a new title
DN: cn=William Stokes,ou=Sales,o=Example
changeType: modify
replace: title
title: Senior Vice President
```

```
# This employee left the company so delete their person entry
DN: cn=Derek Jones,ou=Quality Assurance,o=Example
changeType: delete
```

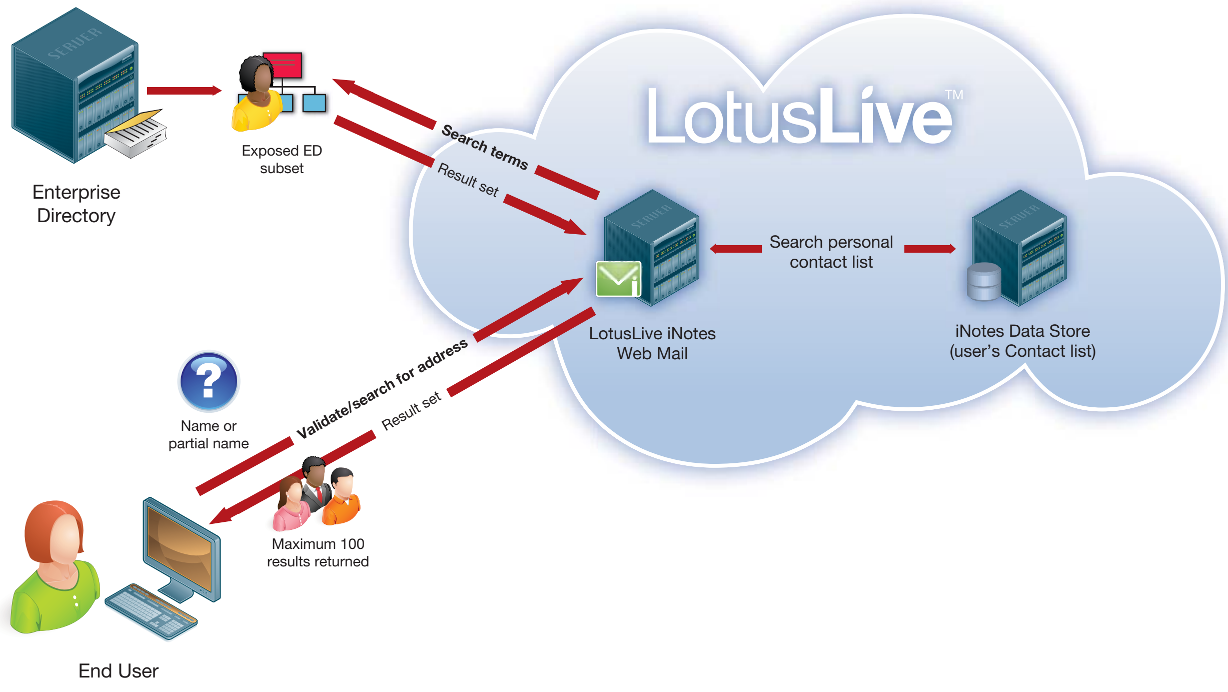
```
# This person got married and changed organizational units!
# Note that this either one of these changes
# effectively changes the unique identifier of this entry.
dn: cn=Marsha Bradford,ou=Product Development,o=Example
changetype: modrdn
newrdn: Marsha May
newsuperior: ou=Marketing, o=Example
```

For the full specification of LDIF please see http://www.faqs.org/rfcs/rfc2849.html

3 Real-time Enterprise Directory Access

3.1. Overview

With Real-time direct LDAP Enterprise Directory Access, the look-up capabilities of the “Address Mail dialog” are extended with the contents of a single remote Enterprise Directory. The lookup happens in real time when a user enters an address in a mail ‘to’ (cc or bcc) field. The remote LDAP server is searched for matching person and group entries in addition to the normal LotusLive iNotes address books.


Enterprise Directory
Exposed ED subset
Search terms
Result set
LotusLive™
LotusLive iNotes Web Mail
Search personal contact list
iNotes Data Store (user’s Contact list)
Name or partial name
Validate/search for address
Result set
Maximum 100 results returned
End User

3 Real-time Enterprise Directory Access

In this scenario the Customer must provide outside the firewall (Internet) access to an LDAP server fronting their Enterprise Directory that must be capable of handling LDAP queries from the LotusLive iNotes users. This query will be run on each user initiated directory look-up, so adequate capacity will be needed.

Because of the remote-call nature of this approach keystroke “type-ahead” address completion is not supported because of performance, bandwidth and load considerations on the network and corporate LDAP server. Also, as the Enterprise Directory is remote, browsing the directory (i.e. scrolling through lists of entries) is also not possible using this method. The amount of data retrieved during a real-time remote lookup will also be restricted to less than could be available using the synchronization method.

Note that LDAP access failures due to bandwidth or service constraints, or system failures, at or en-route to the client’s end are not counted towards any SLA compliance measures. The customer is responsible for ensuring that the SLA of their source LDAP server is no less than the SLA of the LotusLive iNotes service.

Search requests will be performed asynchronously to avoid tying up valuable resources, and a timeout of 60 seconds will be used to terminate long running search requests. The number of matching entries returned by the LDAP server, and presented to the end user, is capped at 100.

This option can only support a single LDAP source. If a client has multiple sources of data (or a non-LDAP source) then they will need to implement a consolidation of the required data into a single LDAP source.

3.2. Configuration

The exposed LDAP person entries are assumed to conform to the inetOrgPerson objectClass. If the match is a person then the mail attribute returned on the search is used to replace the name.

Support for LDAP groups (groupOfNames, groupOfUniqueNames, or Group objectClass) is not available in this mode because LDAP group entries expect the group to be expanded into its component individuals, rather than providing the group mailing address (aka mailing lists or distribution lists). Since the objective is to search for, or validate, the group email address, group addresses must be added to the exposed LDAP as if they were unique persons.

When setting up the fronting LDAP server, keep in mind that LotusLive iNotes will only use this information for name and email address validation, and that loading this LDAP server with extra information (e.g. phone numbers, addresses) is unnecessary, as it will not be used. LotusLive iNotes will retrieve only the minimum information it needs, regardless of what else may be available, to ensure best possible performance. Loading the fronting LDAP server can be done in a number of ways including selective replication, application specific directories (e.g. ADAM), 3rd party directory integration products (e.g. TDI), or other home grown or off-the-shelf tools. This process also provides the opportunity to rewrite group addresses as 'persons'. If it is not practical for the customer to produce a selective partition then access control should be applied to limit access to only the necessary information.

The following configuration information on the customer's LDAP server must be provided.

- hostname – DNS hostname or IP address of the exposed LDAP server
- port – port the LDAP server is listening on (e.g. 389, 636 for SSL)
- channel encryption - to enable SSL (other SSL options may be needed)
- username/password – credentials with sufficient rights to read relevant person and group entries. If specified then an LDAP bind operation specifying the credentials will precede the search.
- base – DN of the subtree which contains the person and group entries
- vendor – e.g. TDS, Domino, Microsoft, Sun, Novell

The first four configuration parameters above are used on the LDAP bind request to establish the session used for the search request. The base parameter is used on the search request. The last two parameters are used in some circumstances to determine the filter on the search request.

3.3. Caveat

Note that this option is **not** considered optimal for the best end-user experience, and is not the approach the LotusLive team recommends. This approach should only be considered if there are insolvable concerns, or company policy, that prohibits the synchronization option from being used.