Syniti Solutions

Authentication Configuration Manual for Windows Server 2016 and Windows Server 2019

Syniti
info@Syniti.com
www.Syniti.com

Syniti

Table of Contents

Overview

NOTE: This document applies to Syniti Solutions versions 7.3 and later.

There are three types of Stewardship Tier authentication: Basic, Integrated and Custom. Either Basic Authentication or Integrated Authentication **must** be supported to log in to the Stewardship Tier.

NOTE: If both types of authentication are enabled, the Stewardship Tier first tries to authenticate the user by Integrated Authentication, then by Basic Authentication.

Authentication methods require configuration steps in Internet Information Services (IIS), in the file system on the web server and in the Stewardship Tier. All Stewardship Tier authentication settings are available in System Administration, on the *Parameters* page, Security Settings tab.

This manual outlines the authentication configuration steps for Windows Server 2016 and Windows Server 2019.

Basic Authentication

Basic Authentication is the default configuration for the Stewardship Tier; no additional configuration is required. With Basic Authentication, the user must input a valid Stewardship Tier user ID and password to log in and access a component (i.e., a WebApp). The user must be granted component security through roles. Refer to the Stewardship Tier online help Set Security section for detailed information on security.

Basic Authentication does not maintain any relationship with the corporate Windows domain or any external authentication provider.

NOTE: Do **not** disable **Support Basic Authentication** unless configuration of Integrated Authentication is complete or there will be no way to log in to the Stewardship Tier.

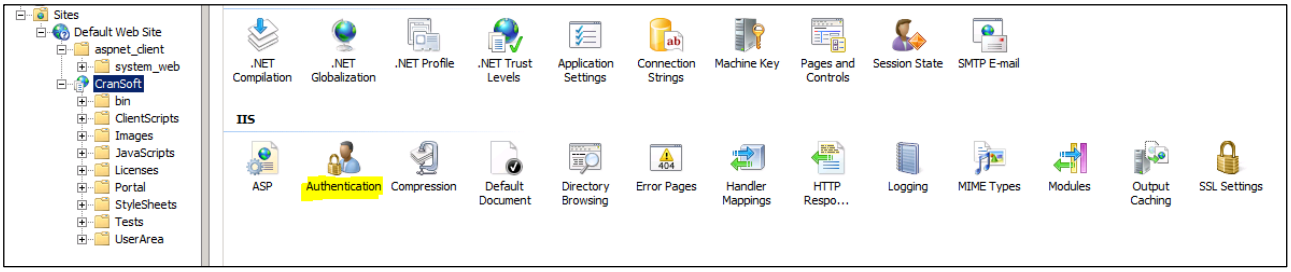
Integrated Authentication

Integrated Authentication associates a Stewardship Tier user ID with a corporate user ID, typically in a Windows Domain environment. Integration with other authentication providers is also possible. Please contact Synti Support by submitting a ticket to the Syniti customer support site at https://support.syniti.com for assistance with alternative authentication providers. Once the user is successfully authenticated (logged in) at a workstation, no additional login is required to access the Stewardship Tier.

To enable Integrated Authentication:

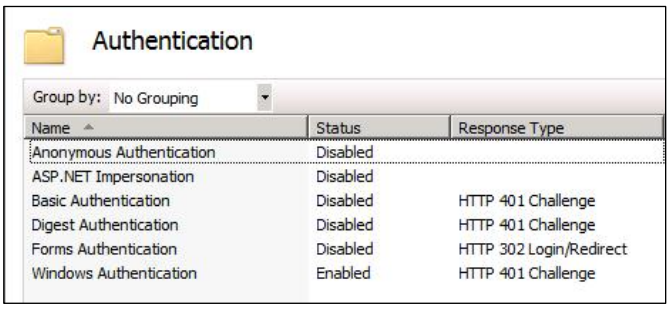
Step 1– IIS and Windows Configuration

1. Open IIS Manager (under Administrative Tools).
2. Expand the tree on the left and locate the virtual directory used for the Stewardship Tier site. This virtual directory name was chosen at installation. In the screenshot below, the virtual directory name is “CranSoft.”
3. Select the virtual directory.
4. Double-click **Authentication**.



Authentication Icon

5. Right-click **Anonymous Authentication** and select **Disable** from the list menu.
6. Right-click **Windows Authentication** and select **Enable** from the list menu.



Authentication List

NOTE: At this point the Stewardship Tier site may not be accessible to all users.

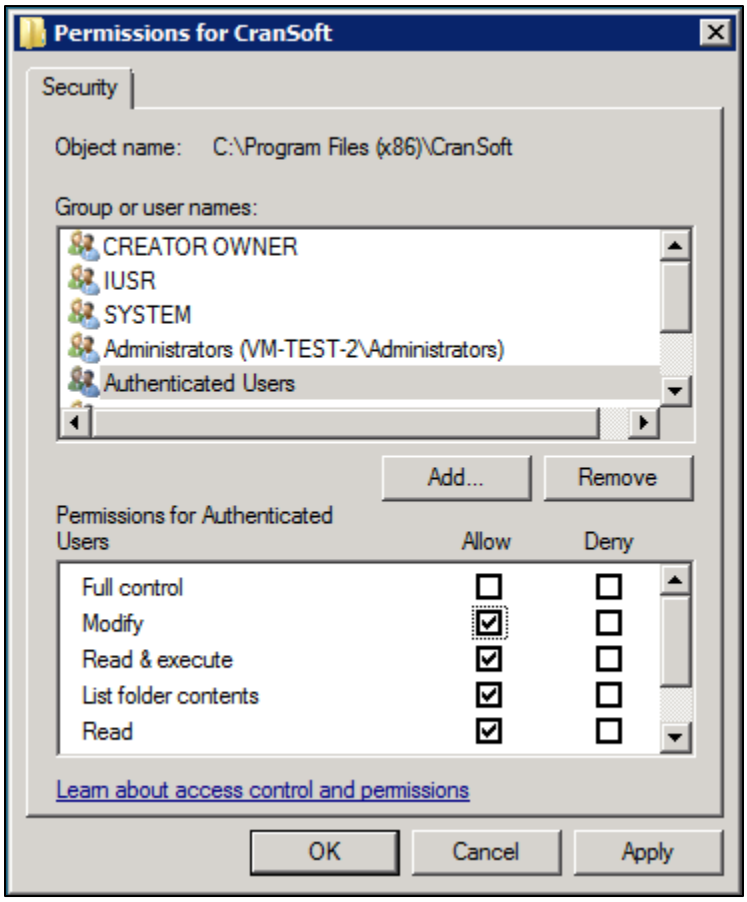
7. Close IIS Manager.
8. Locate the Stewardship Tier Installation Directory in Windows Explorer.

NOTE: The default location for the Stewardship Tier Installation Directory is **C:\Program Files (x86)\BOA\DSP**, but an alternate location may have been selected when the Stewardship Tier was installed.

9. Right-click the DSP directory and select **Properties** from the list menu.
10. Click the **Security** tab.
11. Click the **Edit** button.
12. Enter **Authenticated Users** in the **Enter the object names to select** field.

NOTE: To browse for the Authenticated Users group, click the **Advanced** and **Find Now** buttons.

13. Click the **Check Names** button and verify that the name is recognized.
14. Click the **OK** button.
15. Click the **Allow** check box for the **Modify** option from the **Permissions for Authenticated Users** option box.



Permissions Dialogue Box

16. Click the **OK** button to close the *Permissions for the folder* dialog.
17. Click the **OK** button to close the *Folder Properties* dialog.
18. Repeat steps #9 – 17 to grant Modify permissions to the Authenticated Users group on all folders that are used by the Stewardship Tier and its components, for example **C:\DSW** and **C:\BDCDirect**. The folder names depend on which components are installed and what file locations were chosen during the installation process.

NOTE: The specific folders where permissions must be modified will be different at different sites and only examples can be provided here. It is important that all folder locations accessed by the Stewardship Tier have the appropriate permissions set; otherwise, errors will be reported.

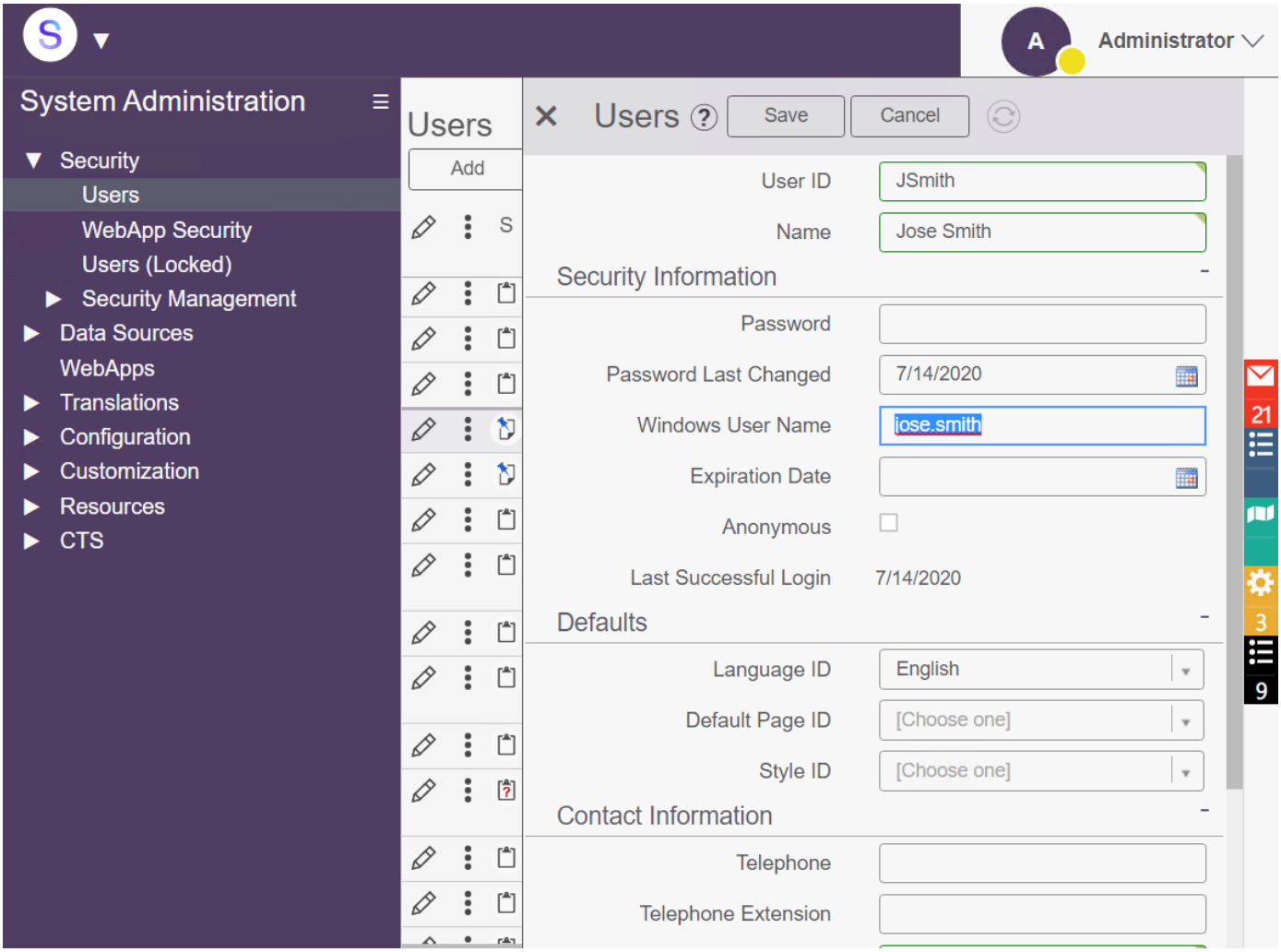
Step 2 – Stewardship Tier Configuration:

1. Log in to the Stewardship Tier site as an administrator.

NOTE: The web browser may ask for valid Windows credentials to gain access to the Login page.

2. Click **Admin** > **Configuration** > **Parameters** in the *Navigation* pane.

3. Click the **Security Settings** tab.
4. Click the **Support Integrated Authentication** check box to enable it.
5. Navigate to **Security** > **Users** in the *Navigation* pane.
6. Locate a User ID who will be accessing the Stewardship Tier using Integrated Authentication.
7. Click **Vertical View**.
8. Click **Edit**.



Windows User Name

9. Enter the user name used for Integrated Authentication in **Windows User Name** field.

NOTE: Provide a Windows User Name in the format domain\username. This name is contained within the Users table. Do not provide a password.

NOTE: If the password field is NULL or empty, a validation warning displays when the record is saved, indicating the user associated with this account will not be able to log in with Basic Authentication. If users will only be logging in using Windows Integrated Authentication, accept the validation warning by clicking the **Yes** button; otherwise, set a password.

10. Repeat steps #6 – 9 for each user that will be accessing the Stewardship Tier using Integrated Authentication.
11. Confirm that Integrated Authentication has been configured correctly by accessing the Stewardship Tier site from a client computer (not the web server). Verify that the site can be accessed without the user having to provide credentials.

NOTE: Perform steps #12–14 below if Integrated Authentication will be the only supported authentication method and Basic Authentication will not be required.

12. Select **Configuration > Parameters** in the *Navigation* pane.
13. Click **Security Settings** tab**.**
14. Click **Support Basic Authentication** check box to disable it. The check box is empty, and Basic Authentication is not supported.

Custom Authentication

When the site parameter **Support Custom Authentication** is enabled, user authentication is delegated to a third-party plugin to be developed on site. This is implemented through an external page that references assemblies provided by the Stewardship Tier and implements the expected functionality. Obtain more information about developing a custom authentication handler by submitting a ticket to the Syniti customer support site at https://support.syniti.com.

Auto Register

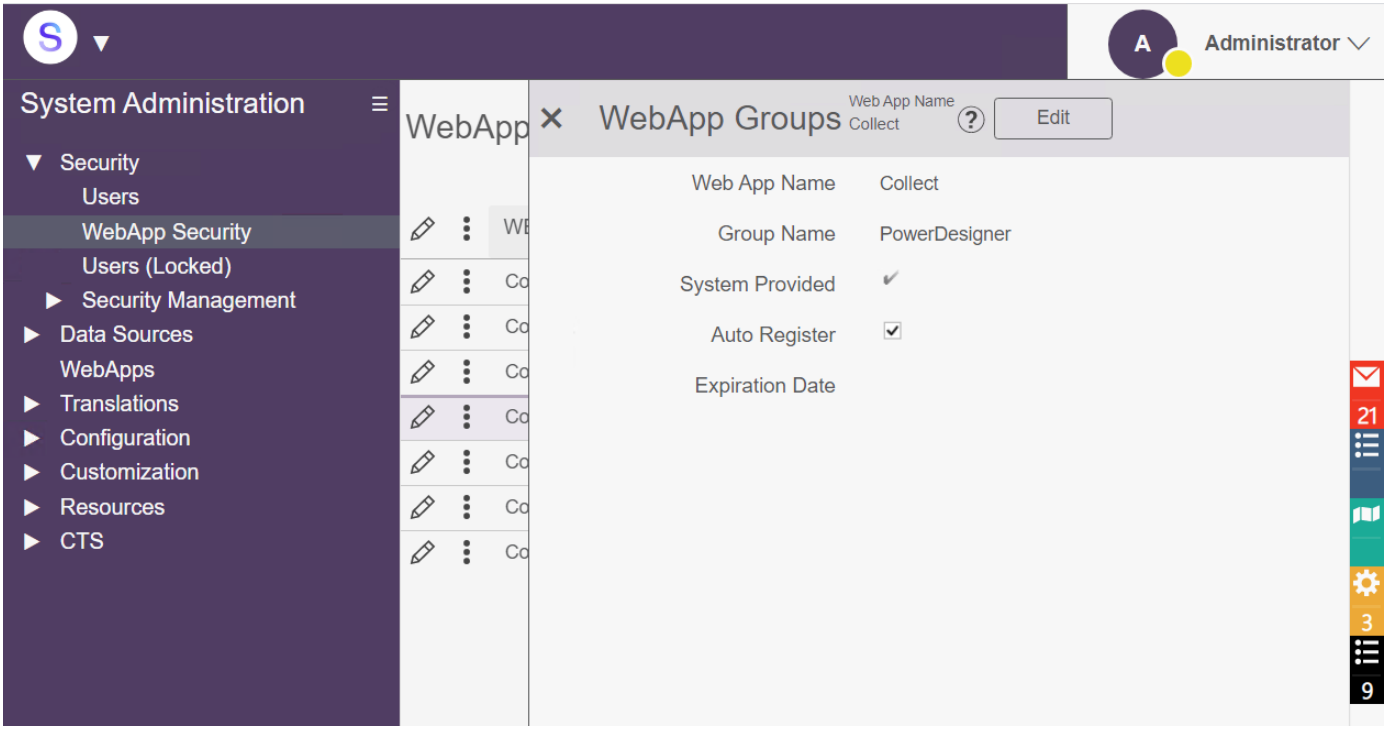
If a majority of new users need a common set of WebApp Group memberships, the Stewardship Tier has a feature that automatically creates users and adds them to WebApp Groups when users attempt to access the site for the first time using Integrated Authentication. This is accomplished through the Auto Register property that is available in the *Vertical* View of a WebApp Group. The new Stewardship Tier user is automatically added to all WebApp Groups with Auto Register enabled.

NOTE: Consider the security implications of enabling Auto Register. Anyone with a valid domain login who attempts to access the site automatically gains permissions to the Stewardship Tier.

NOTE: Auto Register has no effect on the group memberships of existing users.

To Auto Register users to a WebApp group:

1. Select **Admin > Security > WebApp Security** in the *Navigation* pane.
2. Click **Group**s for the WEB APP NAME.
3. Click **Vertical View** for the GROUP NAME.



Auto Register Check box

4. Click the **Auto Register** check box to enable it.

Last Updated on 7/29/2020