Version 1.0

User's Guide

Contents

Release Notes

Release 1.0

RELEASE 1.0.111216

Initial Release of JBuddy LDAP Gateway

Prior Releases

Please refer to the docs/ReleaseNotes.html or the online version available at http://www.zionsoftware.com/support/jmessageserver/ldap/docs/ReleaseNotes.html for the complete release notes of JBuddy LDAP Gateway.

Introduction

Intended Audience

Welcome to the JBuddy LDAP Gateway User's Guide. This guide is intended primarily for two types of readers:

- System Administrators
- Directory Administrators (LDAP or Active Directory)

System Administrators would typically be involved in preparing the hardware and software environment for JBuddy Server installation and ongoing maintenance and administration. Directory Administrators may be a distinct role within the business or handled by System Administrators. They are responsible for the ongoing support and maintenance of the corporate directory and may want to be aware of how JBuddy LDAP Gateway interfaces with the directory for authentication purposes.

Terms

First a clarification on terms is in order. The JBuddy Message Server solution is also known as 'JBuddy Server.' When the term 'directory' is used in this document, it means Active Directory or LDAP-compatible corporate directories where user account credentials are stored. The XMPP Translation Gateway is known as XTG. XTG proxies a connection from a XMPP IM Client to the JBuddy Server.

Summary

For organizations with an existing directory, the JBuddy LDAP Gateway greatly simplifies user account management. The JBuddy LDAP Gateway runs as a separate service and proxies LDAP Bind requests using simple auth (username & password) to a directory service on behalf of JBuddy Server. With this in mind, carefully read through this document to learn more about JBuddy LDAP Gateway, architecture, security considerations, installation and administration.

Architecture

To make the most of JBuddy LDAP Gateway, it is important to understand the role it plays in a JBuddy Server deployment. The JBuddy LDAP Gateway is a separate service within the JBuddy Server solution and may be run on the same server or a different server depending on the requirements of the organization. See Figure 1. Also see the Security section below for deployment considerations. Additionally, multiple instances of the JBuddy LDAP Gateway may be deployed in environments where redundancy is critical.

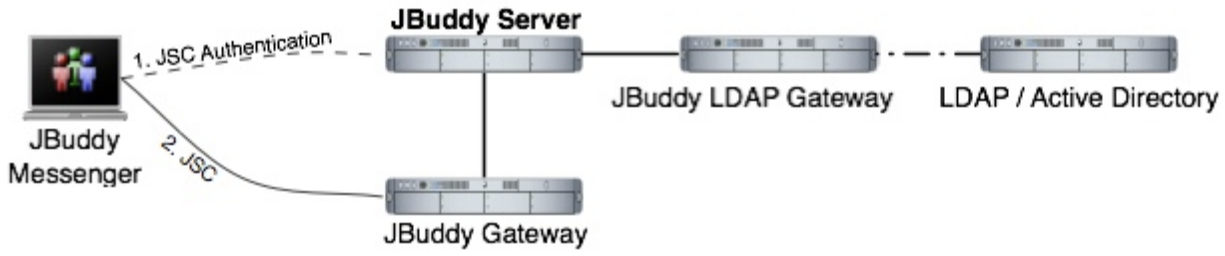

Figure 1: Architecture

JBuddy Server Authentication

If you are only interested in private, enterprise IM using the JBuddy Server, you only need JBuddy IM accounts (even if you intend to connect to the JBuddy Server using XMPP Clients using the XTG). JBuddy IM Accounts can be created one of three ways.

- Automatic
- Manual
- Database bulk load

This guide only covers the Automatic JBuddy IM Accounts since the focus is using the JBuddy LDAP Gateway. Note: **Only the Automatic JBuddy IM Accounts are available for login if the JBuddy LDAP Gateway is used. If the JBuddy LDAP Gateway is not used, only the Manual or Database bulk load created JBuddy IM Accounts are available.**

Authentication with the JBuddy LDAP Gateway

The JBuddy LDAP Gateway version 1.0 is compatible with JBuddy Server version 3.2 and newer and JBuddy Messenger version 3.2.111216 and newer. When used together, the corporate directory becomes the authoritative source for JBuddy IM Accounts and logging into the JBuddy Server. The same username and password used to login to the computer system is available for use in logging into the JBuddy Server.

Automatic JBuddy IM Account Creation

When a JBuddy Messenger user, a JBuddy SDK-enabled application, or a XMPP Client (connecting through the XTG) attempts to login to the JBuddy Server for the first time, the JBuddy LDAP Gateway makes an LDAP Bind request to the corporate directory with the username and password provided by the user. On the first successful LDAP Bind, JBuddy Server automatically creates a JBuddy IM Account in the JBuddy Server's database, based on the username provided. This JBuddy IM Account is owned by the 'Sys Admin' User Profile

provided during JBuddy Server installation. The password for this new JBuddy IM Account is set to a random string to prevent this Account from being used unless the JBuddy LDAP Gateway is available.

Security Considerations

Client Security

Because the JBuddy LDAP Gateway uses simple LDAP bind requests, the user credentials (username and password) are passed unencrypted over the network. It is strongly advised that the JBuddy Message Server be setup to only accept SSL/TLS client requests. See the JBuddy Message Server User Guide for further details.

Server to Server Security

There are two server to server connections that should be secured in order to provide optimum user credential security.

JBuddy Server to JBuddy LDAP Gateway

The JBuddy LDAP Gateway (as well as all the other optional JBuddy Message Server Gateways) locates and connects to the JBuddy Message Server through a Java service called RMI. As part of the JBuddy Message Server installation, a Java RMI service is launched and it typically listens on port 1099 on the same machine as the JBuddy Message Server. Typically optional JBuddy Message Server Gateways will be deployed on the same server as the JBuddy Message Server. Thus the server itself would need to be compromised in order for the communication between the server and gateway to be at risk. The JBuddy LDAP Gateway is provided as a separate installer and therefore could quite possibly be installed on another server, perhaps the server hosting LDAP or Active Directory. Since the JBuddy LDAP Gateway also communicates with the JBuddy Message Server via the Java RMI service the communications path between these services should be as secure as possible. As stated earlier, if they are on the same server, this is generally considered secure unless the machien is compromised.

JBuddy LDAP Gateway and Directory Service

The JBuddy LDAP Gateway connects to the LDAP or Active Directory Service over the network. Since a simple LDAP Bind request is the only available authentication scheme in version 1.0 of the JBuddy LDAP Gateway, this network connection should be secured. Ideally the JBuddy LDAP Gateway will connect to the LDAP or Active Directory Service over a SSL/TLS secure channel. A second option to secure communication between these services would be to install the JBuddy LDAP Gateway on the same machine as the LDAP or Active Directory server. In this way, the communication would be secure as long as the server was not compromised. The preferred method is of course to connect using a SSL/TLS secure channel to the LDAP or Active Directory Service.

Installation

Choice of Installer

The JBuddy LDAP Gateway is available for installation in two forms:

- Within the JBuddy Server installer as an optional install pack

- As a separate JBuddy LDAP Gateway installer

In the first installer form, the JBuddy LDAP Gateway is installed on the same server as the JBuddy Server. In the second installer form, the JBuddy LDAP Gateway alone is installed. This is the form that should be used if you wish to install the JBuddy LDAP Gateway on a different server than the JBuddy Server such as on the same machine as the directory service. The JBuddy Message Server User's Guide briefly describes installation in the first form. This guide will cover the second form of the installation in more detail. The configuration fields used by both installer forms are the same.

System Requirements

To run the JBuddy LDAP Gateway installation program as well as the gateway itself, you must have at least Java Standard Edition (JSE) version 1.4.2.x or newer installed. Note: JSE version 1.4.2.x and version 5.0.x have reached 'end of service life' with support only available for Java for Business subscribers (paying support to Oracle). If you plan to enforce SSL login and message encryption, you must have JSE 5.x or newer installed before running the server and gateways. **We have tested with Oracle's JSE. We have not validated with other versions of Java such as IBM JRE or the OpenJDK project.** The installer as well as the gateway are written entirely in Java and should therefore run on any modern, operating system supported by Oracle's JSE. That said, the startup and shutdown scripts and any operating system 'services' used to launch, monitor and shutdown the gateway utilize native library called Java Service Wrapper (JSW) version 3.2.0 to facilitate better native operating system integration such as with Windows Services. JSW version 3.2.0 was released with an open source license friendly to commercial software. This version includes 32-bit native wrappers for Windows x86, Linux x86 and PPC, and Solaris SPARC. Newer JSW versions and 64-bit versions are available directly from Tanuki Software http://wrapper.tanukisoftware.org/ however, Zion does not offer support for newer JSW versions at this time. If necessary, the JBuddy LDAP Gateway can be operated without the startup / shutdown scripts by passing the proper arguments directly to the JVM from a script, command shell or terminal. Instructions for custom JSW library compilation and non-JSW startup/shutdown are beyond the scope of this guide.

Installing Java

For best performance and scalability, we recommend using the full featured JSE 6.x or 7.x obtainable from Oracle at http://www.oracle.com/technetwork/java/javase/downloads/index.html. The JSE supports the -server flag which is the default and intended use of JBuddy LDAP Gateway. Further, you should select the 32-bit version of JSE if you are running on a 32-bit OS and the 64-bit JSE if you are running on a 64-bit OS. A 32-bit version of JSW should not prevent you from running 64-bit JSE.

Which Java

During installation, if the Installer encounters more than one Java environment, it will make a 'best guess' on which Java environment to use. It updates .conf files located in the conf directory. Near the top of these files it sets the property 'wrapper.java.command=$JAVA_HOME/bin/java' and then a little lower it updates the classpath wrapper.java.classpath.1= $JAVA_HOME/lib/tools.jar.' The $JAVA_HOME variable is replaced with the 'JAVA_HOME' that the Installer believes is the correct version. If you wish to use a different Java, you will need to edit the values above. The -server flag is enabled by default for performance reasons. The JRE available from www.java.com does not support the -server flag, therefore we recommend the JSE over the JRE. You can determine if your JVM environment supports the -server flag by

typing the following in a command shell or terminal: `java -server -version` which should tell you the version of java used as well as if it is the server or client version of the virtual machine.

Command Line Installation

Initially you will need to run the installation on a computer with a graphical interface (see Launching the Graphical Installer below). At the end of the installation, you will be prompted if you wish to save the installation as a XML installation script which can be used later for an automated (non-graphical) installation such as on a remote Linux or unix-based server. If this is your situation, you need to enter information applicable to the remote host when prompted during the Installer. To run a headless installation, copy the installer jar file and xml install script (that you chose to save at the end of the GUI install) to the remote host. Then login to the remote host and from a command shell or terminal, enter the following command:

`java -jar JBuddyLdapGatewayInstaller-1.0.xxxxxx.jar JBuddyLdapGatewayInstallScript.xml` where the JBuddyLdapGatewayInstallScript.xml is whatever name you saved at the end of the GUI install.

Graphical Installation

After a modern JSE is properly installed, double click on the JBuddyLdapGatewayInstaller-1.0.xxxxxx.jar file to launch the installation program. If you prefer, you can launch the Installer by simply entering the following from a command shell or terminal: `java -jar JBuddyLdapGatewayInstaller-1.0.xxxxxx.jar`. Once launched you should see a small Language Selection dialog appear similar to Figure 2 below:

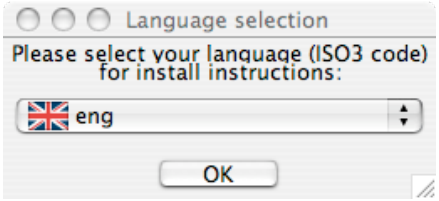

Figure 2: Installer Language Selection Dialog

After selecting eng (English) language and clicking OK, the Installation Welcome window appears similar to Figure 3:

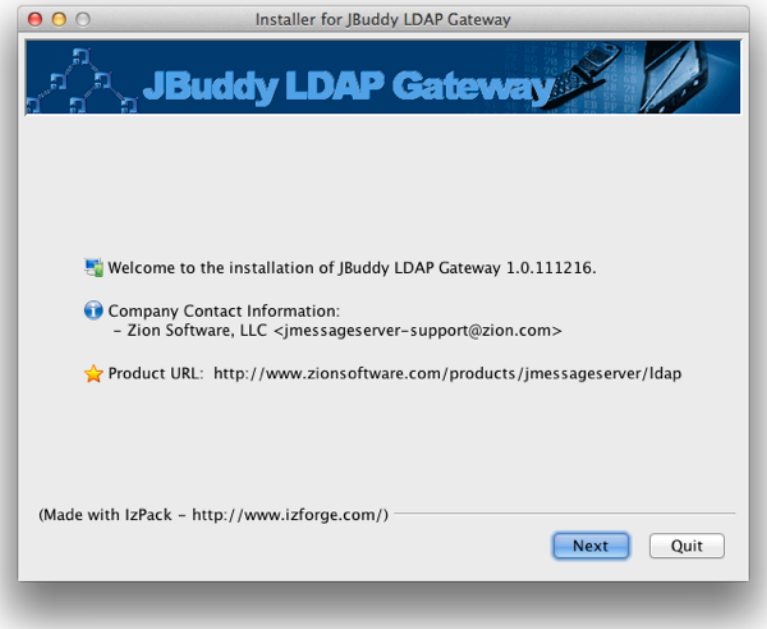

Figure 3: Installation Welcome

After clicking Next, the Installation Information window appears similar to Figure 4:

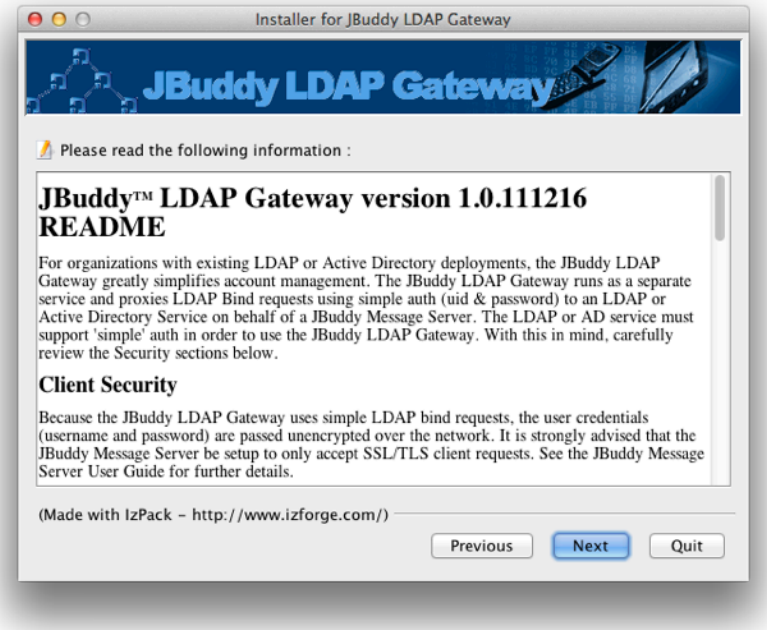

Figure 4: Installation Information

After clicking Next, the License Agreement window appears similar to Figure 5. You must accept the terms of the license agreement before the Next button will be enabled.

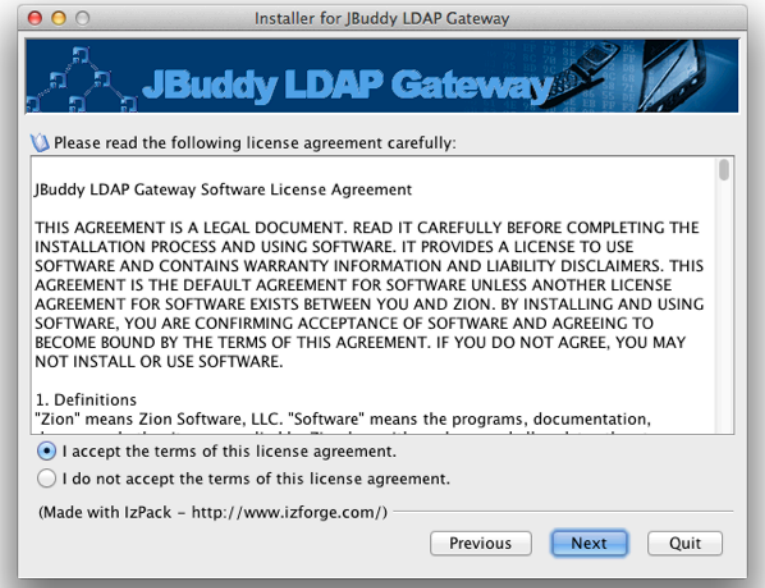

Figure 5: Installation License Agreement

After accepting the license agreement terms and clicking Next, the installation path must be specified as in Figure 6 below. Once Next is chosen a Message dialog appears to inform you that the directory will be created (or if it already exists.)

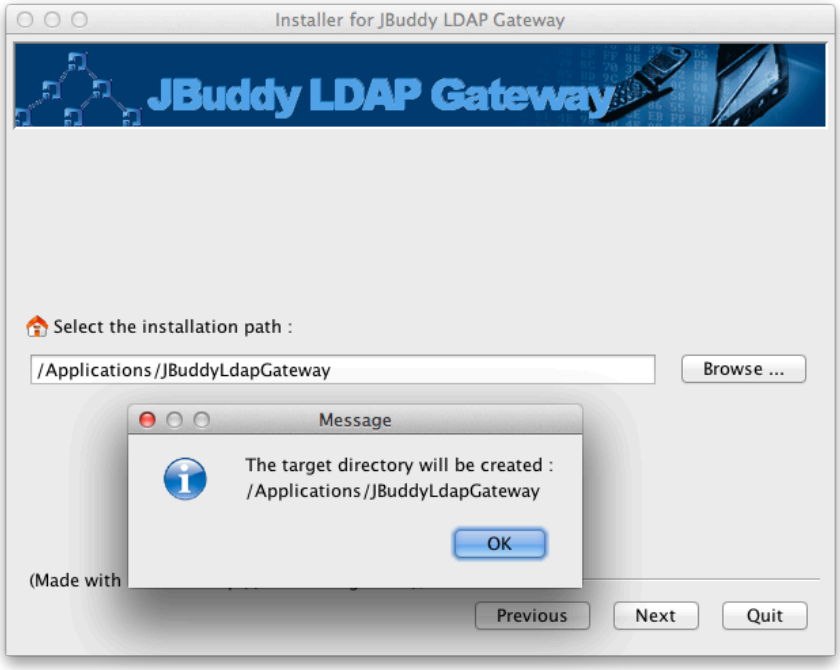

Figure 6: Installation Location

After clicking OK to the Message dialog, the Package Selection window will appear similar to Figure 7:

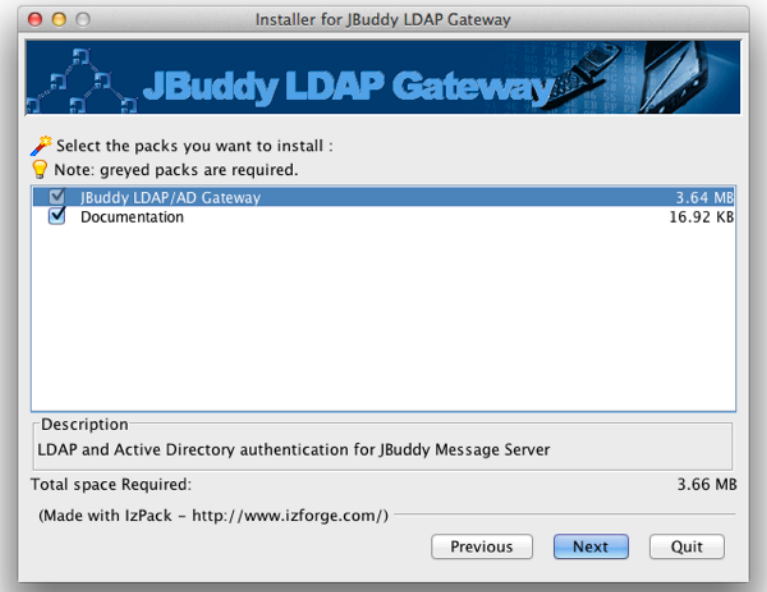

Figure 7: Installation Package Selection

The Package Selection window shows mandatory and optional “packs” that can be installed. Clicking an individual pack changes the description shown. Once you are satisfied with your packs selection, click Next to continue.

The Hosts Configuration window will appear similar to Figure 8 below. JBuddy Server Host is the hostname, IP address, or fully qualified domain name of the machine where JBuddy Server is available for the JBuddy LDAP Gateway to connect. The LDAP Service URI should be left blank if the LDAP DNS SRV records are available (often true for Active Directory). Otherwise, provide the host, IP address or a full uri to reach the directory service.

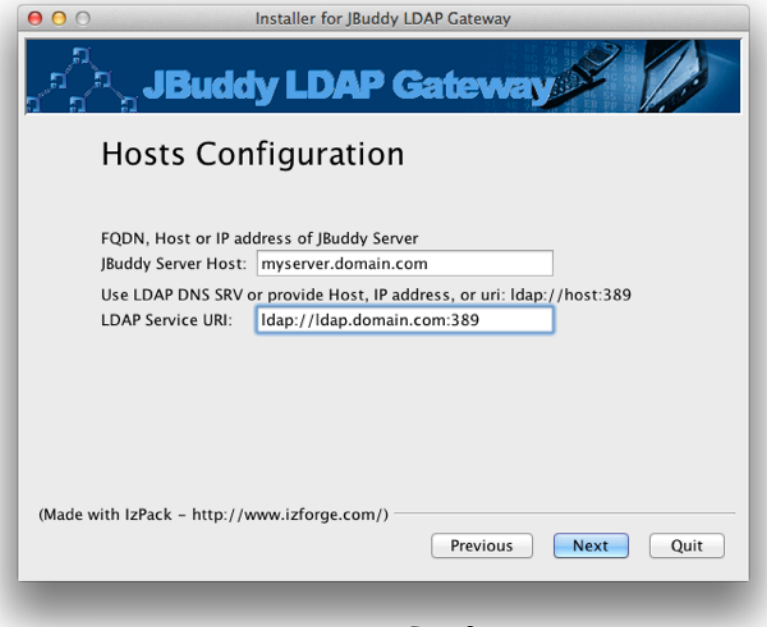

Figure 8: Hosts Configuration

After clicking Next, the Active Directory / LDAP Configuration window will appear similar to Figure 9 below. This window supports basic configuration for both Active Directory and LDAP.

Active Directory

Often, the only field required for Active Directory configuration is the first one. Provide the domain for the Active Directory. See Figure 9 below.

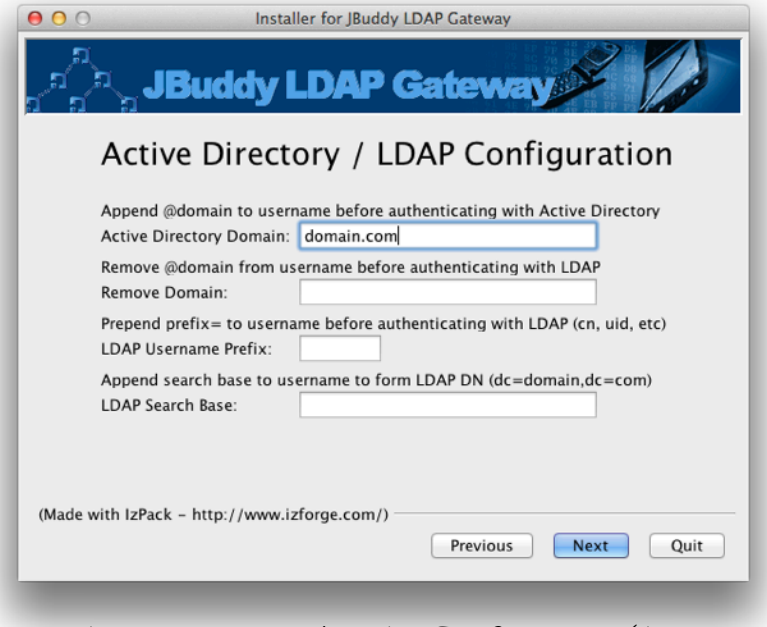

Figure 9: Active Directory / LDAP Configuration (AD example)

LDAP

For LDAP, often the username does not contain @domain.com, however in order to leverage the new DNS SRV support allowing the JBuddy client to find the JBuddy Server without troubling the user to provide the host and port, a domain must be appended to the username at the client. In order to successfully authenticate with an LDAP directory, this domain must usually be removed from the username prior to attempting to authenticate with LDAP. The third and fourth fields on this configuration window also pertain primarily to LDAP configurations. The third field allows the administrator to define the attribute that is prepend to the username prior to authenticating with LDAP. The fourth (and last) field allows the administrator to specify the remaining portion of the LDAP DN (the search base). An example is given below illustrating how the second, third and fourth fields combine to modify the username prior to authenticating with the LDAP directory: username = *jack.frost@domain.com*

Remove Domain: *domain.com*

LDAP Username Prefix: *uid*

LDAP Search Base: *dc=domain,dc=com*

username sent to LDAP: *uid=jack.frost,dc=domain,dc=com*

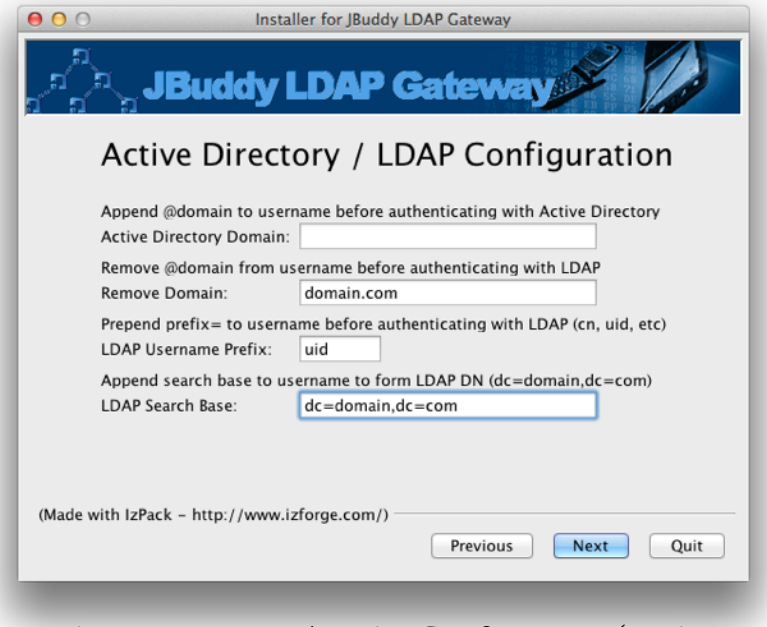

Figure 10: Active Directory / LDAP Configuration (LDAP example)

After providing the values specific to your organization and directory type (Figure 9 Active Directory, Figure 10 LDAP) for directory, click the Next button to proceed to the installation window. See Figure 11 below.

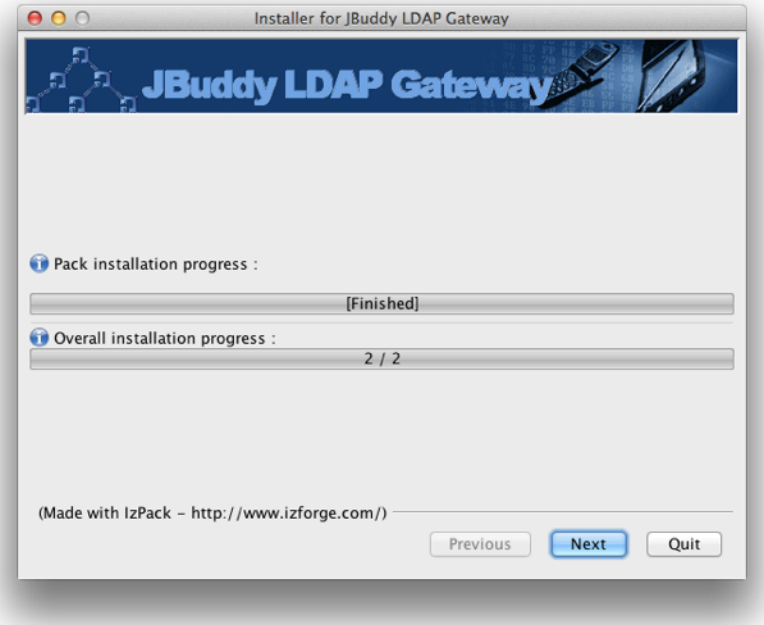

Figure 11: Installation window

After the installation window is finished, click the Next button to proceed to the Post-Processing window. On non-Windows installation, the Post-Processing window will appear but no post-processing needs to be done (see Figure 12.) On Windows installations, the installer attempts to

register JBuddy LDAP Gateway as a Windows Service. The Post-Processing window will display log messages as the post-procesing proceeds (successful or errors). Click the Next button to proceed to the final installer window (see Figure 13.)

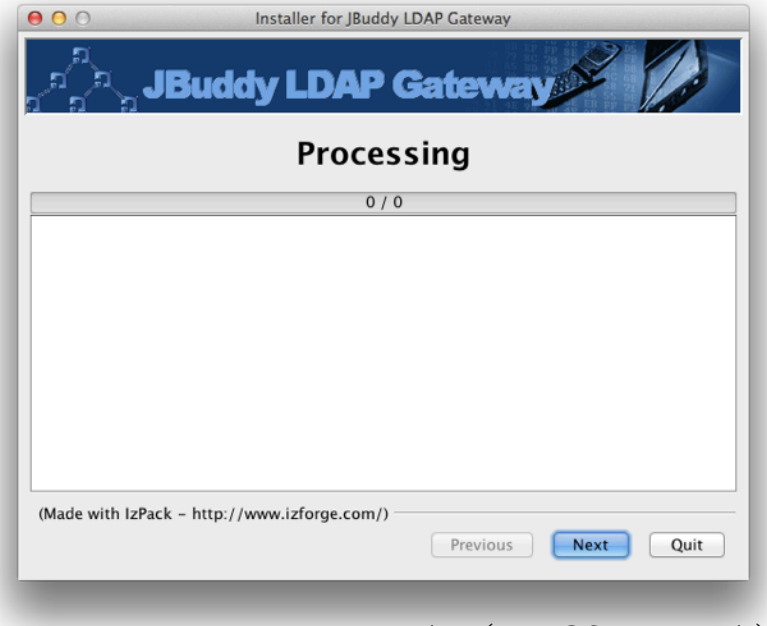

Figure 12: Post-Processing Window (Mac OS X Example)

On this final screen of the graphical installer, you may save the installation script for use with a headless install, described in the Command Line Installation section above or click Done to close the Installer.

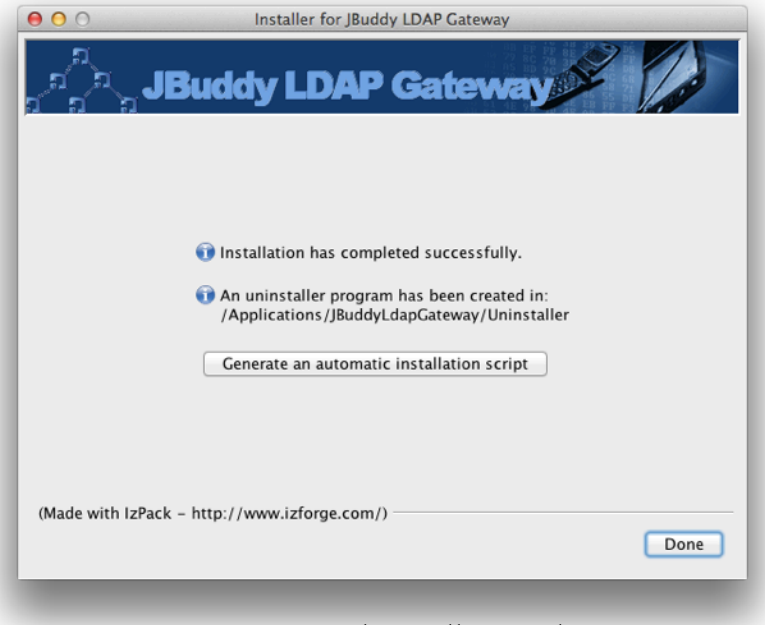

Figure 13: Final Installer window