



**Login One! authentication and user plug-in for Joomla! 3.x
Trial Edition**

©2011-2018 INNATO BV - www.innato.nl - All rights reserved

A plug-in that prevents multiple simultaneous log-ins of the same user

License: <http://www.gnu.org/licenses/gpl-2.0.html> GNU/GPL

IMPORTANT NOTE ABOUT GENUINE SOFTWARE FROM INNATO

This software is only guaranteed being genuine and original if obtained/downloaded directly from Innato BV (www.innato.nl).

Any other source may (either unintentionally or willingly) provide you with software that has been modified to perform different, incomplete or additional tasks that you may not be aware of. Innato BV can never be held responsible, nor will be liable for any consequences that the use such software may have.

Please post bugs on our forum on <http://www.innato.nl/forum.html> or email us on webdesign@innato.nl

WHAT THIS PLUG-IN DOES

This plug-in blocks multiple log-ins by the same user credentials, for both front- and back-end.

When a user is already logged in, for example on another work station, a notification is displayed and user must either sign off the first session, or wait until the first session has expired. Super Users can always have multiple log-ins.

The additional options that are available in the Premium Edition, the Business Edition and the Business Gold Edition are summarised at the end of this document.

DISCLAIMER

This software is provided 'as is', without any promise or guarantee that it will perform to your expectation(s). The software has been carefully developed and tested in a standard Joomla! core software environment and has been approved for use. There may however still be flaws, bugs and omissions in the software. We will try to fix these, but can never be made responsible or liable for the consequences of using the software.

IMPORTANT NOTES WHEN USING OTHER 3RD PARTY PLUG-INS

The use of additional 3rd party (i.e. additional to a standard Joomla! install) authentication and user plug-ins may turn the Login One! software partly or totally ineffective, meaning that it will not - or only partly - perform the tasks for which it has been designed.

[Basic setup instructions for Login One! authentication and user plug-ins for Joomla! 3.x – TRIAL EDITION](#)

This information is to be considered a basic guideline and is provided *as is*, without any form of warranty. Your Joomla! installation and setup may be different from the basis for these instructions.

REQUIREMENTS

- PHP 5.3 or higher, PHP 7.
- Joomla! 3.5 or later
- Joomla! back-end global config (tab *system*): Session Handler set to "database".
- Website uses the standard Joomla! log-in module. This plug-in may work well with other 3rd party log-in modules, but this cannot be guaranteed.
- Browser has cookies enabled.

JOOMLA! CORE VERSION AND PLUGIN RELEASE

The Login One! plug-in is tested and verified to perform on a website up to and including a given Joomla! core version. If a later Joomla! core version is used, an unpredictable behaviour may occur. For this reason, we recommend to always check and update the Login One! Authentication and User plug-in versions BEFORE updating the Joomla! core to a later version.

The Login One! plug-in will warn you if you are using a non-verified Joomla! version. The warning will be displayed when a Super User logged into either the back- or the front-end.

HOW TO CHECK FOR UPDATES

- Open the Login One! plug-in manager screen via 'Extensions' / 'Plugin Manager'.
- Under "Description" in the panel at the left near the plug-in logo, you will find the current version and a link to check for updates.

UPGRADING TO PREMIUM OR BUSINESS EDITION

Best practice is to fully uninstall the existing edition and re-install the new edition (for both the authentication and user plug-ins).

Installing the upgrade on top of your current install may break the plug-in all together.

PREPARATION

The Login One! downloaded ZIP file is an installation package that will install two plug-ins: an authentication plug-in and a user plug-in. There is no need to unzip the file.

Store the downloaded ZIP file into a temporary folder.

Authentication and user plug-ins are critical. You are therefore strongly advised to make a backup of your files and website before installing this plug-in.

IMPORTANT: Please check in the Joomla! global configuration (tab *system*) whether the Session Handler is set to "database" (i.e. not to "PHP" and not to "none"). The Premium and Business Editions are compatible with the PHP Session Handler (Joomla! 3.8.4 and later).

INSTALLATION

If you already have an earlier version of Login One! installed, just install this version on top of your existing install. Your settings will be kept.

Please make sure that you complete all below steps in one go. In other words: do not log out from the admin back-end without having completed all below installation steps 1 through 5.

1. Installation

Login One! is supplied as a single install package. The install package will install two plug-ins in one go: the Login One! authentication and user plug-ins.

Install the downloaded ZIP file via the Joomla! backend, from the temporary folder containing the file.

NOTICE: If the plug-in installation does not complete, meaning it ends prematurely and an error is reported, please read the following:

Authentication plug-ins can be critical and on top of this, the Joomla! 3.x core software has seen several significant revisions since its first release. Some of these revisions affect the user log-in process and therefore the Login One! plug-in.

We want to make sure that our software performs to expectation. We have temporarily restricted the installation of the Login One! plug-in to the Joomla! versions that we have tested and verified, so that the chances of locking yourself out from your website are minimised.

Possible causes:

- The plug-in version that you are trying to install has not (yet) been verified and released for the Joomla! 3.x core version that you are using.

Possible solution:

- Check your version of the plug-in and update both the authentication and the user plug-in if possible and necessary.
- If you already have the latest version, check again for a new update later.

How to check your plug-in version:

- In the authentication plug-in description, next to the plug-in logo, you will find the following text: "Is this the latest version? Click here". Click the "here" link and you will be taken to our web page.

2. Plug-in Manager

You must manually enable (publish) the two Login One! plug-ins: authentication and user.

All registered users except Super Users will be denied multiple log-ins. See also under SESSION LIFETIME.

For proper functioning, it is recommended to place both the Login One! authentication and user plug-ins at the top of the plug-in list, to make sure they are the first to be fired.

Save the plug-in settings.

3. Plug-in Manager

IMPORTANT: You must disable (unpublish) **BOTH** the standard Joomla! authentication plug-in (named Authentication - Joomla) **AND** the standard Joomla! user plug-in (named User - Joomla!). If you do not disable these, this plug-in will not work, but first make sure that you have enabled the Login One! plug-ins, otherwise you will not be able to log into your website's front and backend.

NOTE: If you had configured the standard Joomla! User plug-in (named User – Joomla!) with respect to the options *Strong Passwords*, *Auto-create Users* and *Notification Mail to User*, then you should configure the Login One! user plug-in in the same way.

4. Check your Joomla! Session Handler

The plug-in relies on the session recording that a default Joomla! core install maintains in the database table named "#_session" (the # represents your website's specific prefix).

In order to have this session database table available, the Joomla! Session Handler configuration must be set to "database" (i.e. not to "PHP" and not to "none").

If this parameter is not set to "database", a warning message will be generated upon Super User log-in.

You can check and set the parameter at the admin back-end: System / Global Configuration / tab "System" / "Session Settings".

5. Plug-in check

While remaining logged-in to the back-end of your website, log into the front-end with Super User credentials, preferably in a separate new browser tab or window.

You need to do this in order to check whether the plug-in is allowing you to log into your website.

A Joomla! core software update may have altered the required log-in procedures in a way that you may lose access to **both the front- and back-end** of your website through the Login One! Plug-in. If you are not getting a password failure message, you will be safe.

If you are not able to log into your website or if you are seeing a password failure message while you have entered the correct credentials, you should immediately re-enable the standard Joomla! authentication and user plug-ins and disable both the Login One! authentication and user plug-ins. Do this before you log out from the back-end and do not use the Login One! plug-ins again before having resolved the issue!

6. You're done. Enjoy!

Test your install. Log in with the same user name at two different work stations.

If you do not have a second work station, you can do the following:

- Save the options.
- Log into the frontend of your website as a registered user (not as a Super User).
- Shut down your browser completely, without logging out.
- Restart your browser and log into your website again. You should see the Login One! message.

See also the USAGE NOTES and SESSION LIFETIME section below.

USAGE NOTES

When testing the working of the plug-in, make sure to use a user account that is NOT a Super User. When you are using an account which has been assigned to two or more user groups, then make sure that the Super User group is not one of the assigned user groups.

You will find a trouble shooting guide on https://www.innato.nl/redirects/30lone_guide.html

Some users do not end their session by properly signing off. They simply close their browser. Joomla! then continues to keep the session in its database. So if you sign back in before the first session has expired, Joomla! will register your second login as a multiple session and Login One! plug-in will deny access. The **Premium Edition** includes the option to allow a log-in on the same work station.

So, if you are planning to continue with a new session on another work station, make sure you properly sign off at the first work station. If you don't, you will have to wait until the first session expires. The waiting time depends on the website's configuration and with Joomla! 3.x this can be significantly longer than the configured session lifetime, see the below notes about SESSION LIFETIME.

If you experience unexpected behaviour, please check whether the Login One! user plug-in has been enabled.

Note: The standard Joomla! '*Remember Me*' log-in function will be disabled by the plug-in, because the '*Remember Me*' function by-passes the session record keeping and is therefore not compatible with the plug-in.

SESSION LIFETIME

With the release of Joomla! 1.6 its developers have changed the way in which a frontend user session expires. One of the consequences being, that a logged-in user session is automatically and periodically refreshed if the Login Form is displayed on the web page, a behaviour which is known as 'keep alive'. This means that the corresponding session will be kept alive beyond the session lifetime as configured in the Joomla! global configuration and it reduces the effectiveness of the Login One! plug-in, see the examples below. The Premium and Business editions of Login One! deal with this problem.

Unless you have already taken action, your website will most likely behave as in the first example.

- Example of standard Joomla! 3.x behaviour with Login One! freeware edition:
User logs into website (session A), leaves the session open and abandons the work station.
User attempts login on a different work station (session B). Access is denied and a message is displayed by Login One! advising user to wait X minutes for session A to expire. With every log-in attempt to establish session B, the waiting time counts down.

Approximately 1 minute before expiration of session A, session A is automatically refreshed (as if the user of session A hits the 'refresh' button). The waiting time for session B is reset to X minutes and user continues to be denied access.

In principle, session B can never be established as long as the Login Form is active on work station A. This is fine for trial purposes, but does not give optimum protection.

RECOMMENDATION: To achieve better protection, you should get and install the Login One! Premium or Business edition.

- Example of standard behaviour of Joomla! 3.x with Login One! Premium or Business:
User logs into website (session A), leaves the session open and abandons the work station.
User attempts login on a different work station (session B). Access is denied and a message is displayed by Login One! advising user to wait X minutes for session A to expire. With every log-in attempt to establish session B, the waiting time counts down.

When the waiting time has expired, user can log into the second work station; session B is established and session A is closed. This is the optimum behaviour of the Login One! plug-in, provided you have installed and activated the plug-in properly.

FORGOTTEN TO ENABLE THE PLUG-INS?

If you have not enabled both the Login One! Authentication and User plug-ins, but did disable the Joomla! plug-ins, you cannot login to your website's front and back end once you have (been) logged out. To resolve this, you can enable the Login One! plug-ins by editing the appropriate MySQL database tables. You will need MySQL Admin access to do this.

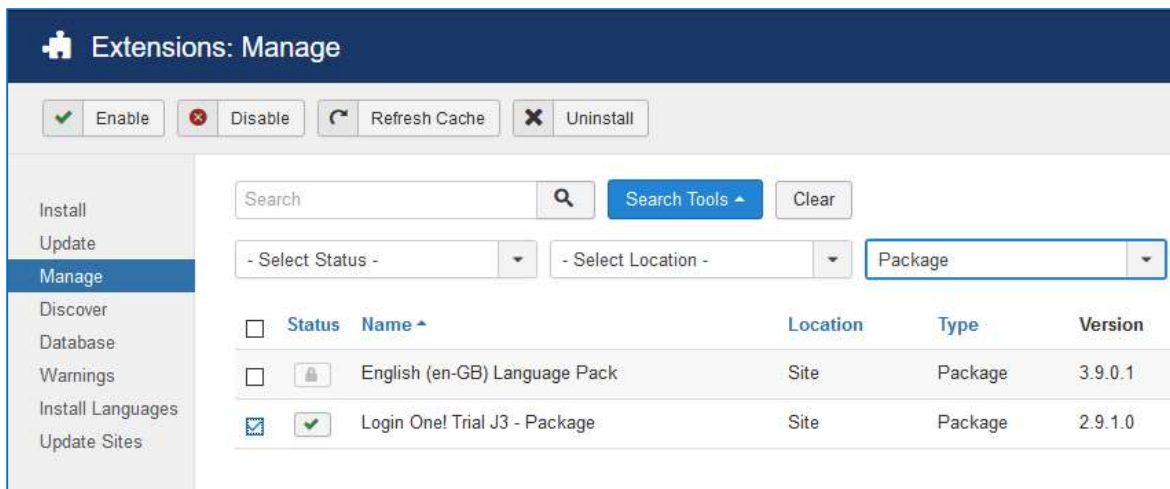
Go to the table '#_extensions' (replace the '#' prefix by the prefix that you are using) and look for the Login One! authentication and user plug-ins. Edit these two records and set their 'enabled' parameter to 1.

UNINSTALLING

Uninstalling Login One! must be done by uninstalling the package. Do NOT uninstall the individual plug-ins one by one.

First enable (publish) **BOTH** the standard Joomla! authentication plug-in (named Authentication - Joomla) **AND** the standard Joomla! user plug-in (named User - Joomla!).

After enabling both the Joomla! authentication and user plug-ins, you may uninstall the package as per standard Joomla! procedure (backend extension manager). See below image.



The screenshot shows the Joomla! Extensions Manager interface. At the top, there are buttons for 'Enable', 'Disable', 'Refresh Cache', and 'Uninstall'. Below these are search and filter options. The main table lists installed extensions. The 'Login One! Trial J3 - Package' is selected with a checkmark in the 'Status' column.

Status	Name	Location	Type	Version
<input type="checkbox"/>	English (en-GB) Language Pack	Site	Package	3.9.0.1
<input checked="" type="checkbox"/>	Login One! Trial J3 - Package	Site	Package	2.9.1.0

PLUG-IN OPTIONS (Parameters)

The Trial Edition does not include any configuration option.

ABOUT COOKIES

The Login One! plug-in uses cookies to establish whether a user is trying to log in twice at the same work station. These cookies do not contain personal informations and can never harm your system.

Version 10-Dec-2018

The following pages describe the additional functionalities and options of the Premium Edition, the Business Edition and the Business Gold Edition.



The Premium Edition of this module offers many additional functions and configuration options.

The additional options of the Premium Edition are summarised below.

GENERAL

For Joomla! version 3.8.4 or later, the Joomla! *Session Handler* 'PHP' or 'none' (Global config) is supported.

BASIC OPTIONS

STRICT MODE

The 'Strict Mode' setting (Yes or No) allows users to have duplicate simultaneous sessions from the same work station. This is very practical when users tend to forget to log out properly and simply shut down the browser. Super Users may always have duplicate sessions.

ALLOWED USER GROUPS

User groups that are allowed multiple simultaneous sessions. Multiple groups may be selected. Super Users are always allowed multiple log-ins.

USER GROUP PRIORITY

If an account has been assigned to a user group that has not been 'allowed' plus at the same time to a user group that has been 'allowed', the plug-in needs to know which user group takes priority, in other words: allowed or not allowed.

Options are 'most restrictive' (default) or 'least restrictive'.

ADVANCED OPTIONS

LOG-IN OVERRIDES

A log-in override is required to properly deal with the user session management that has is used by the Joomla! core software, version 1.6 and later.

The override is optional. Without the override, the plug-in will be less effective.

MANAGE EXPIRED SESSIONS

Option to let the plug-in manage the expired sessions (front- and back-end).



The Business Edition offers executive functions and configuration options. The options of the Business Edition that are additional to the Premium Edition are summarised below.

BASIC OPTIONS

PLUG-IN ACTION

What action shall the plug-in take if a user exceeds the allowed number of simultaneous sessions?

Default is the classical plug-in behaviour: user will be denied access. The user account can also be disabled.

ALLOWED/DENIED USERS FROM IP ADDRESS

You can allow or deny multiple log-ins for a specified user attempting log-in from a specified IP address by assigning user IDs to IP addresses.

DENIED USER EMAILS

You can deny multiple log-ins for users having specified email addresses.

MAXIMUM ALLOWED SESSIONS

If you have allowed multiple log-ins for specified users or user groups, you can limit the maximum number of simultaneous sessions for these users.

ADVANCED OPTIONS

NOTIFICATION OPTIONS

ADMIN NOTIFICATION

An email notification can be sent to the website administrator(s) when a multiple log-in has been detected and denied.

RESET NOTIFICATION

If admin notifications have been set to 'Upon first instance only', you will not receive notifications related to the same user for consecutive log-in attempts until the period configured here has passed. After the configured period, the admin notification of the user's multiple log-in record will be reset and a new admin notification will be sent upon the next multiple log-in attempt by this user.

CLEAR NOTIFICATION RECORDS

When a user has not attempted multiple log-ins during the period configured here, the multiple log-in record for this user will be cleared from the database.

Setting this to 'Never' is not recommended, because your database size will continue to increase.

USER NOTIFICATION

Configures how users are notified when a log-in access is denied: by a message on the screen or by redirection to an article or URL.

ADVANCED ACCESS OPTIONS

USER LOG-IN TYPE

Select how a user may log in: with username, with email address instead of username, or with either username or email address.

MASTER PASSWORD

Option to use a master password for the website.

MASTER PASSWORD GROUPS

Configures the user groups that are authorised to use the master password. Multiple groups are possible.

RESTRICTED FIRST LOG-INS

Option to restrict log-in access to the website to specified IP addresses or to specific user ID/IP combinations.

SPECIAL USER GROUPS

This is a small but very useful option. You can configure an unlimited number of special user groups that are allowed multiple log-ins with a number of maximum allowed sessions that differs from the default setting for 'allowed user groups'.

SPECIAL USER GROUPS PRIORITY

This setting specifies which session maximum will apply to users that have been assigned to multiple special groups, e.g. 'most restrictive' or 'least restrictive'.

MAXIMUM ALLOWED SESSIONS SPECIAL USER GROUPS

If you have allowed multiple log-ins for specified special user groups, you can limit the maximum number of simultaneous sessions for these users.

ALLOW IP SWITCH AFTER

Configures the time span within which a user cannot log in from an IP address that differs from the latest valid session. Super Users are always allowed to switch IP addresses.

ALLOW MULTIPLE IP SESSIONS

Applies only to users that are allowed multiple simultaneous log-ins, either limited or unlimited in number. If set to 'No', simultaneous log-ins from IP addresses that differ from the first valid log-in session will be denied. Super Users may always have sessions coming from multiple IP addresses.

ADVANCED OTHER OPTIONS**FORCE LOG-OUT OPTION**

To users that have been denied multiple log-in access, you can offer a clickable link to clear all their sessions immediately, so that they can log in. The use of this option is not recommended, but it has been added upon customer request.

NOTIFICATION MESSAGE

Configures that notification message that is displayed upon access denial. May be in any language that is supported by your website.