

Technical White Paper

LDAP Integration with bf.collaboration



February 15, 2005

For more information, contact

bf.collaboration, Inc
8126 Larkin Lane
Suite 300
Vienna, VA 22182

Phone: 703-627-2633
Fax: 703-991-4866

Introduction

In today's enterprise information infrastructures, it is very common to maintain an organization-wide global list of users. This list is then used for many purposes including, but not limited to, sending organization-wide correspondence, maintaining employee information, and authenticating users to use enterprise software (i.e. Microsoft Exchange/Outlook, company intranet, etc.).

These global lists are maintained by database-like software known as *Directory Services*. Examples of popular directory services are Microsoft's *Active Directory*, Novell's *eDirectory*, and Netscape's *Directory Server*. These popular directory services each offer an abstract, industry standard way to query and update user information through what is known as Lightweight Directory Access Protocol – or LDAP.

Applications – such as bf.collaboration – that require authentication, and have network access to the Directory Service, can then use LDAP to authenticate against and/or import user/employee information.

This paper explains how bf.collaboration leverages LDAP to provide seamless integration with standard-compliant directory services.

The Process

Many applications that “integrate” with your directory service simply provide a means to import users from your directory service into the application's own user database. Then, actual authentication still only is attempted against the application's own local user database. The bf.collaboration suite of applications also provides this import capability, but also provides a true integrated LDAP authentication process (see

Figure 1) that allows users in your global directory service to authenticate into bf.collaboration, even if they have not yet been imported.

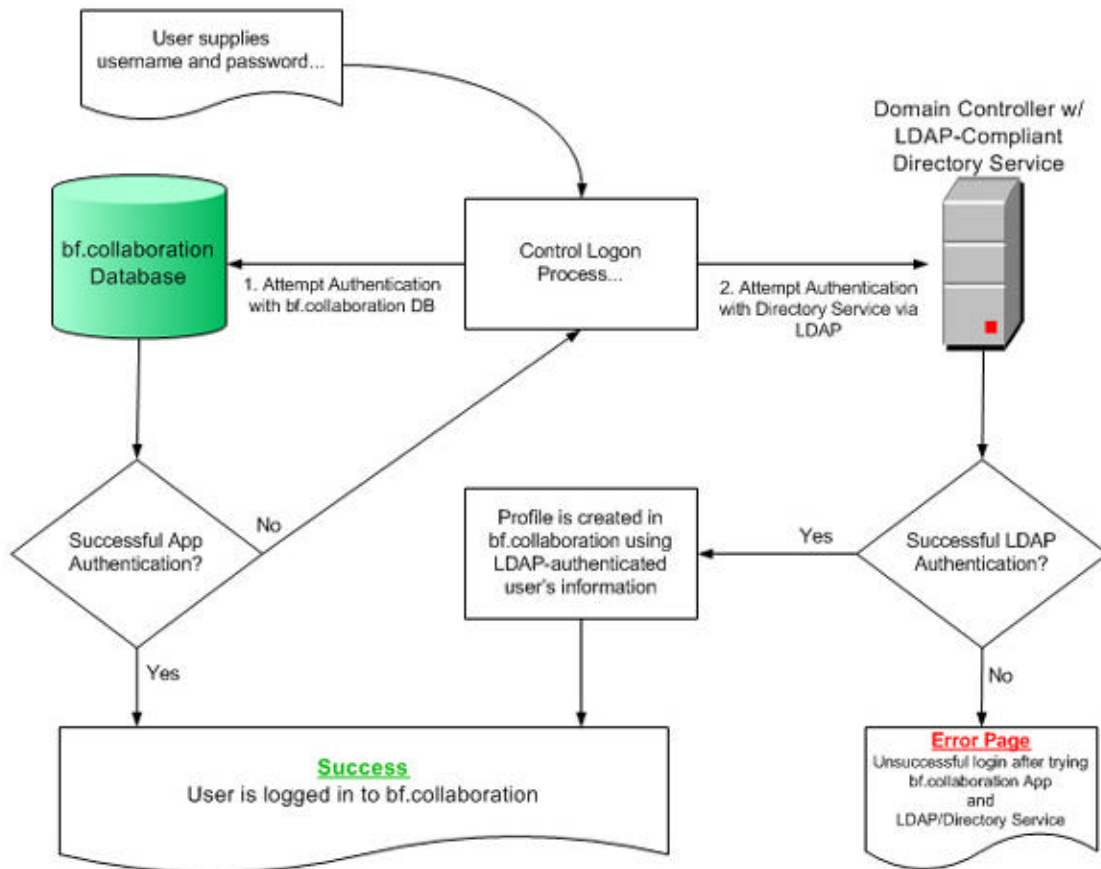


Figure 1: bf.collaboration logon flow diagram

The bf.collaboration logon script first attempts to authenticate the supplied username and password against its own user database. If the username and password cannot be authenticated against the application user database, an attempt is made to authenticate the user against the specified LDAP directory service.

If the user is successfully authenticated with the directory service, the logon script then takes the user's username and email address discovered

from the directory service, and goes back to the bf.collaboration user database and attempts to find the user locally.

If the user is then found in the bf.collaboration application database, they are considered authenticated and let into the application with the credentials afforded of their user profile.

If the user is not found in the bf.collaboration application database, the logon script checks the configuration variable 'AUTOCREATEADUSERS,' and if set to *true*, a user profile is created for the user in the bf.collaboration database, and the user is authenticated into the system.

Conclusions

Enterprise software is supposed to make life easier for your information systems, and the people of your organization. With seamless LDAP integration with your existing directory service – or your future directory service, bf.collaboration adds value to your enterprise information architecture, without the usual side-effects like painful initial user population and multiple logins.