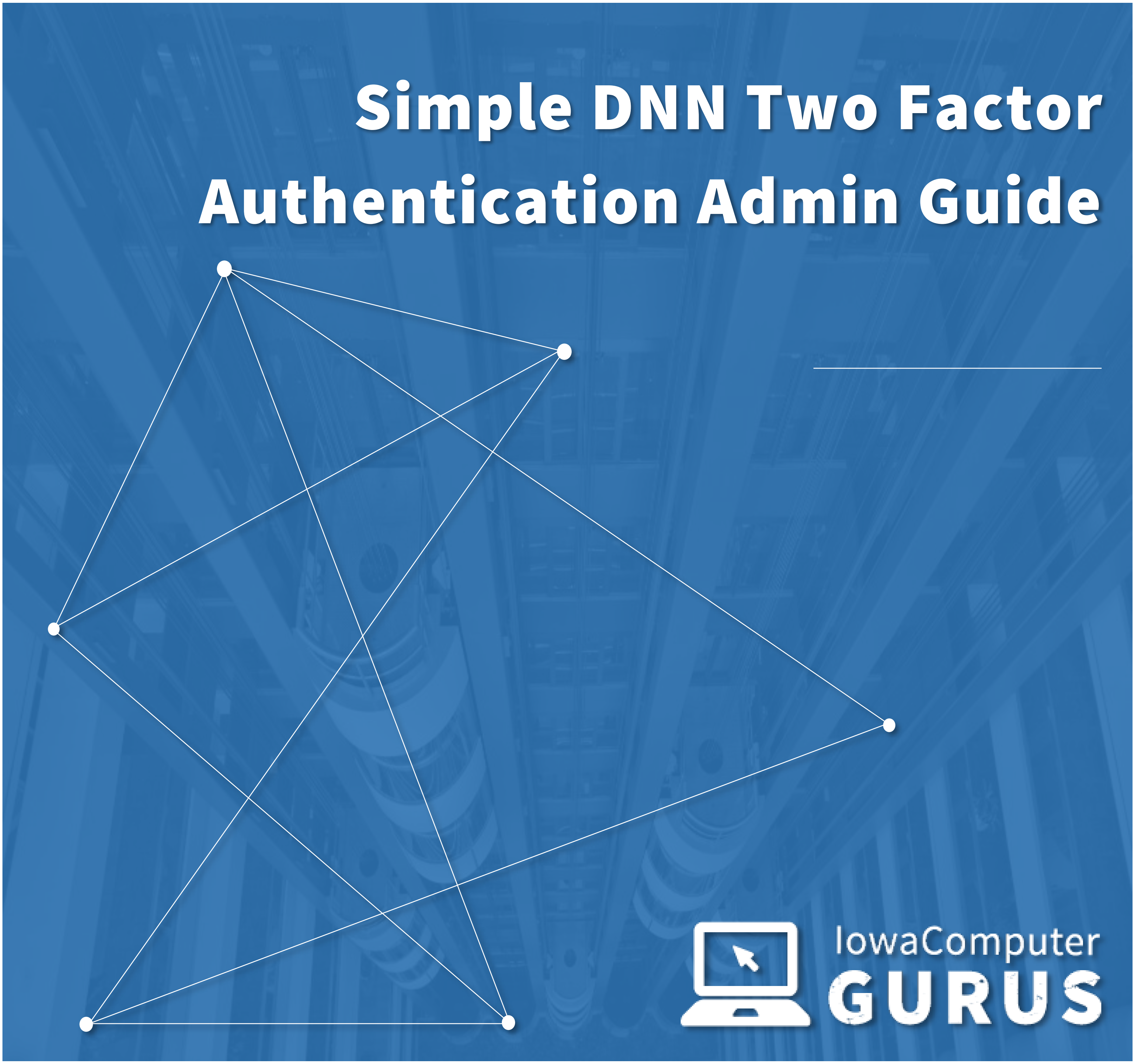
# Simple DNN Two Factor Authentication Admin Guide

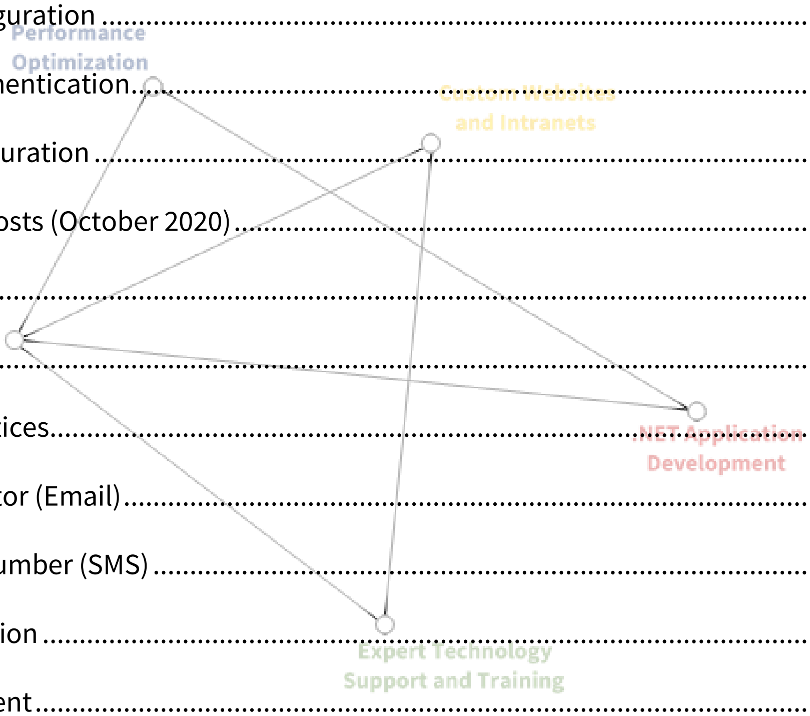


IowaComputer GURUS

**Design** **Develop** **Optimize** **Support**

Technology Services and Support . . . for the Life of Your Project

# Contents


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training

# Overview

This Provider was created to facilitate two-factor authentication upon login within DNN Platform (and Evoq) installations starting with Version 9.3.2 and later. This Provider replaces the default DNN Login provider and introduces new features supporting two-factor authentication for groups of users or all uses with various means of delivery.

## Version History

The table below outlines the history of this solution, along with key features included with each release.

| Version # | Date Released | Highlights |
|---|---|---|
| 2.0.9 | 5/27/2020 | Initial release with two-factor support for Email. |
| 3.0.2 | 10/8/2020 | Updated with Twilio Based SMS options enabled |

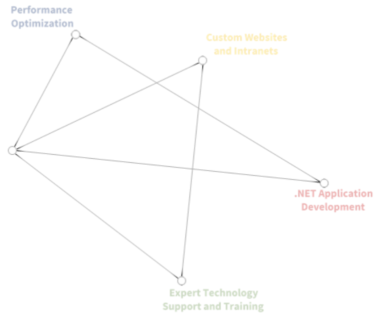
Future releases will add support for SMS and other forms of authentication.

# Installation & Configuration

The Provider is installed following the standard Extensions installation process accessed via the "Settings" -> "Extensions" portion of the Persona Bar. After successful installation the Provider will appear under the Authentication Systems section of extensions. Before first use you will need to follow the configuration steps below to enable and otherwise setup the Provider.

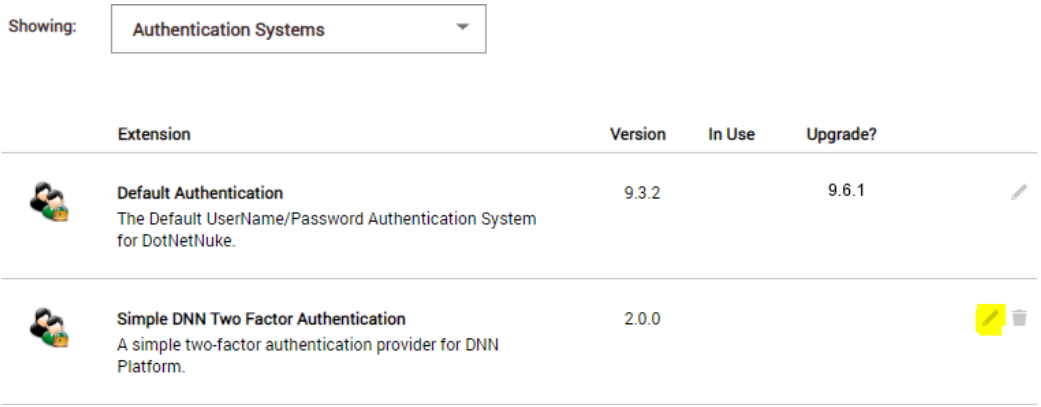
## Prerequisites

Before installation it is important to ensure that your DNN Installation is successfully able to send SMTP emails. Without an ability to send emails Two Factor Authentication might not be able to succeed and you will be unable to login.


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training

## Configuration

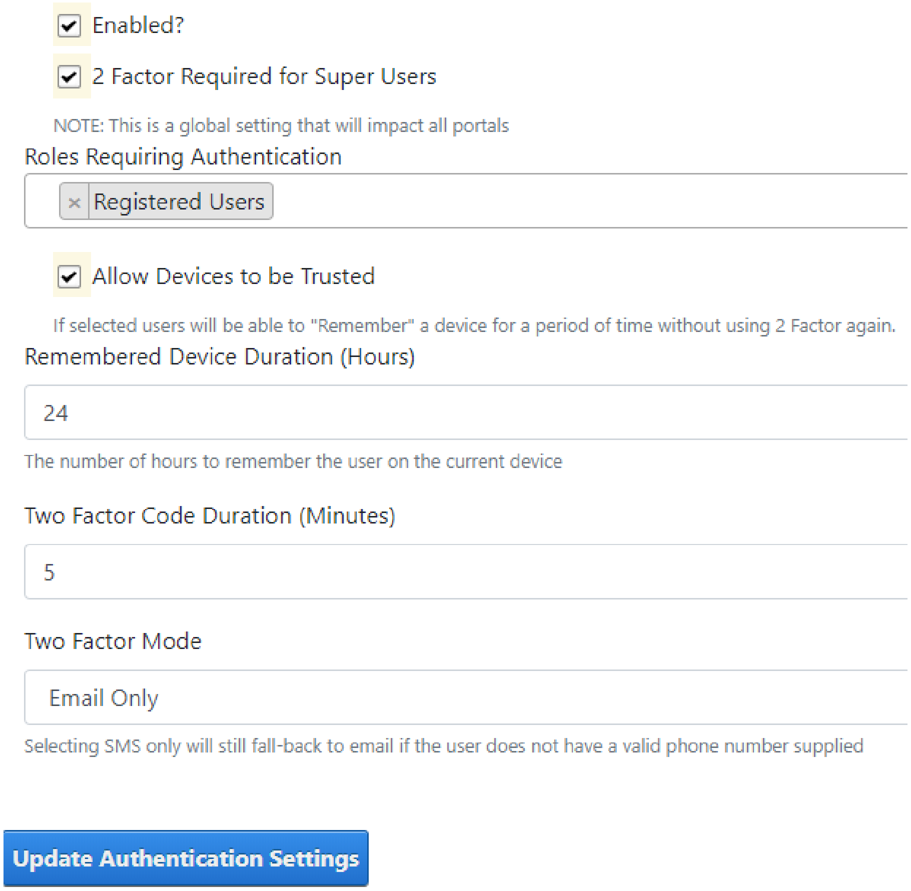
After successful installation, the Persona Bar Extensions page will refresh and display the list of installed Authentication systems, similar to the following. Select the "Edit Pencil" to enter setup mode.



Showing: Authentication Systems

| Extension | Version | In Use | Upgrade? |
|---|---|---|---|
| **Default Authentication**<br>The Default UserName/Password Authentication System for DotNetNuke. | 9.3.2 | | 9.6.1 |
| **Simple DNN Two Factor Authentication**<br>A simple two-factor authentication provider for DNN Platform. | 2.0.0 | | |

Upon opening the "Settings" for the Provider you are able to select the "Site Settings" option to configure the installation for the current Portal. This settings screen will look similar to the following.



☑ Enabled?

☑ 2 Factor Required for Super Users

NOTE: This is a global setting that will impact all portals

Roles Requiring Authentication: × Registered Users

☑ Allow Devices to be Trusted

If selected users will be able to "Remember" a device for a period of time without using 2 Factor again.

Remembered Device Duration (Hours): 24

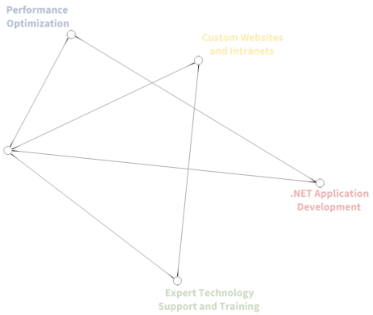
The number of hours to remember the user on the current device

Two Factor Code Duration (Minutes): 5

Two Factor Mode: Email Only

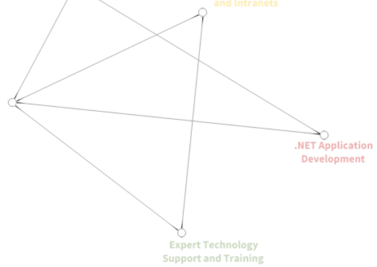
Selecting SMS only will still fall-back to email if the user does not have a valid phone number supplied

Update Authentication Settings


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training

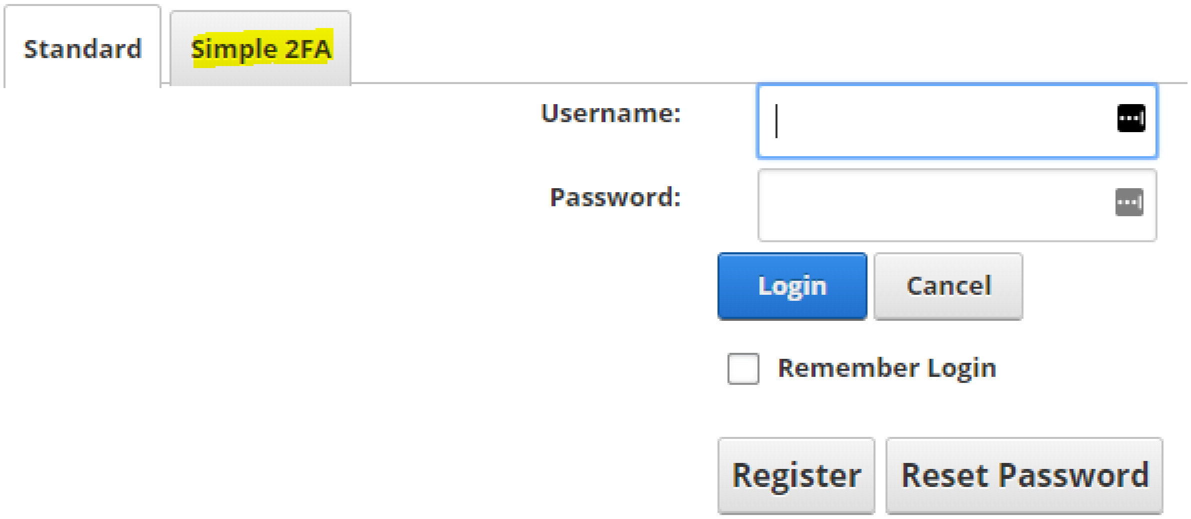
The table below outlines each of the options and their functions.

| Option | Description |
|---|---|
| Enabled | This is a toggle to enable or disable this authentication provider.  If unchecked you should ensure that you have another provider enabled. |
| 2 Factor Required for Super Users | This is a global setting for the installation, if selected, any "Super User" within the installation will be required to use two factor authentication. |
| Roles Requiring Authentication | This allows you to select the individual role(s) that are required to complete two factor Authentication.  If a user is a member of any of the selected roles they will be required to follow the two-factor process.  By selecting "Registered Users" you are able to require two factor authentication for all users |
| Allow Devices to Be Trusted | If checked this will allow a user to remember the device they are currently using to avoid two factor authentication in the future.  The duration of remembrance is controlled by the next option. |
| Remembered Device Duration | This is a value, in hours that an individual device should be remembered allowing the user to bypass two factor authentication. |
| Two Factor Mode | Email Only – This will send two factor authentication requests using email only<br>Twilio SMS or Email – This will require SMS as a first attempt, but will allow users to send via email if they are unable to receive SMS. |
| Twilio Account SID | This is the Account SID from within your Twilio Console, see the next section for instructions. |
| Twilio Auth Token | This is the Authentication Token within your Twilio Console, see the next section for instructions. |
| Twilio Phone Number | This is your account phone number for Twilio. |


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training

## Validation of Configuration

Once following the configuration steps above it is recommended that you log out of the installation and test functionality prior to disabling the default DNN Authentication. Upon visiting your login page you should see a tabbed display on the login page similar to the following.

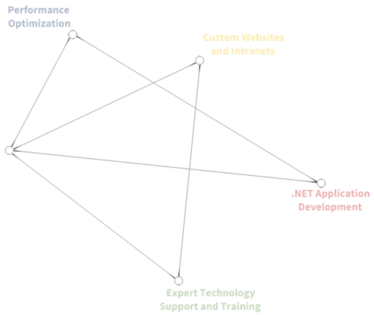


You will want to select "Simple 2FA" and attempt login. This should guide you through the login process.

## Disabling DNN Authentication

Once you have validated that the Two Factor authentication is working as desired the final step is to edit the settings for "Default Authentication" and uncheck the "Enabled" box.  After doing so your installation will be 100% utilizing the new Provider.

Suppose you have any issues with login, after doing the above. In that case, you can utilize the "Emergency Disablement" option discussed later in this document to bypass all Two-Factor behaviors and revert to an implementation of the standard DNN solution.


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training

# Twilio Account Configuration

If you have enabled Twilio authentication in the settings, you will need to have a properly created, SMS enabled Twilio account. You will need the Account SID, Auth Token, and phone number from your Twilio Console.

Given the Twilio platform's dynamic nature, we recommend following the instructions here: https://www.twilio.com/docs/iam/credentials/api to create your own values. The IowaComputerGurus team, on a consulting basis, can additionally be available to assist with the account setup for a nominal fee.

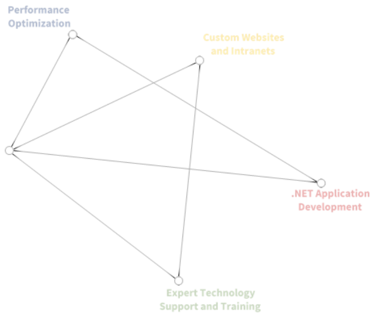
*NOTE: This module does utilize the "Lookup API" as part of Twilio to improve the experience for phone number entry. As such, test credentials with Twilio will NOT work and you must have a paid plan.*

## Estimated Twilio Costs (October 2020)

Twilio is a usage-based provider for SMS services, so it is important to understand what API's we are using to best judge your environment's potential costs. The following information is accurate as of October 2020; please reference Twilio current pricing as this is only provided for reference.

- Initial Device Setup
  - 1 Call to the Lookup Api ($0.005 USD each) to verify the phone number
  - 1 SMS to the recipient ($0.0075 USD)
- Future Device Login
  - 1 SMS to the recipient ($0.0075 USD)

Given the nature of the per-use costs for initial device setup, we do NOT recommend using SMS based two factor for pubic registration as it is not possible to easily limit the number of attempted verifications when adding a new number to an account.


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training

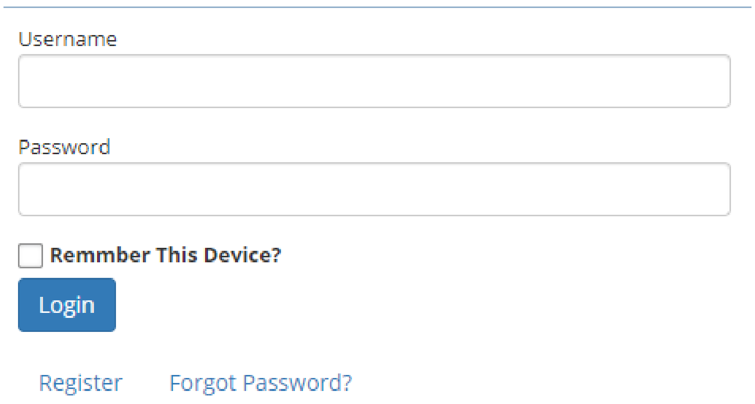
# Basic Usage

As a replacement for the default DNN Authentication provides the primary interface for interaction will be the login form itself, with additional screens displayed depending on the user's selection.

This module follows design concepts from the Bootstrap design concepts; depending on your skin it may be necessary to add/edit styles to meet your needs. All visual text items have been loaded to Localization files for customization as needed.

## Login Form

The login form is the first screen displayed to users and will look similar to the following depending on the enabled features and content.

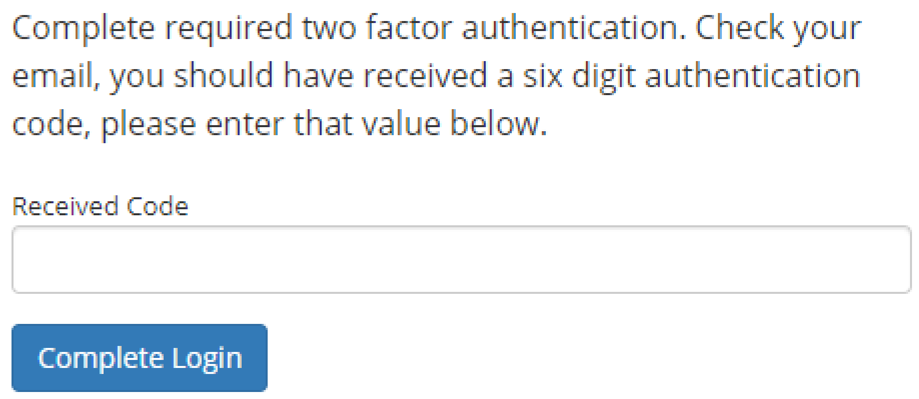


### Login Failure Notices

In the case of a login failure, the standard DNN Platform error message is displayed to the user.  All existing lockout processes will still apply.

## Complete Two Factor (Email)

After a successful login, if the user is required to complete two-factor authentication, they will see this secondary input screen to supply the provided code.



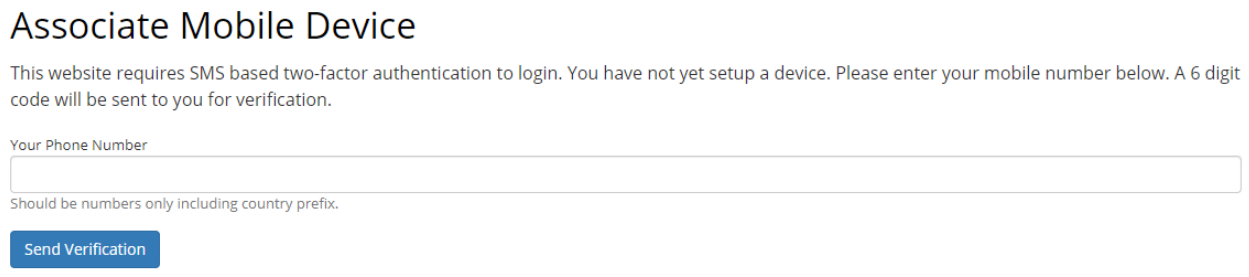
Complete required two factor authentication. Check your email, you should have received a six digit authentication code, please enter that value below.

Received Code

The user may enter the code received from their email and complete the login.  Maximum field lengths have been applied to this field to help ensure successful input.

### Associate Phone Number (SMS)

If a user attempts to login and is required to utilize two-factor authentication the first time, they will be requested to associate a phone number to their Account.



Associate Mobile Device

This website requires SMS based two-factor authentication to login. You have not yet setup a device. Please enter your mobile number below. A 6 digit code will be sent to you for verification.

Your Phone Number

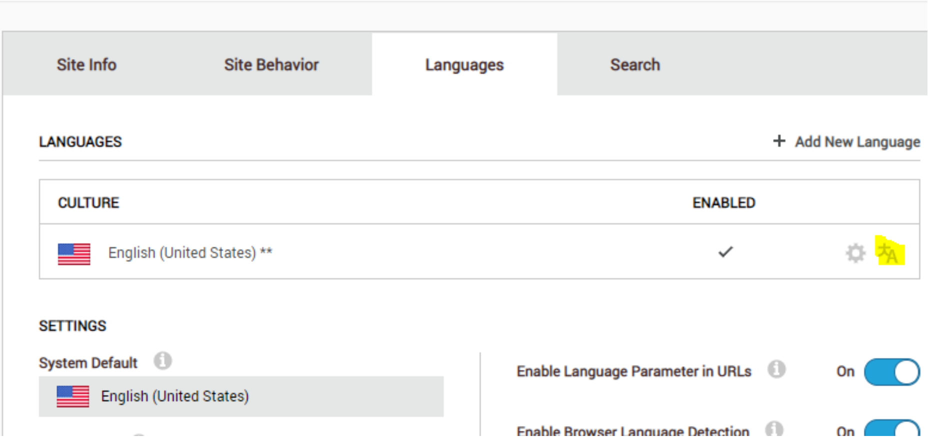
Should be numbers only including country prefix.

Upon clicking "Send Verification," the users supplied phone number will be validated and a one-time use code sent to their device for verification. Once they input the value they will be logged in and future logins will successfully work with two-factor.

## Language Customization

For the ease of use, all displayed items have been stored in Localization files that can be edited by site administrators.  To make these edits, you can navigate to "Settings" -> "Site Settings" -> "Languages" in the Persona Bar.  This will display the following screen.

## Site Settings



LANGUAGES

| CULTURE | ENABLED |
|---|---|
| English (United States) ** | ✓ |

SETTINGS

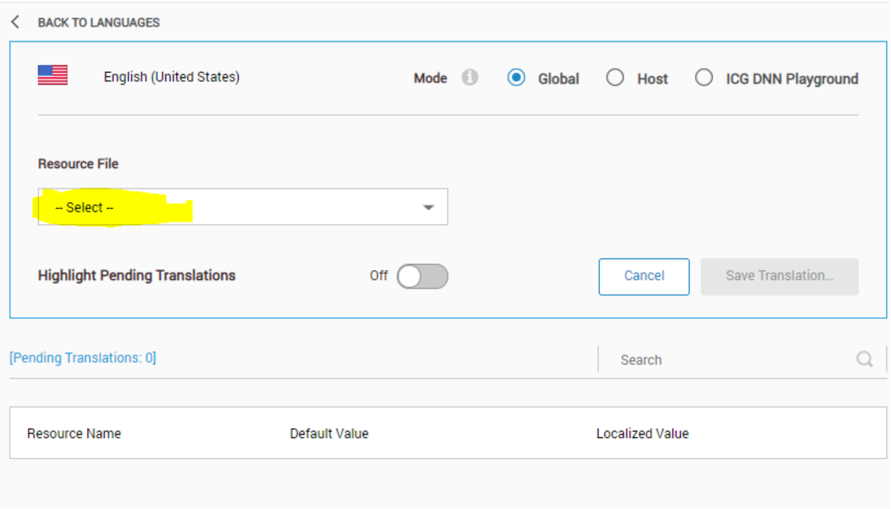
System Default: English (United States)

Enable Language Parameter in URLs: On

Enable Browser Language Detection: On

Select the highlighted option to open the Translation Edit screen, which will look similar to the following.

## Translate Resource F...



English (United States)

Mode ● Global ○ Host ○ ICG DNN Playground

Resource File: -- Select --

Highlight Pending Translations: Off

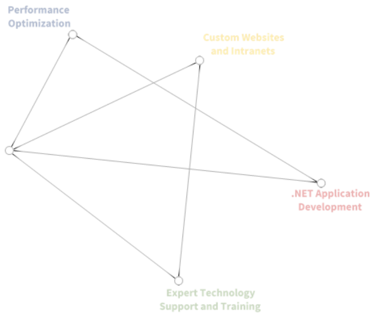
[Pending Translations: 0]

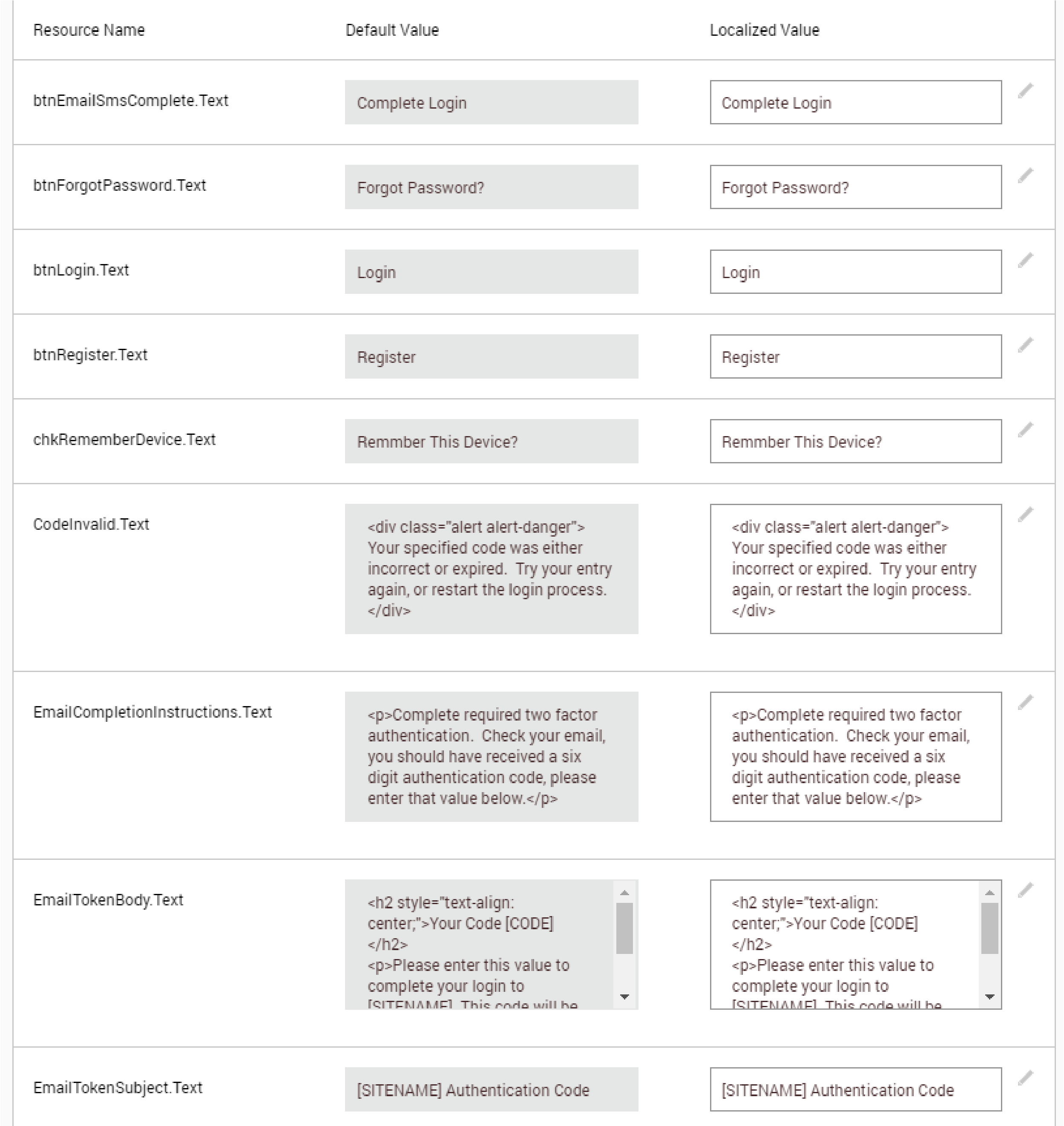
| Resource Name | Default Value | Localized Value |
|---|---|---|

From the highlighted drop-down listing select the following file:

Local Resources/DesktopModules/AuthenticationServices/IowaComputerGurus/SimpleDnnTwoFactorAuthentication/App_LocalResources/Login.ascx.resx

This will display all text values that are provided as part of the Provider and allow customization.


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training



| Resource Name | Default Value | Localized Value |
|---|---|---|
| btnEmailSmsComplete.Text | Complete Login | Complete Login |
| btnForgotPassword.Text | Forgot Password? | Forgot Password? |
| btnLogin.Text | Login | Login |
| btnRegister.Text | Register | Register |
| chkRememberDevice.Text | Remmber This Device? | Remmber This Device? |
| CodeInvalid.Text | <div class="alert alert-danger"> Your specified code was either incorrect or expired. Try your entry again, or restart the login process. </div> | <div class="alert alert-danger"> Your specified code was either incorrect or expired. Try your entry again, or restart the login process. </div> |
| EmailCompletionInstructions.Text | <p>Complete required two factor authentication. Check your email, you should have received a six digit authentication code, please enter that value below.</p> | <p>Complete required two factor authentication. Check your email, you should have received a six digit authentication code, please enter that value below.</p> |
| EmailTokenBody.Text | <h2 style="text-align: center;">Your Code [CODE] </h2><br><p>Please enter this value to complete your login to [SITENAME]. This code will be | <h2 style="text-align: center;">Your Code [CODE] </h2><br><p>Please enter this value to complete your login to [SITENAME]. This code will be |
| EmailTokenSubject.Text | [SITENAME] Authentication Code | [SITENAME] Authentication Code |

You can use this to customize the on-page values as well as the email contents for the actual two factor email.

## Emergency Disablement

If you cannot work with two-factor, such as an inability to connect with SMTP or otherwise, you can disable two-factor authentication by adding the following to the <appSettings> section of the web.config.

```
<add key="ICG_Simple2Factor_Disable2Factor" value="True" />
```

> *Please note that this is an emergency process only! Caution should be used since this disables two-factor authentication for All users and All Portals on the installation*

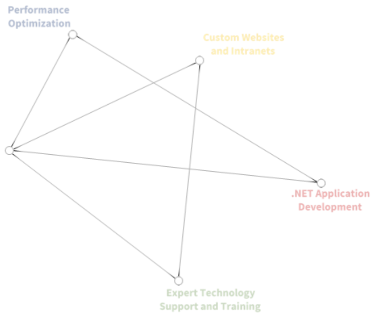
## Known Limitations

The following are known limitations of this authentication provider.

- The Provider cannot complete registration for those users who need to "Verify" their accounts prior to login.
- The Provider does NOT support the usage of DNN's built-in "Remember Me" persistent login cookie
- Users are not able to remove or add additional SMS enabled devices.

## Support

IowaComputerGurus is here to help; if you need any support, please reach out to us at support@iowacomputergurus.com or visit our support portal https://support.iowacomputergurus.com


Performance Optimization
Custom Websites and Intranets
.NET Application Development
Expert Technology Support and Training