

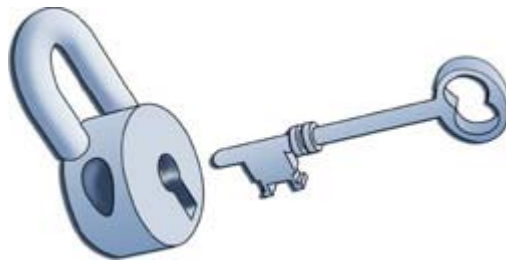


inFusion Authenticator for Microsoft IIS™

Sample Application User Guide

Dynamic user authentication like no other

inFusion Authenticator for Microsoft IIS™ Sample Application Version 2.0



Copyrights

inFusion Authenticator is a product of On-Line Data Solutions, Inc.

Trademarks

Microsoft Windows is a trademark of Microsoft Corporation

ColdFusion is a trademark of Macromedia Corporation

BlueDragon is a trademark of New Atlanta Communications, LLC

iHTML is a trademark of Inline Corporation

Active State Perl is a trademark of ActiveState Tool Corporation

Suggestions and Support

Your suggestions for inFusion Authenticator are welcomed. Please email your comments to support@CoolFusion.com. Technical support for iAuth is also available from this email address or by joining our support email list. You can find details on joining our support list on our web site at www.CoolFusion.com.

On-Line Data Solutions, Inc.
1919 Middle Country Road STE 204
Centereach, NY 11720-3501

Phone: (631) 737-4668

FAX: (631) 737-9539

Sales: sales@CoolFusion.com

Technical Support: support@CoolFusion.com

General	5
System Requirements	5
Installation	6
System Settings	8
User Management.....	12
Final Installation Notes	14
Support.....	15

General

inFusion Authentication Sample application (iAS) is a demonstration application written in CFML that can be used as a basis for creating custom website authentication schemes using iAuth and IIS. iAS version 2.0 is a complete rewrite from version 1.x and utilizes the advanced features of iAuth version 2.5.9 and higher (iAuth version 2.5.9 is current as of this writing).

iAS is a completely functional application with the following features:

- Comes with complete source code
- Compatible with ColdFusion (including CFMX) and BlueDragon
- Account lockout on high login error count (optional)
- Login timeouts
- Different methods of operation including custom login pages (based on sessions) and browser login dialogs
- Multiple login protection
- Web-based admin
- Quotas for specified download types (optional)

System Requirements

iAS requires the following software:

- Windows server running Microsoft IIS version 4 or higher
- Macromedia ColdFusion 2.0 or higher (including CFMX) or New Atlanta's BlueDragon
- inFusion Authenticator for IIS version 2.5.9 or higher

Installation

iAS includes a web interface (written in CFML) and a sample Microsoft Access database that can be optionally upscaled to a database server such as Microsoft SQL server or MySQL. All iAS files are included in a single ZIP file and there is no automated installer.

Note: The iAS ZIP file contains several folders so, when you unzip the file, make sure to unzip with the option to retain folders enabled. You can either choose a folder in your website document path or a temporary path outside of the website folder path (you can then move the files manually after unzipping).

The application.cfm template configures the iAuth datasource as “iAuth.” When you create the datasource on your server you can either name it “iAuth” or, if you use another name, you can edit the application.cfm template accordingly.

Note: You will also need to place the #iAuth.cfm template in the root of the folders that you wish to protect. Please refer to the iAuth manual for details.

iAS includes an Access 2000 database file which can be used for testing.

Note: It is recommended that the database be upscaled to an SQL server (such as Microsoft SQL server or MySQL) in a production environment. While the Access database will work in production, it will be slower than an SQL server.


If you use the included Access database, it is highly recommended that you move it to a folder outside of the web site folder path to prevent unauthorized access.

The Access database includes a single user that is configured as the System Administrator. Once you have copied the iAuth templates to your web server and have configured the datasource you can log in using this default account.

Log in to the application by directing your browser to the web folder in which you installed iAS. For example:

<http://www.domain.com/iauth/index.cfm>

Figure 1 - iAS initial login screen

The image shows the initial login screen for the infusion Authenticator application. At the top, there is a graphic of a padlock and a key, with the word "infusion" above the padlock and "Authenticator" below the key. Below this graphic is a blue header bar with the text "infusion Authenticator Login". Underneath the header bar, there are two input fields: "User Name" with the text "systemmanager" entered, and "Password" with a series of asterisks entered. To the right of the password field is a blue button with the text "Login".

infusion Authenticator Login

User Name: systemmanager

Password: *****

Login

The default Administrator login is:

User Name: SystemManager
Password: Password

It is recommended that once you have logged in as the Administrator, you change the default login to one that is more secure.

System Settings

iAS settings are configured from the web interface. When you log in you will see the menu below.

Figure 2 – iAS Main Menu



Clicking on the Admin Menu button will bring you to the administrator's menu shown below.

Figure 3 – iAS Administration Menu



From here you can choose to edit system settings by clicking on the Settings button. The system settings are shown on the next page.

Figure 5 – iAS Settings Screen



Settings

Timeout (minutes)	<input type="text" value="1"/>	(0=no login timeout)
Max. Login Attempts	<input type="text" value="0"/>	(0=unlimited)
Enforce Single Login	<input checked="" type="checkbox"/>	
Action on Auth Failure	<input type="text" value="Redirect to URL"/>	
Redirect URL	<input type="text" value="http://65.119.242.50/iauth/login.cfm"/>	
Error Page	<input type="text" value="d:\inetpub\wwwroot\iauth\ErrorPage.htm"/>	
Template Error Page	<input type="text" value="d:\inetpub\wwwroot\iauth\TemplateErrorPage.htm"/>	
Quota Error Page	<input type="text" value="d:\inetpub\wwwroot\iauth\QuotaErrorPage.htm"/>	
Realm for Browser Login	<input test"="" type="text" value="iAuth Test "/>	
Charge extensions	<input type="text" value=".gif.jpg"/> (comma-separated list of file extensions)	

[Save](#) [Reset](#) [Main](#)

There are several settings that you can configure (some only pertain to other selections) which will alter overall system behavior. The following table describes each setting in detail.

Table 1 – iAS Settings Parameters

Setting	Description
Timeout (minutes)	The amount of time after which a user will automatically be logged out due to inactivity. This setting is typically used only when you are using the Browser Login Action (Action on Auth Failure) described below. This setting will work for the other types of actions, however, the other types of actions rely on sessions and you would typically use the session for a login timeout. Setting this parameter to 0 will disable the inactivity timeout.
Max. Login Attempts	The maximum number of login errors before the account is automatically disabled. Setting this parameter to 0 will disable this function.
Enforce Single Login	If this setting is enabled then a login will only be possible from one PC.
Action on Auth. Failure	<p>Determines the overall login method of the system. The possible settings are:</p> <p><i>Redirect to URL:</i> This option causes the browser to be redirected to the URL of your choice; typically a login form. The next setting determines the redirect URL.</p> <p><i>Display Error Page:</i> This setting causes the designated error page to display on the browser.</p> <p><i>Browser Login Prompt:</i> This setting causes the browser to display its built-in login prompt (HTTP 401 response).</p> <p>Note: If you are using the browser default login then you should allow anonymous access and remove basic and integrated authentication from the folder properties via the MMC.</p>
Redirect URL	The URL for redirection when <i>Action on Auth. Failure</i> is set to "Redirect to URL."
Error Page *	The full path to the error page to be displayed when <i>Action on Auth. Failure</i> is set to "Display Error Page"
Template Error Page *	The full path to the error page to be displayed if an exception is thrown in the #iAuth.cfm template.
Quota Error Page *	The full path to the error page to be displayed if the user attempts to download a file that is a charged item and they are over quota.
Realm for Browser Login	The realm to display on the browser login if <i>Action on Auth. Failure</i> is set to <i>Browser Login Prompt</i>
Charge Extensions	A comma-delimited list of file extensions that have an associated cost. This is used in association with <i>Credits</i> field in the <i>User Management</i> section.

Note: These pages are cached in application variables (refer to application.cfm) for speed. This means that changes to these pages are not immediately reflected in the system. In order to alleviate this you can either:

1. click the *Save* button on the iAS *Settings* page

or

2. modify the iAS templates to remove the page caching.

User Management

Users are managed in iAS by logging in as an administrator and then clicking on

Admin Menu → Edit Users

Figure 6 - The iAS Edit User Screen



The image shows the 'Edit User' screen in the iAS (Infusion Authenticator System) interface. At the top, there is a logo featuring a padlock and a key, with the text 'infusion' and 'Authenticator'. Below the logo is a blue header bar with the text 'Edit User'. The main area contains a form with the following fields and controls:

- User ID: 7
- Enabled: Yes (dropdown menu)
- Login Name: joe_smith (text input)
- Password: password (text input)
- Expires: No (dropdown menu)
- ☐ Start Date/Time: [text input] [calendar icon]
- ☐ End Date/Time: [text input] [calendar icon]
- ☐ Credits (bytes): -1 (text input)
- Administrator: No (dropdown menu)

At the bottom of the form are three buttons: 'Update', 'Reset', and 'Main'.

There are several possible settings for each user. The following table describes each setting in detail.

Table 2 – iAS Users Parameters

Setting	Description
User ID	This is the USER ID from the database. This is read-only and for informational purposes only.
Enabled	Determines if the account is enabled. Note: An account can be disabled automatically if there are too many failed login attempts by setting the <i>Max Login Attempts</i> field in the <i>Settings</i> section.
Login Name	The name that the user will login with.
Password	The password that the user will login with. Note: The password in iAS is not case sensitive but can be easily changed in your code.
Expires	Determines if the account expires according to the <i>End Date/Time</i> setting.
Start Date/Time	Determines the start date and time of the account. Format: mm/dd/yyyy hh:mm
End Date/Time	Determines the date and time of account expiration. Format: mm/dd/yyyy hh:mm
Credits	The number of credits (in bytes) that the user currently has.
Administrator	Determines whether the user is an administrator.

Final Installation Notes

A typical iAS installation will include a login folder and one or more protected folders. The login folder should include all of the files from the iAS zip file that are contained in the iAS folder. The protected folder should contain all of the files located in the Protected folder.

The #iAuth.cfm template uses several include files. In order to streamline your application you can physically include those files in your #iAuth.cfm template and also remove code logic that you are not using.

Testing Your Installation

Once you have created a login folder, protected folder, datasource and have configured your system you can begin testing. Point your browser to the protected folder and, depending on your settings, you should either be redirected to a login page, an error page or you should see a browser login prompt. When you enter your credentials, you should be able to access files in the protected folder.

Support

Limited support for this application is available by sending email to support@coolfusion.com.