



Syniti Solutions

**Authentication Configuration Manual for Windows Server 2008 and
Windows Server 2012**



Table of Contents

Overview	1
Basic Authentication	2
Integrated Authentication	2
Custom Authentication	6
Auto Register	6



Overview

NOTE: This document applies to BackOffice Associates® Solutions versions 6.0 and later.

There are three types of Data Stewardship Platform (DSP®) authentication: Basic, Integrated and Custom. Either Basic Authentication or Integrated Authentication **must** be supported in order to log in to the DSP®.

NOTE: If both types of authentication are enabled, the DSP® 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 DSP®. All DSP® authentication settings are available in System Administration, on the *Parameters* page, Security Settings tab.

This manual outlines the authentication configuration steps for Windows Server 2008 and Windows Server 2012.



Basic Authentication

Basic Authentication is the default configuration for the DSP®; no additional configuration is required. With Basic Authentication, the user must input a valid DSP® user ID and password to log in and access a component (i.e., a WebApp). The user will need to be granted component security through roles. Refer to the DSP® online documentation 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 DSP®.

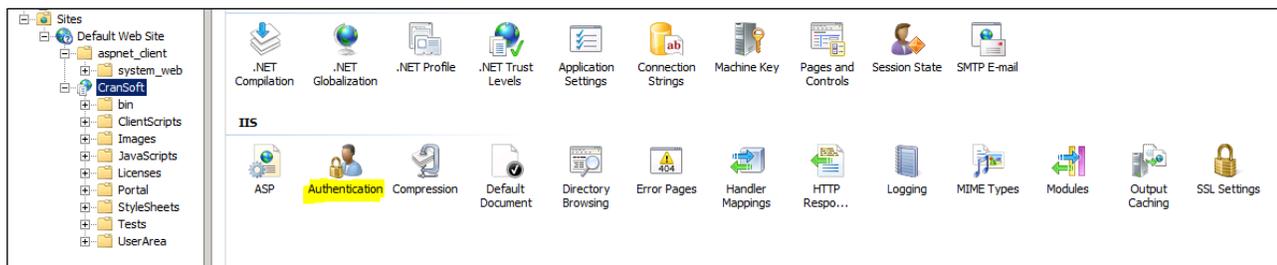
Integrated Authentication

Integrated Authentication associates a DSP® user ID with a corporate user ID, typically in a Windows Domain environment. Integration with other authentication providers is also possible. Please contact BackOffice Associates® Support by submitting an issue to the BackOffice Associates® customer support site, reachable at <https://support.boaweb.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 DSP®.

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 DSP® 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**.

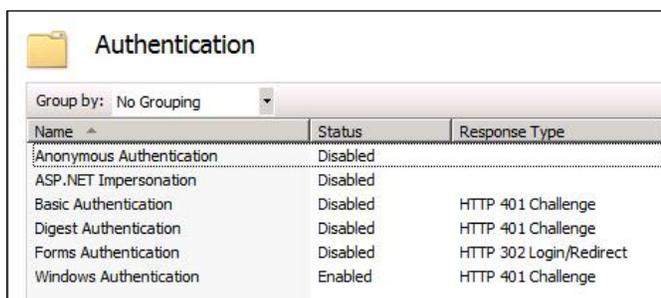


Authentication Icon

5. Right click **Anonymous Authentication** and select **Disable** from the list menu.

Copyright © 2020 Syniti and/or its affiliates. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Other names appearing within the product manuals may be trademarks of their respective owners.

6. Right click **Windows Authentication** and select **Enable** from the list menu.



The screenshot shows the 'Authentication' folder in IIS Manager. It contains a table with the following data:

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Authentication List

NOTE: At this point the DSP® site may not be accessible to all users.

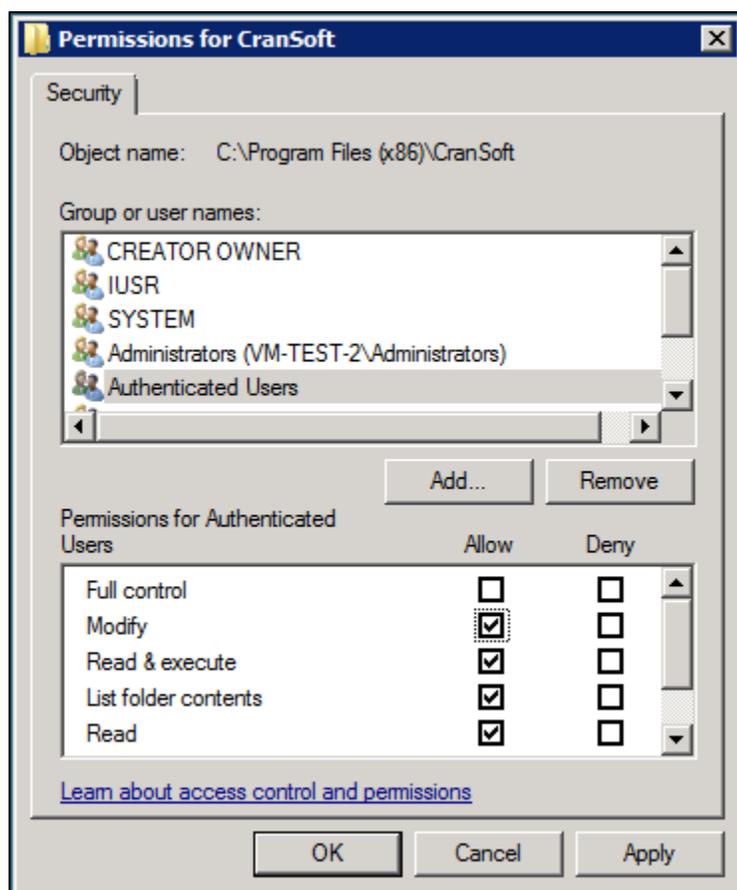
7. Close IIS Manager.
8. Locate the DSP® Installation Directory in Windows Explorer.

NOTE: The default location for the DSP® Installation Directory is **C:\Program Files (x86)\BOA\DSP**, but an alternate location may have been selected when the DSP® 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 **Advanced** and **Find Now** buttons.

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



Permissions Dialogue Box

16. Click **OK** button to close Permissions for the folder dialog.
17. Click **OK** button to close 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 DSP® and its components, for example **C:\DSW** and **C:\BDCDirect**. The folder names will depend on which components are installed and what file locations were chosen during the installation process.

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

Step 2 – DSP® Configuration:

1. Log in to the DSP® 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.

Copyright © 2020 Syniti and/or its affiliates. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Other names appearing within the product manuals may be trademarks of their respective owners.

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

The screenshot displays the 'System Administration' interface. On the left is a navigation pane with 'Security' selected, containing sub-items: 'Users', 'WebApp Security', 'Users (Locked)', and 'Security Definitions'. The main content area is titled 'Users' and includes 'Save' and 'Cancel' buttons. The user 'JSmith' is selected, with their name 'Jose Smith' displayed. The form is organized into sections: 'Security Information' (Password, Password Last Changed: 11/26/2013, Windows User Name, Expiration Date), 'Defaults' (Language ID: English, Default Page ID: [Choose one]), 'Contact Information' (Telephone, Telephone Extension, E Mail Address: joesmith@example.com), 'Format Options' (Locale ID: Default), and 'Logs' (View Log In History button).

Windows User Name

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

Copyright © 2020 Syniti and/or its affiliates. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Other names appearing within the product manuals may be trademarks of their respective owners.



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 **Yes** button; otherwise, set a password.

10. Repeat steps #6 – 9 for each user that will be accessing the DSP® using Integrated Authentication.
11. Confirm that Integrated Authentication has been configured correctly by accessing the DSP® 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 if Integrated Authentication will be the **only** supported authentication method and Basic Authentication will not be required.

12. Select **Configuration > Parameters** on *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 DSP® and implements the expected functionality. More information on developing a custom authentication handler can be obtained by submitting an issue to the BackOffice Associates® customer support site at <https://support.boaweb.com>

Auto Register

If a majority of new users will need a common set of WebApp Group memberships, the DSP® has a feature that will automatically create users and add 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 DSP® user will automatically be 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 will automatically gain permissions to the DSP®.

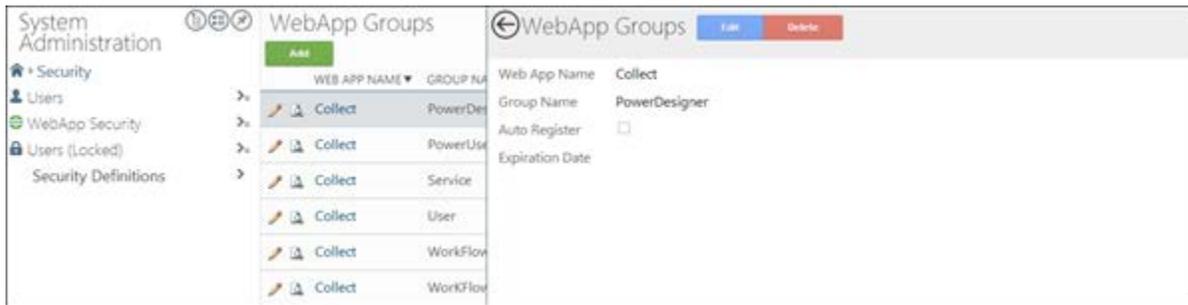
NOTE: Auto Register has no effect on the group memberships of existing users.

To auto register users to a WebApp group:

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

Copyright © 2020 Syniti and/or its affiliates. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Other names appearing within the product manuals may be trademarks of their respective owners.

Syniti



Auto Register Check box

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

Last Updated on 7/29/2020