



Using Firefly v5 with Windows 2003 Active Directory

Initial Release Date: 22nd April 2008

Document Modification Date: 22nd April 2008



Introduction

Firefly Web Server has a pluggable user management system using JAAS (Java Authentication and Authorization System). It can therefore be used with many different user management technologies. One of the most popular, particularly in the Microsoft Windows environment is Active Directory (AD).

This document outlines the settings that are needed to make Firefly work with AD. It is assumed that you have a reasonable understanding of AD security management. If this is not the case, please refer to <http://msdn.microsoft.com> where you will find many articles on the subject.

Assumptions

You are running the following technology:

- Windows 2003
- Tomcat 5.5 or upwards
- Java 1.5 or upwards

Background

Firefly Web Server uses Profiles to manage privileges. The name of the Profile is used to match a user to the correct set of privileges. When running Firefly Web Server with AD, the following steps occur:

1. The username/password are passed to our login module for authentication
2. The login module uses LDAP protocols to connect to AD.
3. The login module queries AD to find the user account information
4. If the login is successful, the login module queries AD to find the group information for that user
5. The list of groups for that user are then matched, by name, to Profiles in Firefly Web Server
6. If the Group name in AD is the same as the Profile name in Firefly Web Server, the user login is associated with that Profile and given the applicable privileges. If the user has multiple Group names that match with a Profile, the first Profile is used – we do not mix profile privileges.

Setting up Firefly Web Server

It is assumed that you have a working installation of Firefly Web Server already installed. If this is not the case, please refer to the Firefly Web Server installation guide as the full installation is not covered in this document. To set up Firefly Web Server to use Active Directory, you need to do the following:

1. Open C:\Program Files\Apache Software Foundation\Tomcat 5.5\webapps\sparkstudio5\WEB-INF\classes\server_settings.xml with Notepad.
2. Change the **Server.authenticationMode** setting value to **tomcat-ldap** (it's SparkStudio by default)
3. Change the **Server.authenticationAppserver** setting value to **tomcat** (it's also SparkStudio by default)
4. You may also wish to change the **Server.defaultAdminProfileName** setting value to the name of the AD Group that will be used to identify the Administrator for Firefly Web Server. It is



admin by default. The value here must match the name of a Group in AD – i.e. the Group that has Administrator rights.

Configuring the LDAP Login Module

As our user management system is pluggable, you can create and use your own login modules. As part of the standard product, we provide a number of login modules for your convenience – in particular the LDAP Login Module which is used to connect to AD.

The configuration file for this module is located at:

C:\Program Files\Apache Software Foundation\Tomcat 5.5\webapps\sparkstudio5\WEB-INF\classes\com\informavores\settings\ldap.properties

This file can be opened using Notepad and has the following settings:

Property	Example values	Definition
LDAPPopulateRoles	true / false	Determines if the user roles should be populated. This value should always be set to 'true'.
LDAPContextFactory	com.sun.jndi.ldap.LdapCtxFactory	The context factory used to connect to LDAP. LdapCtxFactory is the standard factory used by Java.
LDAPUserKey	cn	The LDAP key used to identify the user account. This is used for filtering by the login username entered by the user.
LDAPAuthenticationType	simple	Determines the authentication type for the context. This value should always be set to 'simple'.
LDAPRoot	ou=MyCompany, dc=mycompany, dc=com	This is a standard LDAP query for defining the LDAP sub-tree location.
LDAPServerUrl	ldap://mycompany.com:389	The URL for the AD server.
LDAPPasswordKey	unicodePwd	The location of the password field. This value should always be 'unicodePwd'.
LDAPUserSuperContext	ou=MyCompany, dc=mycompany, dc=com	This is a standard LDAP query for defining the LDAP sub-tree location.
LDAPGroupObject	objectcategory\=group	The group object category that will be used to filter the correct group object. This value should always be as shown.
LDAPUniqueMember	member\=	The unique member used to find the listing of groups.

* Note: the '=' symbol needs to be escaped with a '\' character in all cases.



For most users, the following settings should be used:

```
LDAPPopulateRoles=true
LDAPContextFactory=com.sun.jndi.ldap.LdapCtxFactory
LDAPUserKey=cn
LDAPAuthenticationType=simple
LDAPPasswordKey=unicodePwd
LDAPUniqueMember=member=
LDAPGroupObject=objectcategory\=group
```

And the following should be altered appropriately:

```
LDAPRoot=ou\=MyCompany,dc\=mycompany,dc=com
LDAPServerUrl=ldap://mycompany.com:389
LDAPUserSuperContext=ou\=MyCompany,dc\=mycompany,dc=com
```

Once you have edited the file, simply save it to the same location.

Finishing

Once all of the above settings have been configured, you will need to restart the Apache Tomcat service. In addition to this, you will likely need to:

- Create a number of Profiles in Firefly Web Server with the appropriate privileges – you'll need to log in as Administrator to do this
- Create Groups in AD with the same name as the above Profiles
- Make users Members of the appropriate AD Group

Troubleshooting

If you are having difficulties logging into the server, you can do the following

1. Open C:\Program Files\Apache Software Foundation\Tomcat 5.5\webapps\sparkstudio5\WEB-INF\classes\log4j.properties using Notepad
2. Add the following line at the bottom of the file (which will tell our software to output debug messages):

```
log4j.logger.com.informavores=debug
```

3. Restart the Apache Tomcat service
4. Attempt to log into Firefly Web Server
5. Go to C:\Program Files\Apache Software Foundation\Tomcat 5.5\logs and open the latest .log file starting with **stdout_**
6. Go to the bottom of the file and work your way backwards through the messages to see if there are any errors.

If you see anything you do not understand, please contact support@informavores.com.