Security Rights Setup for BS&A .NET Applications

*Questions? From your BS&A program, go to **Help>Contact Customer Support** and select **Request Support Phone Call** or **Email Support**. Or, you may call us at (855) 272-7638 and ask for the appropriate support department. Questions for our I.T. department may be submitted by phone (same number), or by emailing tech@bsasoftware.com.*

This whitepaper is an informational document outlining the process for setting up proper Windows folders and security rights to allow updating of the applications, syncing of application versions via file copy processes, and user-initiated application database backups.

The BSA Windows Folder Share

BS&A uses a Windows folder share to hold files for what is referred to by BS&A as the "Shared Program Folder". This folder contains a sub-folder for each BS&A .NET application. The files in this folder, with the exception of Attachment folders*****, are non-volatile files that can be replaced. BS&A recommends a low security setting on the share for ease of use.

Requirements:

- A Windows folder share with appropriate share and security rights
- An administrator user with security rights to add and modify folders
- Basic knowledge of Windows folder security

Setup:

BS&A strongly recommends the share be kept on an SQL server housing databases for the applications. Reasoning for this strategy is that the BSA share houses a temporary location where the SQL server will store database backups that are initiated by the end user. Follow these steps to configure the share:

1. Create a BSA folder on the SQL server.
2. Share the folder as BSA.
3. Give "Everyone" full control****** over the share.
4. Add "Everyone" to the folder security. Give them all rights except for "Full control".

Setting the "Shared Program Folder" Path:

All BS&A applications are consistent in methodology for setting this path. The applications simply need to point to the BSA share. They will automatically create and use the appropriate sub-folder. To set up the path, follow these steps:

1. Login to a BS&A .NET application with an Enterprise Administrator user name.
2. In the "Application Views" section at in the upper left, click "Program Setup".
3. Click the "Administration" tab. On that tab, click the "Shared Program Folder" button.
4. Click the edit link and type in the BSA share path. Typically, this will be \\SQLSERVERNAME\BSA.
5. Click Close.

The Program Update Security User

BS&A understands the need for security in network environments. As a result, a feature is available in the .NET applications to allow a non-administrator*** user to run updates to their applications. The option is called "Program Update Security". When using this option, the network administrator can insert a user that has local administrator rights to the computer running the applications. All updates are executed as this user, allowing the application to update without giving the Windows user currently logged into the computer administrator rights over the PC.

Requirements:

- A Windows user with local admin rights to ALL machines running BS&A .NET applications
- General knowledge of Windows users and security rights
- A Windows Active Directory Domain is strongly recommended for this process

Setup:

To set "Program Update Security", follow these steps:

1. Login to a BS&A .NET application with an Enterprise Administrator user name.
2. In the "Application Views" section in the upper left, click "Program Setup".
3. Click the "Administration" tab. On that tab, click the "Program Update Security" button.
4. Check the box to allow users to run BSA program updates.
5. Fill in the 3 boxes below with the appropriate Domain/Username/Password of the admin user.
6. Click Close.

Denying Rights to Run an Update From Inside a BS&A Application

Any administrator wanting to stop the BS&A application users from running an update can do so using a security setting inside of each application.

Requirements:

- Basic navigation knowledge of BS&A .NET applications
- An Enterprise Administrator within BS&A .NET

Setup:

To deny rights to download/run an update to the application, follow these steps:

1. Login to a BS&A .NET application with an Enterprise Administrator user name.
2. In the "Application Views" section at in the upper left, click "Program Setup".
3. Click the "Administration" tab. On that tab, click the "Users" button.
4. Select the user to deny rights to
5. Click the "Security Settings" button. Switch the user to "Custom Access". ****
6. Make sure the Program Setup(left) / Download latest version (right) checkbox is cleared.

Notes:

*Some BS&A applications have file attachments that are stored in the BSA share by default. These files are volatile and cannot be recovered without a backup. It is understood that additional security might be necessary for these attachments. For additional assistance moving these files to a more secure location, please contact the BS&A tech department at tech@bsasoftware.com.

**Standard Windows security practice recommends controlling share access at the folder security level. It is suggested to give everyone full control to the share itself, then use the security tab to control which users have access.

***Administrator in the "Program Update Security" section of this document refers to a local administrator over the computer running the BS&A applications. It is not referring to a domain administrator unless the two are one and the same.

****A user with "Custom Access" must have checkboxes selected for each action they will be allowed to perform. If an administrator wants to deny rights to download an update, they must select all other appropriate checkboxes to allow a user to have other functions. These options will not be selected by default.