External Database Authentication Provider

Administrators Guide

Last Updated: May 11th, 2015

IowaComputer GURUS

Contents

The Purpose of This Document 2
Document Revision History 2
Disclaimer 2
Copyright 2
Provider Overview 3
Key Features 3
Pre-Requisites for Use 3
External Database Preparation 4
Database Users & Connections 4
Provider Installation and Configuration 5
Installing to DNN 5
Configuring for Authentication 5
Configuring Role Assignments 7
Troubleshooting 8
Support & Contact 8
Contact Details 8

The Purpose of This Document

This document is intended for those looking to administer the External Database Authentication provider module provided by IowaComputerGurus. It should be noted that technical experience is needed to properly administer this module. Should assistance be needed please do not hesitate to contact us.

Document Revision History

Revision Date	Provider Version	Minimum DNN Version	Notes
10/23/2008	01.00.00	5.x	Initial module release
12/31/2008	02.00.00	5.x	Updated for stability & account creation improvements
1/27/2009	02.05.00	5.x	Updated for support of Role Assignment and other new features
12/19/2011	06.00.00	6.x	Updated for DNN 6.x support
5/11/2015	06.00.02	6.x	Updated for new document format

Disclaimer

This document is provided as an additional source of information on the usage of this module. Module content, features, and functionality are subject to change at any time and will be distributed to the public with unique version numbers. It is the reader's responsibility to ensure that this documentation matches the current version of the module in question. Additionally the reader understands that by using this documentation and the module that they agree to the terms of use, posted on the IowaComputerGurus.com website and available from all module download pages.

Copyright

Provider Overview

The ICG External Database Authentication provider is a DotNetNuke 6.0.0 and later authentication provider designed to allow users to be authenticated against an external database, once authenticated the users are migrated into the DNN system, for standard processes to work as one might expect. Future user authentication relies on the external database, and users' information is updated on each login.

Administrators when configuring the module may elect to sync information from DNN back to the external system, or also handle arbitrary role membership processes using configuration options discussed in this manual.

Key Features

The following attributes list the high-level features of the current module release.

- Works with any existing database schema for authentication with few limits. MS SQL Server only, and plain-text password only.
- Ability to use email address or separate username field within DNN
- Can sync DNN User Id to external system for further integration
- External database can be updated with DNN Profile Updates
- Allows for standard user interactions within DNN
- Bypass rule for Administrator and Host user accounts to avoid lockout situations in cases of misconfiguration or network communication issues.
- Ability to assign one or more roles to a user based on external database information
- Easily extensible module structure to integration with other systems. (With source code purchase.)

Pre-Requisites for Use

The External Database Authentication Provider requires usage with DNN Version 06.00.00 or later and Microsoft SQL Server 2005 or later. In addition to baseline product version the installing user must have a familiarity with SQL server to add needed components to external database and properly configure the provider to communicate with the database. ICG can provide limited assistance with this, please see the contact information at the bottom of this document for information.

External Database Preparation

Prior to installing the DNN portion of the provider it is best to configure the external database system for use first. This will ensure that all external integrations will work as desired before moving to the integration portion.

As part of the installation download a file "ExternalDbScript.txt" was provided. This file contains examples of the two procedures needed for proper execution. Of these two procedures only the ValidateUser procedure is required, the other query is only to be used if you desire to allow DNN to update the external database.

Using these queries as a base, update them to match the schema of your desired database. When making the queries ensure that column names match the values in the samples. If your database columns are different than the example simply use an AS alias to modify the query result value. Once modified and stored in your database, you can continue to the next step.

Database Users & Connections

The ICG External Database Authentication Provider communicates to the external database system using a standard SQL Server connection string. This will require proper connection credentials to allow the stored procedure(s) created in the prior step to be executed. For assistance with proper connection string creation please see http://www.connectionstrings.com

Provider Installation and Configuration

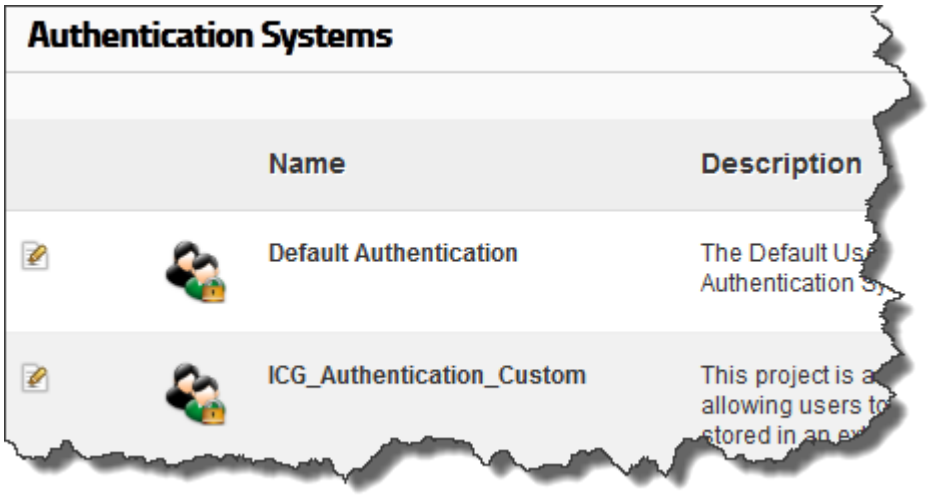
Installation & configuration of the provider is a simple process. Before starting ensure that the external database is configured and the valid connection information in available. ICG recommends manually testing credentials prior to stepping through installation.

Installing to DNN

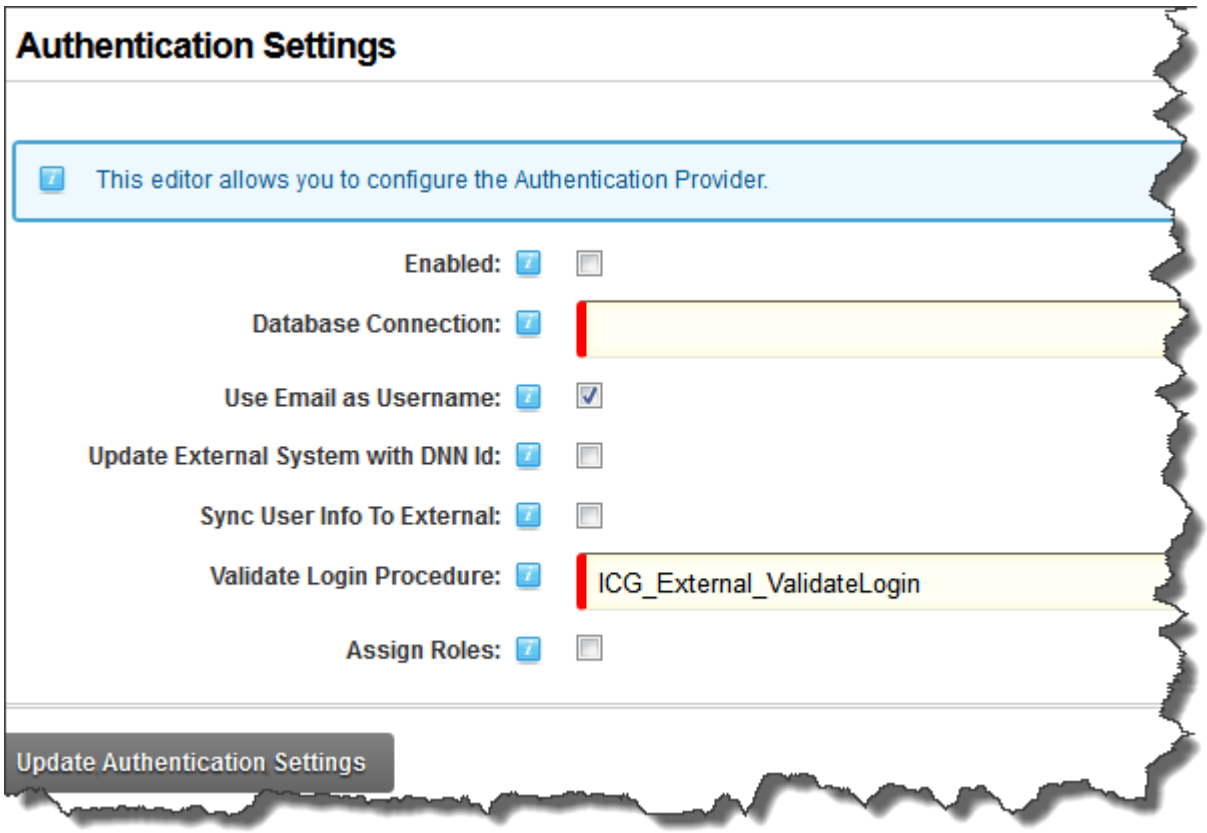
Base installation follows standard DNN module installation steps. When logged in as a "Host" user navigate to "Host" -> "Extensions" and use the "Install Extension" option to browse to the _install.zip file.

Configuring for Authentication

Once installed configuration of the provider is done under the "Admin" menu in the "Extensions" sub item. Within the extensions page user the "Authentication Systems" section a new value of ICG_Authentication_Custom shall appear. The following image shows a sample representation of this display.



From here select the "Edit" option on the left side of the ICG item. This will open the main configuration screen for the provider.



This is the heart of the configuration of the system, the enabled checkbox is used to enable/disable the control. Without this option selected, users will not be able to authenticate using the provider. The database connection is the FULLY formed database connection to the external SQL Server system configured in step 3 of these instructions. The basic form of a SQL Server connection is "server=SERVERNAME; database=DATABASENAME; uid=USERNAME; pwd=PASSWORD;" Where items in all caps are replaced with the respective value.

The next option, *Use Email As Username*, if selected will treat the email as the username, and your stored procedure created in step 3, does NOT need to return a username value.

The next option, *Update External System with DNN Id*, if checked will send communication to the external database after a successful user creation in DNN with the DNN UserId. This is a one-time sync and is great if other processes need to match users within DNN to users in the external system.

After this we see the *Sync User Info to External* option. This will send an update call to the external database upon every login to sync critical DNN user information.

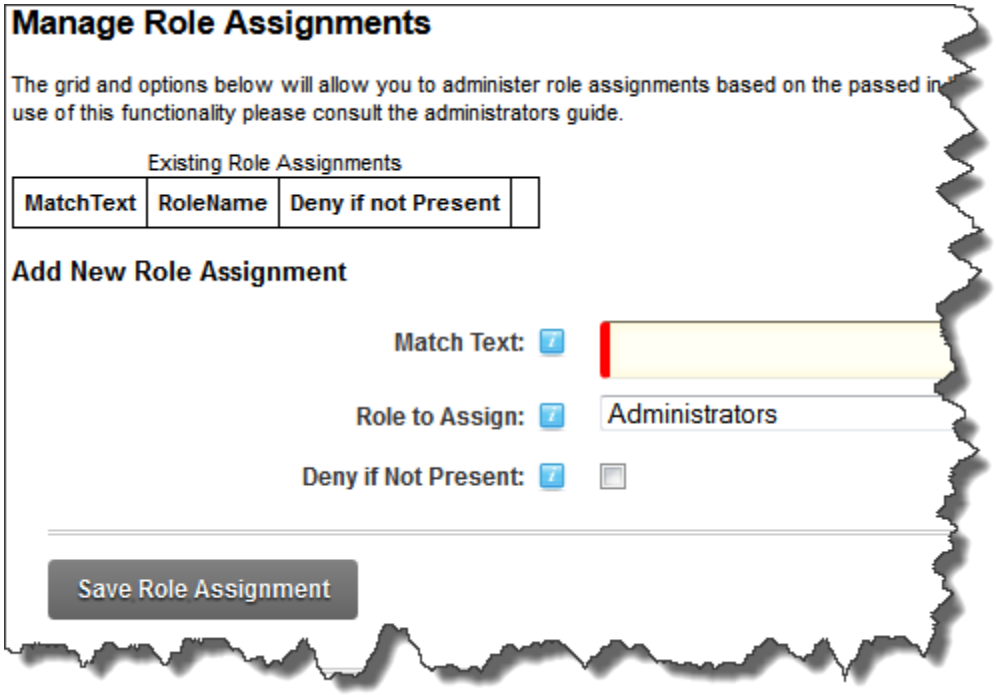
The final checkbox at the bottom is the *Assign Roles* option, allowing the specification of role assignments to users. Please see the next section for detailed instructions after enabling this feature.

The final collection of settings are the prompts for stored procedure names. These settings match the stored procedure names created in step 3. Changes only need to be made to this section if the names from the default setup scripts were not used.

After clicking update, you have completed the installation/configuration of the module and it is ready to use. Please test the module PRIOR to disabling the default DNN authentication module.

Configuring Role Assignments

An optional configuration element allowing for advanced security role assignments to be made will display if the Assign Roles option was selected in basic configuration. If enabled the following interface will be displayed.



Role assignments operate based on the "RoleInfo" column within the validation criteria. Passed values are separated using the comma (,) as a delimiter. In the role configuration you may supply a match text, role to assign and deny if not present.

As an example if a user is authenticated with a RoleInfo value of "sales,support,accounting" and a Match Text rule of "sales" was used to assign to the role "Sales" this user would receive the sales role. Conversely if a match text of "IT" was defined granting access to IT with the "Deny if not present" box is selected the user will be validated to be NOT in the IT role, even if manually assigned.

NOTE: We strongly recommend NOT using this process for administrator roles as after initial authentication and assignment of "Administrators" users will only be authenticated by DNN.

Troubleshooting

If after following all of the defined steps above you are still unable to authenticate using the credentials from the external database be sure to check the DNN Event Viewer for details. Our most commonly reported error is due to minimum password requirement differences between DNN & External systems. DNN by default requires a minimum of 6 characters for passwords. If the external system uses less than this changes to the <membership> node within the DNN web.config will be needed to reduce the password complexity.

If you are experiencing another issue, please contact us.

Support & Contact

Should you need assistance with this module you may use our customer support portal available at: http://support.iowacomputergurus.com We strive to respond to all support requests within one business day.

Contact Details

You may reach IowaComputerGurus using the following information

IowaComputerGurus, Inc
5550 Wild Rose Lane, Suite 400
West Des Moines, Iowa 50266

Email: support@iowacomputergurus.com
Website: http://www.iowacomputergurus.com
Support: http://support.iowacomputergurus.com
Phone: (515) 270-7063