Accessing the Domino directory with LDAP

by Mark Gordon

[Editor's note: This article resides in "Iris Today", the technical Webzine located on the http://www.notes.net Web site produced by Iris Associates, the developers of Domino/Notes.]

Did you ever wish there was a phone book for Internet mail addresses, or perhaps an operator you could call? If you use Notes to send mail, you can click an Address button to browse through a list of names in the Domino Public Address Book. But what if you want to address mail to somebody whose name is in an Exchange directory or an X.500 mail directory? This is what LDAP is for: to allow users to use a single mail client to look up recipients in various vendors' directories. If your mail client supports LDAP and the directory servers support it, you are all set! As you'll see, a seamless directory access world is not quite here, but it is coming, and you'll see how Domino helps make it possible.

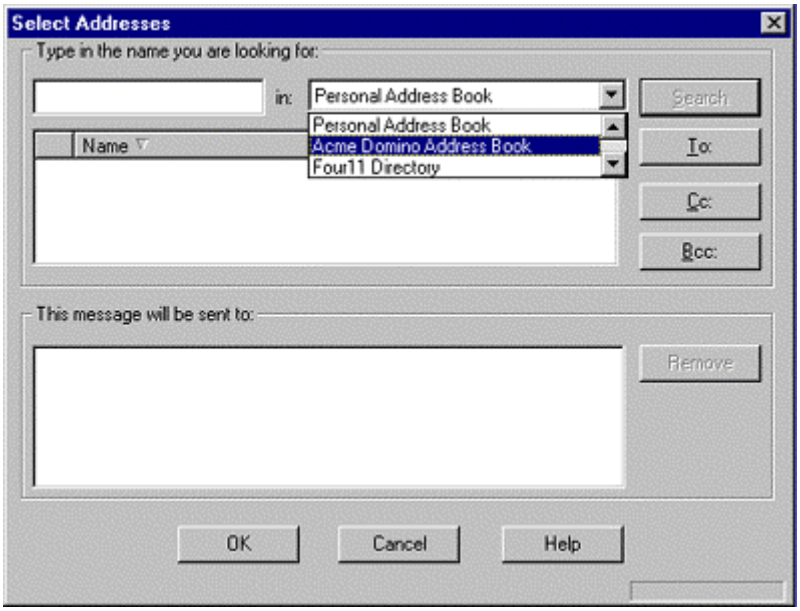
This article discusses more about what LDAP means, why Domino supports it, and what it can do for your users. If you are already familiar with LDAP, you may want to skim the introduction. However, I'll also describe the LDAP features Domino 4.6 offers -- that is, *how* Domino supports the standard -- and give you an overview of how to get the service set up in Domino.

An introduction to LDAP

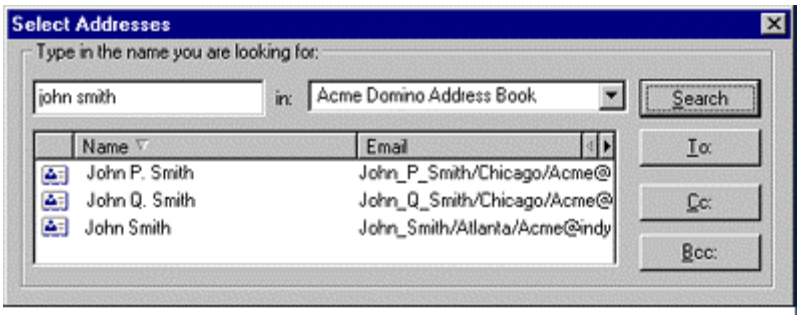
LDAP stands for *Lightweight Directory Access Protocol*. Notice that the first word in the LDAP acronym is *Lightweight*., because this protocol is a lighter version of the original X.500 directory access protocol (DAP). LDAP does not require nearly as large a footprint as the full DAP -- DAP requires the full OSI stack -- so it is more practical for inclusion into mail clients. So what does this mean in terms of features? If a mail user does a search for the name *John Smith* using the DAP protocol, the DAP server not only looks for John Smith, but also checks other servers it knows about. With LDAP, the server simply sends back a referral to the LDAP client if there are other related servers to search. The LDAP client must then perform the subsequent referral searches. LDAP also uses a simpler text-string coding technique, which makes developing LDAP-compliant clients and servers easier than their more complex DAP counterparts.

An LDAP End-User Experience

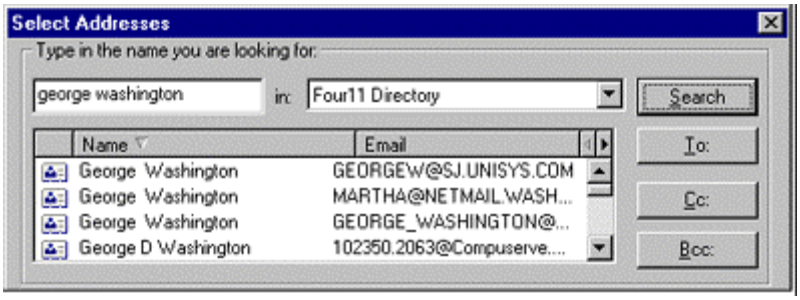
So how does an LDAP client look up names for you as you're addressing mail? First, you configure your LDAP client to point to one or more directories. (This process is quite simple. See the section below on setting up LDAP). Using Netscape Communicator as an example: when you address a message, you click the Address options button, and you are prompted to specify which directory you want to search:



This scenario is pretty simple. If you type John Smith, you are shown a list of all the John Smiths to choose from.



Searching your company's Domino server for John Smith might be fine. You may get five matches or 20. But I wouldn't recommend searching a large directory such as Four11 (a public Internet White Pages service that provides both Web and LDAP access) for John Smith. Even a less common name, like George Washington, returned 43 matches:



What is a Referral Anyway?

What happens if the server you are accessing doesn't have the entry, but knows where it can be found? LDAP servers can be set up to "know about" other LDAP servers, and to refer LDAP clients to those other servers if the user is not found in the first server. Rules can also be configured that direct the user to a particular server based on the search criteria. An LDAP server for the Acme company might be configured

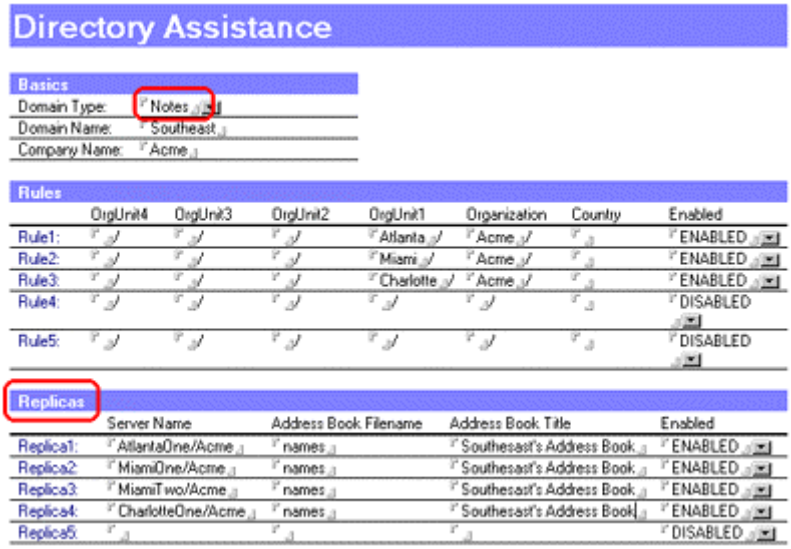
to refer all requests for Atlanta employees to a server in Atlanta, for example. That way, each mail user can have her mail client configured to access just her home directory, but that directory server will refer her to others as needed.

Before we explore how Domino supports the LDAP specification for referrals, let's step back a moment and examine how the prior release of Domino already supported the referral concept for Notes clients.

A Quick Look at the Native Notes Equivalent to LDAP: Master Address Books

In large Domino installations there are often multiple Domino domains. This is done either to avoid one overly large address book or because of the company's organizational or political structure. Domino 4.5 introduced the Master Address Book feature for such organizations, so that users can use the Notes Mail addressing features *lookup* and *type-ahead* to search through multiple domain address books seamlessly, no matter what server they are stored on.

The Master Address Book defines all the domains for the organization, and keeps track of the file names and servers where all the domain address books are located. It stores the naming rules for a collection of domains, so that when a user types in an address, Domino knows which address book to check. For example, the Acme company might have several domains, one for each region of the country. The address book for domain *Southeast* might include organizational units /Atlanta/Acme, /Miami/Acme, and /Charlotte/Acme. So within the Acme Master Address Book -- which is replicated between servers in ALL the Acme domains -- there would be a Directory Assistance document that looks like this:



Directory Assistance

Basics

Domain Type:	Notes
Domain Name:	Southeast
Company Name:	Acme

Rules

	OrgUnit4	OrgUnit3	OrgUnit2	OrgUnit1	Organization	Country	Enabled
Rule1:				Atlanta	Acme		ENABLED
Rule2:				Miami	Acme		ENABLED
Rule3:				Charlotte	Acme		ENABLED
Rule4:							DISABLED
Rule5:							DISABLED

Replicas

	Server Name	Address Book Filename	Address Book Title	Enabled
Replica1:	AtlantaOne/Acme	names	Southeast's Address Book	ENABLED
Replica2:	MiamiOne/Acme	names	Southeast's Address Book	ENABLED
Replica3:	MiamiTwo/Acme	names	Southeast's Address Book	ENABLED
Replica4:	CharlotteOne/Acme	names	Southeast's Address Book	ENABLED
Replica5:				DISABLED

As you can see from the screen, the naming rules are set up by specifying for each domain's Public Address Book the organizational units that are stored in that domain and on which server(s) a replica of that address book can be found. If any user in any of Acme's domains were to type *John Smith/Atlanta/Acme*, the type-ahead feature would check with the Master Address Book and verify that address in the appropriate address book on the appropriate server.

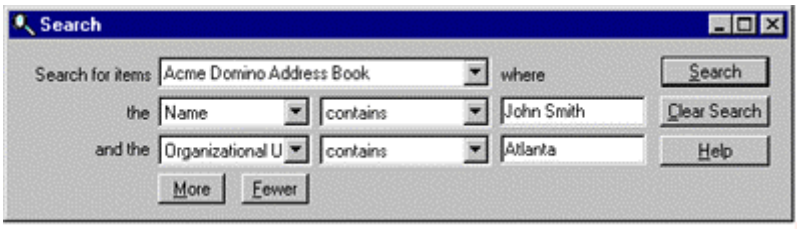
Note: If directory assistance using the Master Address Book in Domino is new to you, but you're an experienced Notes 4.1 administrator, you may ask how this approach compares to Cascading address books. The short answer: it's more flexible, supports server failover, and supports the type-ahead feature.

Domino 4.6 Adds Directory Assistance Support for LDAP Clients

To support directory assistance in LDAP (they are called *referrals* in LDAP), Lotus has merely added the appropriate protocol support to the Directory Assistance function it already supported. Instead of having a reference to other Domino address books on other Domino servers, the Directory Assistance entry for an LDAP server refers to other LDAP servers.

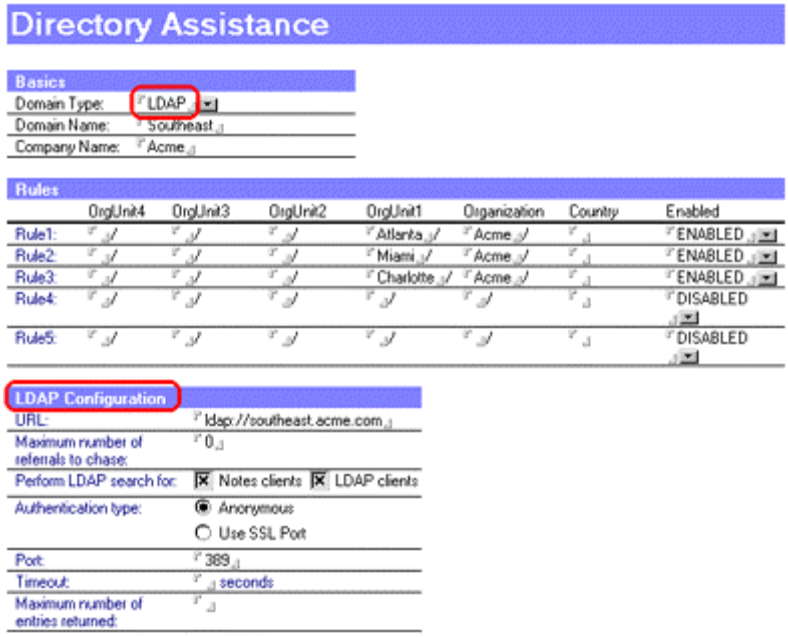
Let's say that instead of using Domino throughout the company, as the above example implies, the Acme corporate office in Chicago uses Domino for mail, but the plants in the Southeast use Exchange. Although headquarters uses Domino, and most of the corporate staff use Notes Mail clients, a few use Netscape Communicator mail clients. Fred in Accounting uses his Netscape Communicator client, and searches for John Smith/Atlanta. But Fred's Netscape client is configured to access the Domino address book via LDAP, not the Exchange directory in Atlanta, where the John Smith entry is stored. His mail client *could* be configured to access both directories, but it isn't -- people in accounting don't send mail to people in the plants too often, so the administrators haven't taken the time to configure all the directories on each LDAP client.

Can Fred look up John in Atlanta, or is he out of luck? This is where the concept of referrals comes into play. As shown in the following screen, Fred can specify an organizational unit (in this case, Atlanta) when searching for the name John Smith.



His home Domino server knows that */Atlanta entries are stored on the Exchange server, so it can *refer* Fred to the LDAP URL of the Exchange server. It does this by passing an LDAP URL to Fred's mail client, which then automatically requests that URL for him and pulls up the Exchange directory. Fred then sees the entries matching John Smith in the Exchange server.

The Directory Assistance documents within the Master Address Book are where you configure Domino to point to another server based on a rule such as */Atlanta/Acme. You specify an *LDAP* domain type instead of a *Notes* domain type. Notice that the LDAP *Directory* Assistance document differs from the Notes *Directory Assistance* document shown above:



The document calls for a URL field pointing to another LDAP server, as opposed to the Notes Directory Assistance document, which lists servers and replicas of the target domain's address book. This example shows that any request for users in Atlanta, Miami or Charlotte should be referred to the URL of an LDAP server on host southeast.acme.com, which in our example is the Exchange server in Atlanta.

Using this LDAP URL syntax, you can refer to an LDAP server anywhere on your intranet or the Internet. If your company uses LDAP to access directories in a mix of mail systems -- such as Domino, Exchange, and NDS -- you can configure the servers to refer mail clients to each other when the criteria of the search requires it.

It is worth noting that while to the user it's not obvious whether a name lookup is being handed off to another Domino server or an LDAP server, Domino handles native Notes directory assistance differently than LDAP referrals. With a Notes client lookup into the Master Address Book, the Domino server does the lookup into the appropriate domain address book on behalf of the user. With an LDAP client, the domino server sends the referred URL back to the client, which then does another lookup to the second server.

How Domino supports LDAP

The current version of LDAP is version 2, which is what the Domino 4.6 supports. Domino supports searches by either person, group, organization, or organizational unit. It also supports complex searches -- Boolean searches involving multiple criteria.

Security is enforced only at the simple level (LOGIN level), therefore Lotus has elected to support read-only access to LDAP directories for now.

LDAP version 3 should be approved this year, and Lotus expects to support it in an upcoming release of Domino. Lotus also plans to support read-write access to directories, as well as chaining (directory assistance done by the server rather than by passing referrals to the client), international character set support, enhanced security and advanced search capabilities in an upcoming release of Domino.

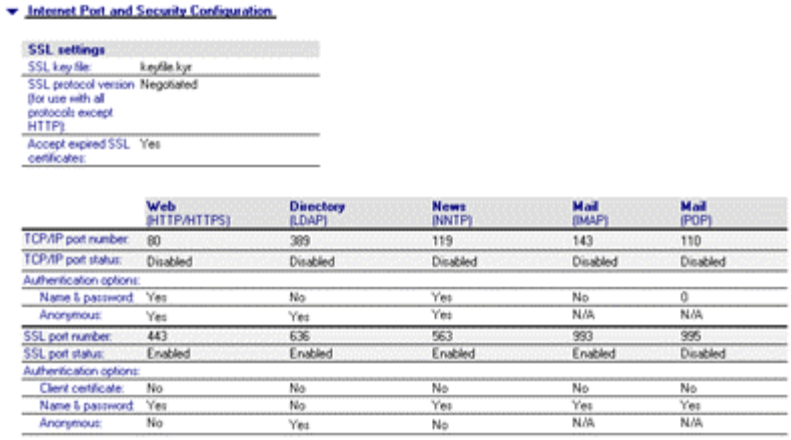
How to set up LDAP in Your Domino Network

Use the following steps to set up LDAP.

1. **Upgrade the Address Books.** If you are upgrading from Notes 4.5, you must first upgrade the Public Address Book with the 4.6 template, and also upgrade the Master Address Book with the 4.6 Master Address Book template.

2. **Set up a Master Address Book**. If you are setting up a Master Address Book for the first time, see the Domino Administration Help database in the *doc* subdirectory on your Domino server, and refer to the help topics for setting up and enabling the Master Address Book. These topics will explain how to create a Master Address Book based on the template, and how to reference the Master Address Book in each server document in your domain(s). For each directory assistance document in the Master Address Book -- there is one per LDAP server you are referring clients to -- specify the naming rules and the URL for the server as shown in the screens in the */Atlanta/Acme example.

3. **Configure the Server document (Internet Port and Security Configuration section)**. The Server document contains a new section called Internet Port and Security, which includes settings for LDAP access. You can use the defaults and simply enable the LDAP port.

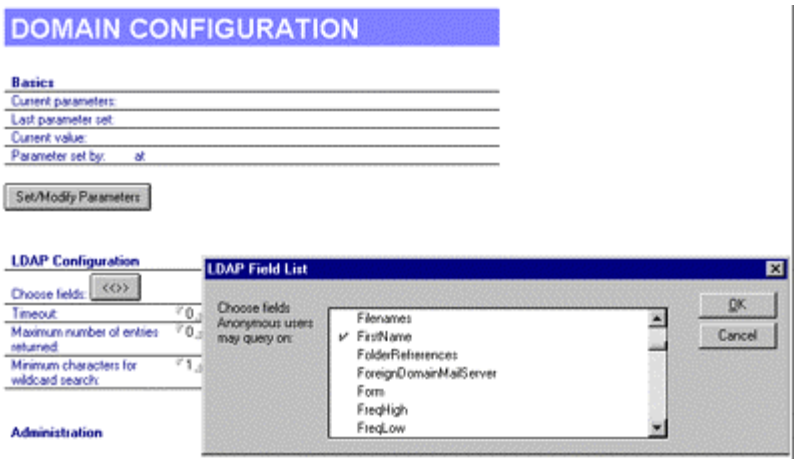


▼ Internet Port and Security Configuration

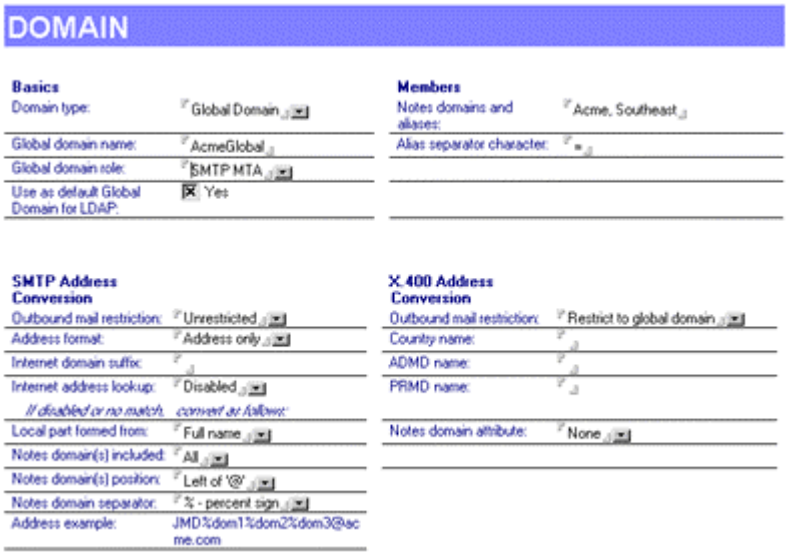
SSL settings	
SSL key file:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept expired SSL certificates:	Yes

	Web (HTTP/HTTPS)	Directory (LDAP)	News (NNTP)	Mail (IMAP)	Mail (POP)
TCP/IP port number:	80	389	119	143	110
TCP/IP port status:	Disabled	Disabled	Disabled	Disabled	Disabled
Authentication options:					
Name & password:	Yes	No	Yes	No	0
Anonymous:	Yes	Yes	Yes	N/A	N/A
SSL port number:	443	636	563	993	995
SSL port status:	Enabled	Enabled	Enabled	Enabled	Disabled
Authentication options:					
Client certificate:	No	No	No	No	No
Name & password:	Yes	No	Yes	Yes	Yes
Anonymous:	No	Yes	No	N/A	N/A

4. **Configure the Domain Configuration document.** The Domain Configuration document allows you to specify which fields in the Person documents are available to anonymous LDAP clients for searching. By default, the name fields and the organization are available, but you can create a Domain Configuration document to grant access to more fields if you prefer. Just go to the Server - Connections view in the domain address book, and create a Domain Configuration document using the Create menu.



5. **Configure the Global Domain document.** The Global Domain document defines the rules for converting Notes users' mail addresses to Internet mail addresses. You must create a Global Domain document to specify addressing rules for your entire Internet domain whether you are using the Domino SMTP MTA or the LDAP server, or both. Domino follows the addressing rules for this document for all Internet addressing.



6. **Load the LDAP Server Task.** Type *LOAD LDAP* at the Domino server console. Add *LDAP* to the *Server Tasks* = line of the NOTES.INI file to have the LDAP service start automatically with the Domino server.

Conclusion

The Domino 4.6 support for LDAP is a step towards getting true directory assistance for Internet mail. If you use Domino in conjunction with other LDAP-compliant mail systems, your organization gains a great deal of flexibility in how you provide this mail addressing lookup capability.

For More Information

For more information on LDAP, see these sources:

- SunWorld Online Article: *LDAP: The Next-Generation Directory?*
- Netweek Article: *LDAP Seeks to Solve Directory Confusion*
- Intranet Archive*: Emerging Standards: LDAP*