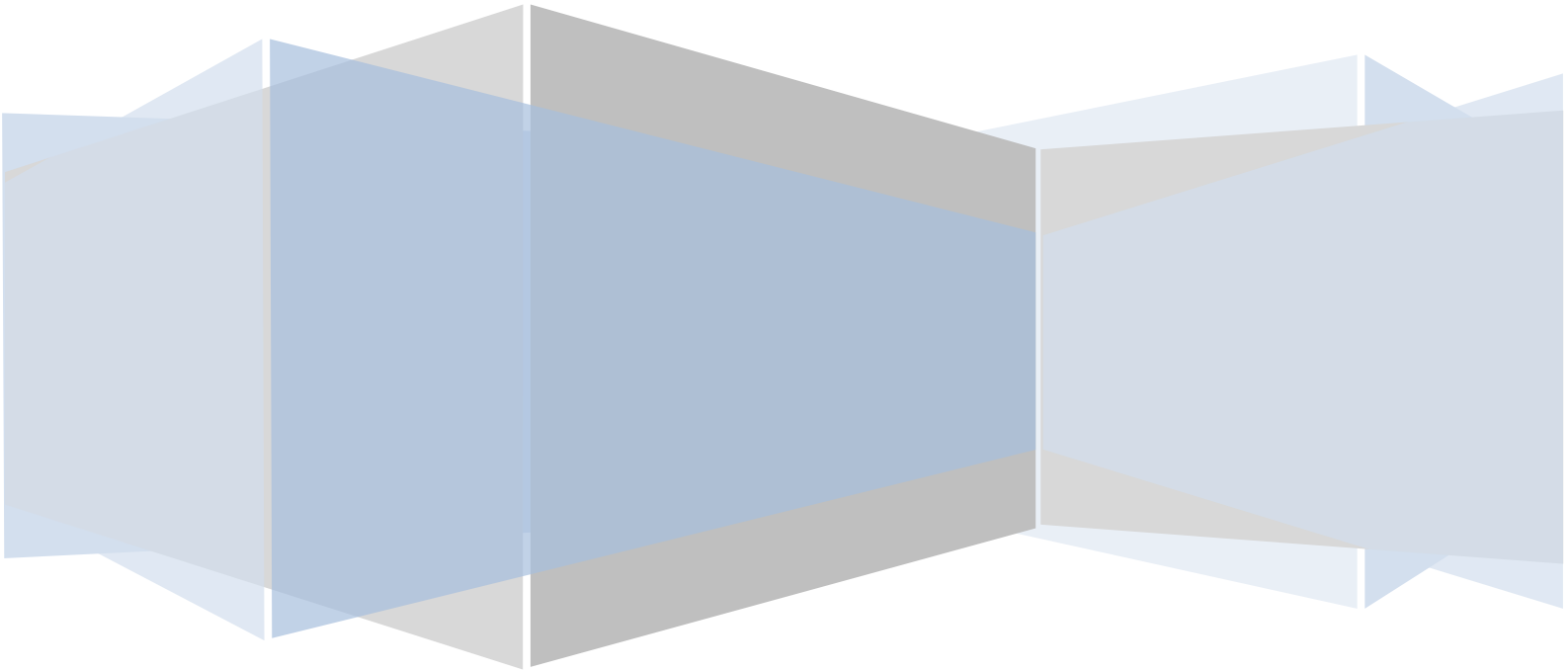
Configuring BMC AREA LDAP

Using AD domain credentials for the BMC Windows User Tool

Version 1.0



Introduction

This following document describes the basic configuration for the BMC AREA LDAP plugin. This should only be considered if the customer wants to use their domain username and password, not utilising SSO, through the BMC Windows User Tool.

LDAP Basics

The following section describes common terms used by AD/LDAP associated with the BMC AREA plugin.

What is LDAP and why use it?

LDAP is a lightweight protocol for accessing information in a Directory Service (Lightweight Directory Access Protocol). It is used by many Groupware, Middleware, and OS vendors that store data in what can be called an LDAP database, or rather a data repository that can be accessed via the LDAP protocol. There are many different LDAP client tools that exist for the purpose of accessing and administering an LDAP database. Active Directories, Novell Directory Services, SunONE, and many other products support LDAP. If you are using an LDAP compliant product to store user information, then the AR System can be configured to make use of that data for authentication and other purposes.

What does it mean to “Bind” in LDAP?

An LDAP “Bind” is the equivalent to a ‘Login’. To bind, you provide a valid Directory Service account name and password.

What is an “Attribute” in LDAP?

An attribute in LDAP is a structure used to hold data. In some ways, an attribute is like a column in a database. However, within a database, columns are defined in a certain way. There is a data type associated with a column. Attributes are different than database columns in that they can be multi-valued. They are defined based on attribute syntax, which is like a set of rules that tells the LDAP server what type of data is being stored. In this way, the LDAP server can make comparisons between different types of data.

What is a BaseDN in LDAP?

A BaseDN is essentially a location in the LDAP Directory Service. In LDAP, data can be presented in a hierarchical tree structure. So the BaseDN is the level of this structure at which you will begin looking for your data. Literally, BaseDN means the Distinguished Name of the Base (location in the tree to begin).

Within the BMC AREA LDAP Configuration form, this value is represented as the “User Base” in the “User and Group Information” section.

What is a Bind User?

This is a user account within the AD/LDAP that can query the repository for any existing users.

What is the User Search Filter?

What needs to be specified here is a valid LDAP filter that is used to identify a user's unique LDAP object, based upon the value they provide in the BMC Windows User Tool login prompt. The most common way to uniquely identify a user in LDAP is by their username. It takes an LDAP Administrator or one of the LDAP tools to query the LDAP database to determine the name of the object that will uniquely identify a user. Once this object is identified, the object is equated to a keyword based upon the value the users provide in the Windows User Tool prompt. The object equalling the keyword makes the value for the User Search Filter.

$\USER$ is the keyword to get the value entered by the user at the login prompt.

For example, in Microsoft Active Directory, you can often use the "samAccountname" object since it normally is the value for the username. Here is what the User Search Filter value would look like for this example:

samAccountname=$\USER$ or cn=$\USER$

This is a common example that applies to Active Directory only. Any object in LDAP that uniquely identifies the user can be used. The format would be:

<object name>=$\USER$

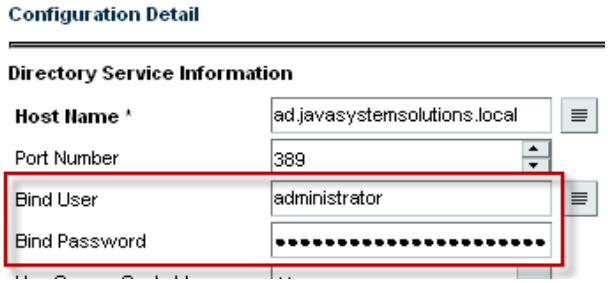
What is the default port for LDAP and can it be changed?

The default port for LDAP is TCP 389 but this can be changed. The BMC article KA336513 describes how to change it.

How a user is authenticated using the BMC AREA LDAP plugin?

The AREA LDAP plug-in performs the following steps to authenticate a user:

- The Plug-in “binds” as the “Bind User” defined in the Directory Service Information section of the AREA LDAP Configuration form. This is typically a user who can query the AD/LDAP repository.



- The Plug-in performs a query in the LDAP database using the values for the Host Name, Port Number, User Base, and User Search Filter in the AREA LDAP Configuration form.

- If a user in not found, return an invalid user error, otherwise continue.
- The Distinguished Name and all available attributes for the user are returned to the Plug-in.
- The Plug-in then performs another “bind” as the Distinguished Name found in the previous step with password passed from the BMC Windows User Tool.
- If Bind fails, return a bad password error (ARERR 329), otherwise the AR Server is informed that the user is successfully authenticated.

Installation and Configuration

The following sections describe the installation and configuration steps to enable the BMC AREA Ldap plugin with the JSS SSO Plugin.

Step 1 – The BMC AREA LDAP Configuration form

The following section describes the minimum values needed to enable this BMC feature. Login to the application via the Windows User Tool or Mid Tier as an administrative user.

From the application list, select the AR System Administration Console

Select System > LDAP > AREA Configuration

Field	Possible Values
Host Name	This is the host name of your AD/LDAP controller. E.g. ad.javasystemsolutions.local
Port Number	The default is 389
Bind User	This is a user name configured in the AD/LDAP who has the permissions to query the repository
Bind Password	The domain password for the account above
User Base	You can ask your AD administrator for this namingContext or you could following this section to utilise the ldp.exe
User Search Filter	There are typically two possible values for this field. Use one and test. **samaccountname=$\USER$** or **cn=$\USER$**
Group Membership	No
Use Secure Socket Layer	No
Failover Timeout	120

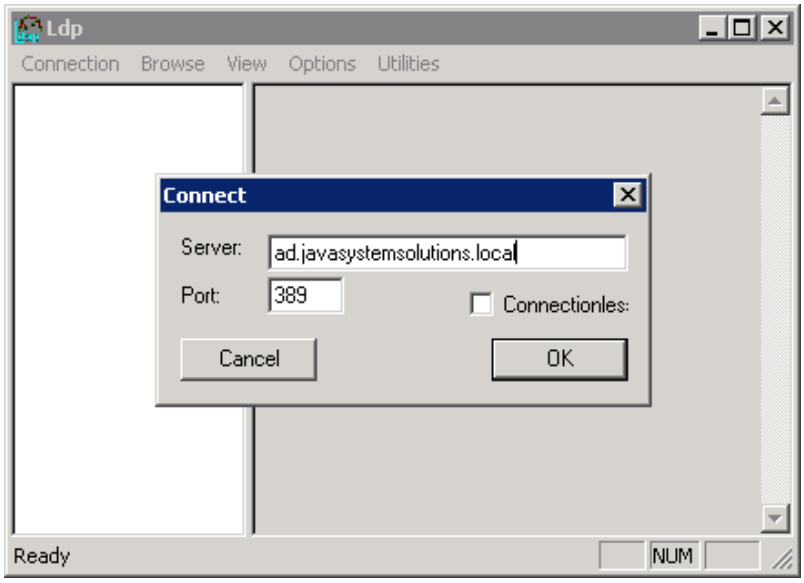
Chase referral	Yes

Using ldp.exe to find the BaseDN / User Base

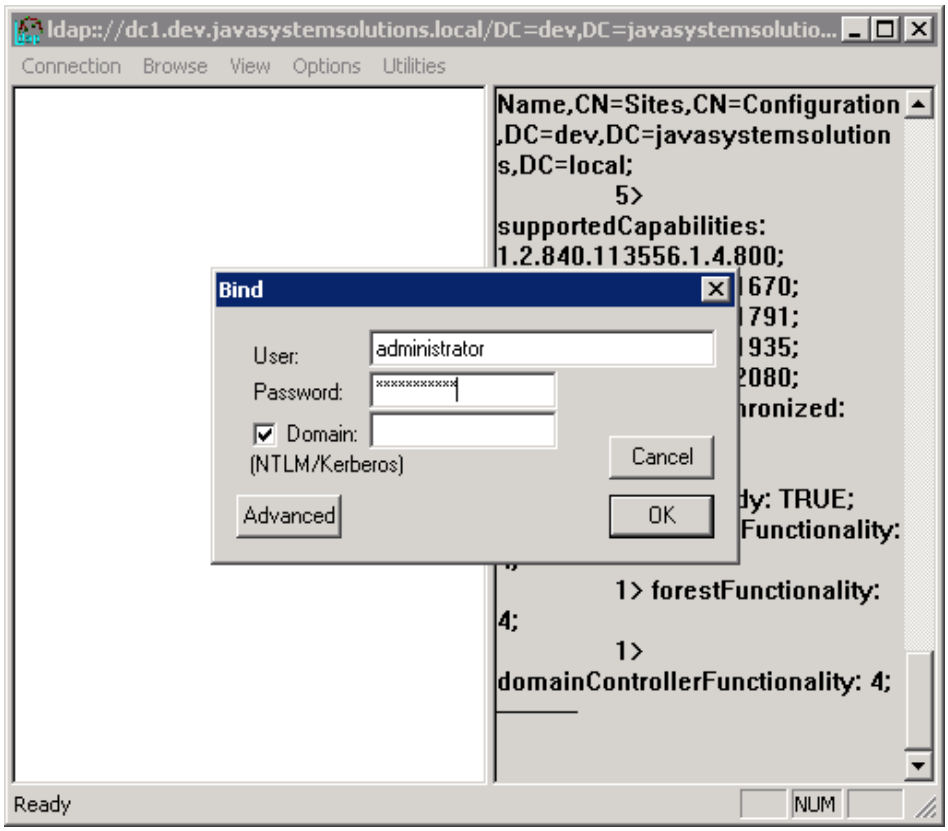
Download the ldp.exe from the following URL

http://www.javasystemsolutions.com/downloads/ldp.exe

Select Connection > Connect from the menu.



Once you select OK, from the menu, select Connection > Bind and fill in the details from your Bind User and Bind Password

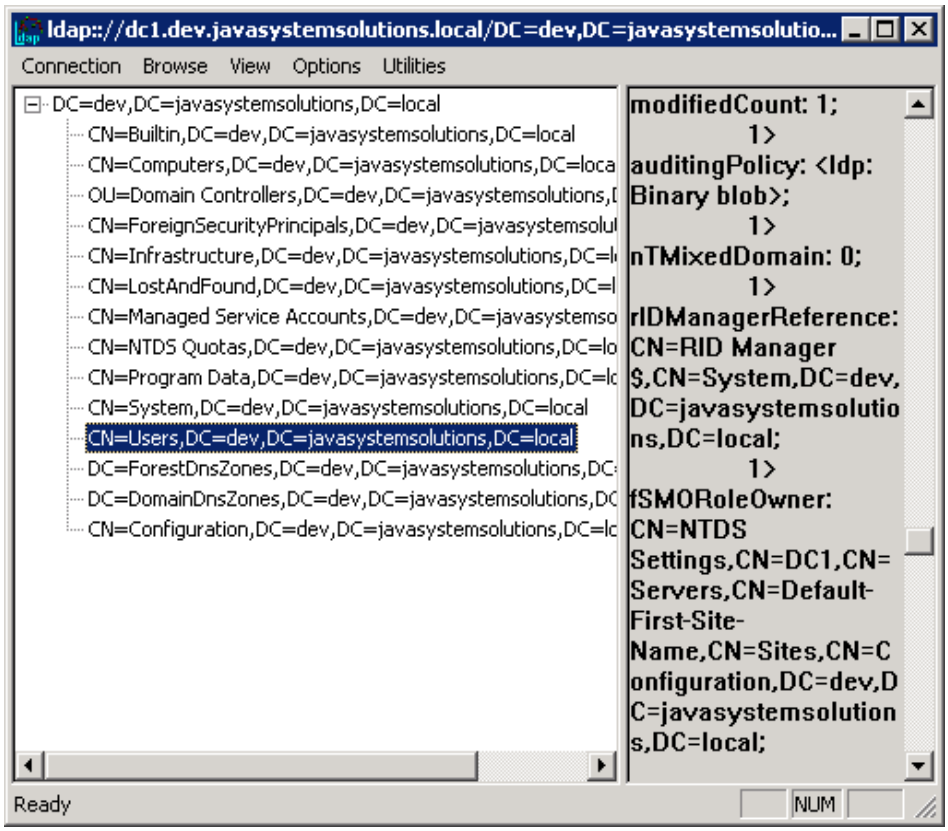


Then from the menu select View > Tree

A BaseDN box will appear, just select OK

A tree will appear on the left pane. Expand the selection

Look for the selection that is most likely to have the users.



The highlighted area will be the BaseDN / User Base for the AREA LDAP configuration form.

Step 2 – Configuring the ar.cfg/conf

Open the ar.cfg (Windows) or ar.conf (LINUX or UNIX).

Verify the arealdap.dll (Windows) or arealdap.so (LINUX or UNIX) is present and configured to use the BMC AREA HUB. The following rules must be applied and checked.

- Areahub is configured. This can be verified by the typical line:
    - Windows
        - Plugin: “/pathToARSystemInstallation/arealdap/areahub.so”
    - LINUX/UNIX
        - Plugin: “C:\Program Files\BMC Software\AR System\arealdap\areahub.dll”
- JSS SSO Plugin is configured to be the first AREA-Hub-Plugin within the ar.cfg
    - Starting from the top of the file, the first instance of AREA-Hub-Plugin must contain the jss-sso.dll (Windows) or jss-sso.so (LINUX or UNIX)
    - Windows
        - **AREA-Hub-Plugin**: “/pathToARSystemInstallation/arealdap/areahub.so”
    - LINUX/UNIX
        - **AREA-Hub-Plugin**: “C:\Program Files\BMC Software\AR System\arealdap\areahub.dll”
    -
- BMC AREA LDAP plugin configured after the JSS SSO Plugin
    - Starting from the top of the file, the after the instance of SSO Plugin.
    - Windows
        - **AREA-Hub-Plugin**: “/pathToARSystemInstallation/arealdap/arealdap.so”
    - LINUX/UNIX
        - **AREA-Hub-Plugin**: “C:\Program Files\BMC Software\AR System\arealdap\ arealdap.dll”

Step 3 – Verifying the configuration.

All plugins will report to the AR Server arplugin log. Login to the application via the Windows User Tool or Mid Tier as an administrative user.

From the application list, select the AR System Administration Console

Select System > General > Server Information > Log

Select the arplugin log and set the Plugin Log Level to ALL.

The AR server will need a restart.