

Plexcel Joomla! Plugins Manual

Table of Contents

Change Log.....	1
Requirements.....	2
Installation.....	2
Install Prerequisites.....	2
Install the Plugins.....	2
Method 1: Use the 'Install from URL' option.....	2
Method 2: Use the 'Upload Package File' option.....	2
Enabling the Plugins.....	3
Disabling New Account Creation.....	3
Securing the Login Form.....	3
Username Canonicalization.....	4
Windows Group Based Access Control.....	4
Automatic Contact Creation.....	5
Diagnosing Errors.....	5
Patching Old Versions of Joomla! for Special Characters in Usernames.....	5
Joomla! 1.5 FTP Directory Permissions.....	7

This document describes requirements and the installation procedure for the Plexcel Joomla! 1.5 plugins.

IMPORTANT: The Plexcel Joomla! Plugins require the Plexcel PHP extension which is a separate package. You must install the Plexcel PHP extension before enabling these plugins.

Change Log

2.1.1 Sep 22, 2009 – This document has been completely reviewed and updated to reflect the most current information regarding the Plexcel Joomla! Plugins and the latest version of Joomla!.

2.1.0 Oct 7, 2008 – Added automatic creation of Contact entries (disabled by default), improved plugin configuration parameter descriptions, suppressed meaningless administrative login error message with SSO plugin enabled and improved documentation regarding automatic contact creation, securing the login form and disabling the creation of new accounts.

2.0.2 Mar 27, 2008 – The plugin will now fail with a detailed error message if the Plexcel PHP extension is not installed and loaded.

Requirements

The following requirements must be satisfied for the Plexcel Joomla! 1.5 plugins to work.

- Joomla! 1.5
- The Plexcel PHP extension also from IOPLEX Software. Plexcel has the following requirements.
 - Linux or FreeBSD on i386 or x86_64
 - PHP 5.0, 5.1 or 5.2
 - Apache 2 (with HTTPS for secure login form)
 - Browsers that support Kerberos SSO (e.g. Internet Explorer, Firefox, ...)
 - Installer must have sufficient AD privileges to create the HTTP service account
 - Linux web server must have valid entries in DNS
 - SELinux must be sufficiently disabled
 - Apache must run in a UTF-8 locale to support internationalized text
 - Time on all machines must be synchronized (e.g. using NTP)

For detailed Plexcel requirements and installation instructions please see the Plexcel Operator's Manual.

Joomla! 1.0 is not supported. Only Joomla! 1.5 has the necessary plugin "hooks" to properly support these authentication mechanisms.

Installation

Install Prerequisites

Install Apache 2, PHP and MySQL. These packages should be installable from your package manager (e.g. yum on Red Hat Linux, apt-get on Ubuntu, etc).

Install Plexcel. See the Plexcel Operator's Manual for details.

Install Joomla! 1.5.

Install the Plugins

Install the three Plexcel Joomla! 1.5 Plugins. There are two slightly different methods for doing this.

Method 1: Use the 'Install from URL' option

If your web server has direct access to the Internet, you may use the Joomla! plugin page to download and install the plugins directly from the IOPLEX Software website.

Specifically, login to the Joomla! Administrator area, select *Extensions > Install/Uninstall* and enter your FTP *Login Details* (if necessary). Then copy and paste the first of the below URLs into the *Install from URL* field and click *Install*. If successful, do the same for each of the other plugins.

<http://www.ioplex.com/d/plexcel-joomla-auth.zip>
<http://www.ioplex.com/d/plexcel-joomla-user.zip>
<http://www.ioplex.com/d/plexcel-joomla-sso.zip>

Method 2: Use the 'Upload Package File' option

If method 1 is not suitable (e.g. because a proxy server is in the way) you will need to do download and extract the following package:

<http://www.ioplex.com/d/plexcel-joomla-2.1.0.zip>

Within this package are the individual Joomla! 1.5 plugin .zip files.

Go to *Control Panel > Extensions > Install/Uninstall* and enter your FTP Login Details (if necessary). Enter the path of the first plugin .zip file into the *Upload Package File* field and click install. Do the same for the other plugins.

Note: If you get a *JFTP::write: Bad response - Unable to write entry* error trying to install from a zip file, make sure you are installing the individual zip files *within* the *plexcel-joomla-2.1.0.zip* file and not that file itself.

Enabling the Plugins

To enable the Plexcel Joomla! Plugins visit *Control Panel > Extensions > Plugin Manager* and enable the plugins below by clicking on the red X for each.

Authentication - Plexcel Active Directory Authentication
User – Plexcel Active Directory Authentication
System - Plexcel Active Directory Single Sign-On (SSO)

Note: If you get an error "Call to undefined function *plexcel_log()*", the Plexcel extension is not enabled. As described in the Requirements and Prerequisites sections, you must first install, enable and verify that the Plexcel PHP extension is working correctly.

The Plexcel Joomla! Plugins should now be fully functional. When a user visits the site they should automatically login without entering their credentials. They should be able to logout and enter alternative credentials. Using either authentication method for the first time should also automatically create accounts with information populated from AD (e.g. their full name and email address).

Note: New users may need their browsers to be configured for automatic login (e.g. by visiting *Internet Explorer > Tools > Internet Options > Security > Local intranet* and adding the target or domain of the web server). See Step 5 in the Plexcel Operator's Manual for details.

Disabling New Account Creation

Once Plexcel authentication has been enabled, you may wish to disable the builtin Joomla! account registration. This is particularly true if you will also be using Windows Group Based Access Control (described later) as that is only enforced through the Plexcel authentication plugin. Meaning, someone could effectively bypass any Plexcel based access control by simply registering and using a regular local Joomla! account.

To disable new account creation in Joomla! visit *Control Panel > Site > Global Configuration > System > User Settings > Allow User Registration > No > Save*.

Note: Regular Joomla! accounts such as 'admin' may still be used to login to Joomla! even after disabling new account creation.

Securing the Login Form

By default, Joomla! does not secure the login form with HTTPS. Transmitting Windows domain passwords in clear text over the network is almost certainly a violation of security policy even for small companies. It is strongly recommended that you enable HTTPS protected logins to secure domain passwords.

Note: Plexcel SSO authentication does not require SSL because it only transmits SPNEGO / Kerberos data encrypted with the user's secret key and never transmits the password itself.

Before you can enable HTTPS protected logins you must first make sure that your site is accessible through HTTPS. Test HTTPS by visiting your site under *https://mysite...* (as opposed to *http://mysite...*). If HTTPS does not work, you will need to revisit your Apache configuration to enable it.

Note: RedHat based systems like RHEL, CentOS, Fedora, etc all have Apache + SSL packages with self signed certificates that can be installed using the package manager. Provided the right packages are installed, SSL should work without additional configuration.

Note: Unless you install a non-self signed SSL certificate, browsers will present users with a warning when they try to use the login form indicating that the certificate is not trusted. However, users can accept the certificate and add an exception for the target site after which the browser will no longer complain. Larger organizations frequently setup an internal certificate authority to properly support SSL throughout their network.

To enable HTTPS protected logins in Joomla! visit *Control Panel > Extensions > Module Manager > Login Form > Encrypt Login Form > Yes > Save*.

Note: The login form itself will not be under SSL but the HTTP request containing the credentials will be to an SSL protected route.

Username Canonicalization

Usernames in a Windows environment can take several forms. Because Joomla! requires a local account for upper level logic and storing preferences, it is important that the same username string is used consistently. Plexcel permits setting how you wish usernames to be canonicalized. The following three forms are supported:

Canonicalization Form	Example	Notes
nETBIOSName\sAMAccountName	ACME\alice	
sAMAccountName@dnsRoot	alice@acme.net	This is the default username canonicalization form.
sAMAccountName	alice	Beware that this form cannot ensure uniqueness in a multi-domain environment. Unless you are absolutely certain that users will never authenticate from multiple domains, we strongly recommend that you use one of the qualified username forms above.

To change username canonicalization behavior visit *Control Panel > Extensions > Plugin Manager > Authentication – Plexcel Active Directory Authentication > Username Canonicalization Form* select the desired form and *Save*.

Note: You must establish the desired username canonicalization form *before* users authenticate with the site. Otherwise, users will receive errors or accounts will be orphaned. Meaning, you could end up with two accounts like 'alice' and 'alice@acme.net' - one of which will be useless. If you do change username canonicalization after accounts have been created, users may receive an error like "This e-mail is already registered. If you forgot your password ...". To resolve this issue, you must go to *Control Panel > User Manager* and change the username of each user from the old form to the new form (such as from bcarter@acme.net to ACME\bcarter).

Windows Group Based Access Control

The Plexcel Joomla! Plugins can be set to only authenticate users in specific groups. If a user is excluded by these lists, no local account will be created and the user will simply not be authenticated. They will have the privileges of an anonymous user only.

To enable Windows group based access control, visit *Control Panel > Extensions > Plugin Manager > Authentication – Plexcel Active Directory Authentication* plugin. Into the *Groups Allowed Access* text area, enter a **semicolon separated list of Windows groups** that should be allowed to authenticate with your site.

For example, the following *Groups Allowed Access* list would grant the three groups access to the site:

```
ACME\Domain Admins; ACME\IT Management; ACME\Business Control
```

Note: When entering multiple groups, do not forget the semicolons!

You may also use names with no domain, LDAP DNs, names qualified with a DNS domain or principal names of individual users like the following example:

```
Domain Users; CN=Business Control,CN=Users,DC=acme,DC=net; acme.net\Business Control;  
larry@acme.net
```

The *Groups Denied Access* list may be used (albeit less likely) to exclude users that also happen to be in a group in the *Group Allowed Access* list. For example, if you have ACME\Domain Users in *Groups Allowed Access* and ACME\Consultants in *Groups Denied Access*, then ACME\Consultants will be denied access whereas everyone else in ACME\Domain Users will be allowed access.

Automatic Contact Creation

The Plexcel Joomla! authentication plugin can be configured to automatically create standard Joomla! contact entries for each user when they login. New contacts will be linked with the corresponding user account and a configurable category ID. Information will also be automatically updated whenever the user's session is initialized.

The following contact field table shows which Windows account fields (as displayed in the Active Directory Users & Computers utility) are used to populate the Joomla! contact fields.

Joomla! Contact Field	Windows Account Field (from ADUC)	LDAP Field Name
Name	General > Display name	displayName
Alias	General > First name	givenName
Contact's Position	Organization > Title	title
E-mail	General > E-mail	mail
Street Address	Address > P.O. Box, Street	postOfficeBox, streetAddress
Town/Suburb	Address > City	l
State/County	Address > State/province	st
Postal Code/ZIP	Address > Zip/Postal Code	postalCode
Country	Address > Country/region	c
Telephone	General > Telephone number	telephoneNumber
Mobile Phone Number	Telephones > Mobile	mobile
Fax	Telephones > Fax	facsimileTelephoneNumber
Web URL	General > Web page	wWWHomePage
Miscellaneous Information	Telephones > Notes	info

Before you enable automatic contact creation, it will be necessary to first determine the correct numeric contact category ID with which contacts should be associated. To determine this ID visit *Control Panel > Components > Contacts > Categories* and look at the far right column for the numeric ID of the desired category. Remember the value for the next step.

To enable automatic contact creation visit *Control Panel > Extensions > Plugin Manager > Authentication – Plexcel Active Directory Authentication*. In the *Parameters* section, enable *Automatic Contact Creation* and enter the desired numeric contact category ID. Click *Save*.

Note: The default Joomla! template does not display a Contacts menu item. To create a Contacts page visit *Control Panel > Menus > Main Menu > New > Internal Link > Contacts > Category > Contact Category Layout*, enter a Title (e.g. Employee Directory) and category (this must match the aforementioned contact category ID) and click *Save*. There should now be a new menu item that displays all contacts created through this automatic contact creation feature.

Diagnosing Errors

If Plexcel authentication fails for any reason, view the Plexcel log file (usually `/var/lib/plexcel/plexcel.log`) and fall back to trying the Plexcel examples. For example, if the time on the server becomes out of sync with AD you will get "Clock skew too great" errors and authentication will stop working. This error is displayed clearly in the log file. Refer to the Possible Issues section in the Plexcel Operator's Manual for other examples of Plexcel errors.

Patching Old Versions of Joomla! for Special Characters in Usernames

At some point prior to the release of Joomla! 1.5.14, Joomla! did not accept special characters that could appear in standard Windows account usernames. In particular, older versions of Joomla! will reject usernames with hyphens (-) and backslashes (\) with the following error:

Please enter a valid Username. No spaces, at least 2 characters and must contain only letters and numbers.
E_NOLOGIN_ACCESS

If you are using one of these older versions of Joomla! and you have usernames with hyphens or you would like to use the backslash username canonical form (see *Username Canonicalization* above) you will need to apply the following one line change to the Joomla! source code.

In the file `libraries/joomla/database/table/user.php` around line 152 change:

```
if (eregi( "[\<|\>|\"|\'|\%|\;|\(|\)|\&]", $this->username) ||
    strlen(utf8_decode($this->username )) < 2) {
```

to:

```
if (eregi( "[<>\"%();&]", $this->username) || strlen(utf8_decode($this->username )) < 2) {
```

Joomla! 1.5 FTP Directory Permissions

Permissions on the Joomla! tmp directory and FTP server can be tricky to get right. Both Apache (running as www-data or apache) and the FTP server (running as the user logged in) must have write access. For Apache it will likely be necessary to change both the ownership and permissions with the following commands (this assumes a Joomla! installation directory of /home/someuser/joomla-1.5):

```
# chown someuser:www-data /home/someuser/joomla-1.5/
# chmod 777 /home/someuser/joomla-1.5/
```

It may also be necessary to adjust FTP daemon parameters. For example, Red Hat and Ubuntu both use vsftpd which will need an /etc/vsftpd.conf with the following lines uncommented:

```
local_enable=YES
write_enable=YES
local_umask=022
```

Whenever a change is made to the FTP daemon configuration it is necessary to restart is like:

```
# /etc/init.d/vsftpd restart
```

To test this configuration, login to the web server using ftp, change to the Joomla! directory and try to write a file like:

```
$ ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.1.0)
Name (localhost:someuser): <enter>
331 Please specify the password.
Password: paSsw0rd<enter>
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd joomla-1.5
250 Directory successfully changed.
ftp> put dead.letter
local: dead.letter remote: dead.letter
227 Entering Passive Mode (127,0,0,1,41,25)
150 Ok to send data.
226 File receive OK.
368 bytes sent in 8e-05 secs (4.5e+03 Kbytes/sec)
ftp> quit
221 Goodbye.
```

If the above works, Joomla! should be able to install extensions.

Note: If you attempt to copy configuration.php-dist as the initial configuration.php, the FTP Configuration step of the web-based installation will fail with "Error: The XML response that was returned from the server was invalid." whereas we have found that starting with an empty configuration.php for the web-based installation results in success.